Corso di Laurea in Matematica - Università di Firenze

Appunti di Teoria Elementare dei Numeri

Francesco Fumagalli

Corso di Teoria dei Numeri

A.A. 2017-2018

(Versione 1.14)

A Martino, il mio ϵ

PREFAZIONE

Il materiale presente in queste note dovrebbe coprire interamente il corso di *Teoria dei Numeri* che terrò nell'A.A. 2017/18 per il Corso di Laurea Magistrale in Matematica (9 CFU), presso l'Università degli Studi di Firenze. In realtà, per questioni di tempo, è probabile che alcune parti che compaiono in questi appunti non potranno essere presentate in classe. Mi auguro comunque che non accada il contrario, e che gli studenti del corso possano qui trovare un utile riscontro di quanto sarà effettivamente svolto a lezione.

Il corso e la seguente dispensa vogliono essere un'introduzione ai cosiddetti *metodi elementari nella Teoria (Analitica) dei Numeri*. La maggior parte dei teoremi qui presentati riguardano i numeri interi; gli enunciati sono chiari e facilmente comprensibili. È tutt'altra cosa invece per quanto riguarda le loro dimostrazioni, le quali spesso hanno richiesto tecniche sofisticate in svariati ambiti della Matematica, ad esempio si passa dall'analisi complessa alla geometria algebrica, la coomologia, ecc. ecc. Una volta però dimostrato un teorema, e soprattutto se il suo enunciato è semplice, si è soliti cercare una dimostrazione che faccia uso solamente di "argomenti elementari" e che, almeno in linea teorica, possa essere compresa anche da chi non possiede conoscenze specifiche in particolari settori della Matematica. Le dimostrazioni elementari non sono migliori di altre, né sono necessariamente facili. In realtà, come vedremo, molte di queste sono tecnicamente difficili. Hanno però il grande vantaggio di soddisfare ad una condizione estetica ben precisa: utilizzano pressoché solo argomenti aritmetici.

Nello scrivere queste note ho raccolto materiale da diverse fonti, coll'intento sempre di prediligere le dimostrazioni più chiare ed eleganti, quelle che - per dirla secondo le parole di Paul Erdös - provengono direttamente dal *"Libro"*.

Un importante punto di partenza per questa stesura sono state alcune note del corso di *Matematiche Elementari da un punto di vista superiore*, tenuto dal Prof. C. Casolo negli A.A. 2002/03 e 2003/04 (Corso di Laurea Triennale). Buona parte del materiale presente nei primi tre capitoli è presa direttamente da lì . Per il resto, i principali testi da me consultati e utilizzati sono stati (in ordine di importanza):

- M. B. Nathanson, *Elementary Methods in Number Theory*, [46];
- M. B. Nathanson, *Additive Number Theory: the Classical Bases*, [45];
- T. Apostol, *An introduction to Analythic Number Theory*, [4];

- J. M. De Koninck e F. Luca, *Analytic number theory: exploring the anatomy of integers*, [13];
- H. E. Rose, *A Course in Number Theory*, [56].

Questo materiale è stato poi integrato, ed in parte aggiornato, con informazioni prese direttamente da articoli scientifici (tutti presenti nella bibliografia) e siti internet/blog; tra questi citiamo:

- *What's new. By Terence Tao*: `https://terrytao.wordpress.com/`,
- *Andrew Granville's Home Page*: `http://www.dms.umontreal.ca/~andrew/index.php`.

Quello che state leggendo è stato scritto in LaTeX usando il file di stile ArsClassica. Una guida molto utile che mi sento di consigliare, è *L'arte di scrivere con LaTeX* di L. Pantieri e T. Gordini ([51]).

Buona lettura,

Francesco Fumagalli
Firenze, 7 giugno 2017

NOTAZIONI E CONVENZIONI

La notazione adottata rispecchia quella stardand oggigiorno normalmente in uso. In questa pagina ci limitiamo a ricordare il significato di alcuni simboli.

Denoteremo con $\mathbb{N}$ l'insieme dei numeri interi non-negativi (chiamati anche numeri naturali) e con $\mathbb{N}^*$ quello degli interi positivi, mentre gli insiemi dei numeri interi, razionali, reali e complessi vengono denotati rispettivamente con $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$.

Il valore assoluto di un numero complesso z, viene indicato con $|z|$, la parte reale e immaginaria di z, rispettivamente con: $\Re(z)$ e $\Im(z)$. Invece se x è invece un numero reale, indicheremo con $\lfloor x \rfloor$ la *parte intera* di x, ovvero il più grande numero intero che è minore o uguale ad x. La *parte frazionaria* di x sarà invece denotata con $\{x\}$ ed è definita dalla relazione $\{x\} := x - \lfloor x \rfloor$; pertanto per ogni $x \in \mathbb{R}$, abbiamo che $\lfloor x \rfloor \in \mathbb{Z}$ e $\{x\} \in [0, 1)$.

Se a e b sono due interi, scriveremo $b|a$ per dire che b divide a, ovvero che esiste un intero q per cui $a = bq$. Gli interi a e b si dicono *congrui modulo* un intero m, e si scrive $a \equiv b \pmod{m}$, se $m|a - b$.

L'insieme dei numeri primi positivi viene denotato col simbolo $\mathbb{P}$. Il generico numero primo viene solitamente indicato con p (o con q), così come di solito n indica un arbitrario numero naturale. Riserviamo la notazione p_n per chiamare l'n-esimo numero primo (ad esempio $p_{11} = 31$).

Scriveremo $p^a \| n$ per intendere che p^a è la più grossa potenza di p che divide n, ovvero $p^a | n$ e $p^{a+1} \nmid n$.

Se $a_1, a_2, \ldots, a_n$ sono n numeri interi, il simbolo $(a_1, a_2, \ldots, a_n)$ indica sia un elemento del prodotto cartesiano $\mathbb{Z}^n$ sia il *Massimo Comune Divisore* (positivo) fra gli interi a_i ($i = 1, \ldots, n$). Il significato sarà chiaro dal contesto. Useremo invece $[a_1, a_2, \ldots, a_n]$ per denotare il *Minimo Comune Multiplo* degli interi a_i ($i = 1, \ldots, n$).

Se X è un insieme arbitrario, l'unione vuota di sottoinsiemi di X è $\varnothing$, mentre l'intersezione vuota è X stesso. Similmente, la sommatoria su un insieme vuoto di numeri è uguale a 0, mentre il prodotto è 1.

Le convenzioni sopra esposte per i numeri naturali passano agli indici di sommatorie e produttorie. Ad esempio, quando scriveremo

$$\sum_{m|n} \mu(m) \quad \text{e} \quad \sum_{p \le x} \log(p)$$

indicheremo le somme ripettivamente su tutti i divisori positivi m di n e su tutti i numeri *primi* (positivi) minori o uguali ad x.

INDICE

Parte I.

Preliminari

"Conterò
poco, è vero: - diceva l'Uno ar Zero - ma tu
che vali? Gnente: propio gnente.
Sia ne l'azzione come ner pensiero
rimani un coso voto e inconcrudente. lo, invece, se me metto a capofila de cinque zeri tale e quale a te, lo sai quanto divento? Centomila. È questione de nummeri. A un dipresso è quello che succede ar dittatore che cresce de potenza e de valore più so' li zeri che je vanno appresso."
([59])

1 DIVISIONI E NUMERI PRIMI

Questo primo capitolo, così come buona parte del seguente, consiste in un rapido ripasso (con qualche interessante approfondimento) di alcuni concetti elementari già studiati nei corsi di Algebra dei primi due anni (per i quali si rimanda il lettore alle dispense [7] e [8]).

MASSIMO COMUNE DIVISORE

Ricordiamo l'assioma del *buon ordinamento* per l'insieme $\mathbb{N}$: esso afferma che

> *ogni sottoinsieme non vuoto di* $\mathbb{N}$ *possiede un elemento minimo.*

Teorema 1.1.1 (Divisone euclidea.) *Siano a, b numeri interi, con $b \geq 1$. Allora esistono, e sono unici, due interi q, r tali che*

$$a = bq + r \quad e \quad 0 \leq r \leq b - 1.$$

Dimostrazione. Sia S l'insieme di tutti i numeri naturali della forma $a - bt$, con $t \in \mathbb{Z}$. Osserviamo che S non è vuoto; infatti, se $a \geq 0$ allora $a = a - b0 \in S$; se $a < 0$, allora, poiché $b \geq 1$, $a - b(a-1) \in S$. Dunque, per il principio del buon ordinamento, S ha un elemento minimo che chiamiamo r. Poiché $r \in S$ esiste un $q \in \mathbb{Z}$ tale che $a = bq + r$.

Se fosse $r \geq b$, si avrebbe

$$0 \leq r - b = a - bq - b = a - b(q+1) \in S,$$

contro la minimalità di r. Dunque $0 \leq r < b$.

La dimostrazione dell'unicità di q ed r è lasciata per esercizio. ∎

Siano m, n numeri interi non entrambi nulli. Ricordiamo che un elemento $d \in \mathbb{Z}$ si dice un *Massimo Comun Divisore* (MCD in breve) di m ed n se

- $d|m$, $d|n$ e
- per ogni intero c, se $c|m$ e $c|n$ allora $c|d$.

Ogni coppia di interi non entrambi nulli ammette due massimi comun divisori, che differiscono per il segno. Denotiamo con (m, n) il MCD *positivo* di m e n. I numeri m, n si dicono *coprimi* se $(m, n) = 1$.

Proposizione 1.1.2 (Formula di Bezout) *Siano a, b interi non entrambi nulli. Allora il massimo comun divisore (a, b) è il minimo numero intero positivo (non nullo) d, che si può scrivere nella forma $d = ua + vb$, con $u, v \in \mathbb{Z}$.*

Dimostrazione. Poiché a e b non sono entrambi nulli, l'insieme

$$\{z = xa + yb \mid x, y \in \mathbb{Z},\ z \geq 1\}$$

è non vuoto e pertanto per l'assioma del buon ordinamento ha un minimo $d = ua + vb$. Dividiamo a per d, sia $a = qd + r$, con $0 \leq r \leq d - 1$. Ora

$$0 \leq r = a - qd = (1 - qu)a + (-qv)b,$$

e quindi, per la scelta minima di d, deve essere $r = 0$. Dunque d divide a. Analogamente si prova che d divide b. Infine, se c è un divisore comune di a e b, chiaramente c divide anche d. Pertanto $d = (a, b)$. ■

La definizione di Massimo Comune Divisore fra due interi si generalizza in modo ovvio al caso di un numero arbitrario di interi. In modo simile alla Proposizione 1.1.2, si dimostra che se A è un sottoinsieme non vuoto (e non nullo) di $\mathbb{N}$, esiste un unico MCD positivo di A, che denotiamo con (A) (o con $MCD(A)$), questo è l'intero positivo d tale che

- $d|a$, per ogni $a \in A$ e
- per ogni intero c che divide ogni elemento di A, si ha che $c|d$.

Esattamente come fatto nella Proposizione precedente, si dimostra (per induzione su k) che se $(a_1, a_2, \ldots, a_k) = d$ allora esistono z_1, z_2,..., $z_k \in \mathbb{Z}$ tali che

$$d = \sum_{i=1}^{k} a_i z_i.$$

Proposizione 1.1.3 *Sia $A = \{a_1, \ldots, a_k\}$ un sottoinsieme di $\mathbb{N}$ tale che $MCD(A) = 1$. Se $b \in \mathbb{N}$ è tale che $b \geq (a_k - 1)\sum_{i=1}^{k-1} a_i$, allora esistono $x_1, \ldots, x_k \in \mathbb{N}$ tali che $b = \sum_{i=1}^{k} a_i x_i$.*

Dimostrazione. Siano $z_1, z_2, \ldots, z_k \in \mathbb{Z}$ tali che $b = \sum_{i=1}^{k} a_i z_i$. Dividiamo con resto ogni z_i per a_k:

$$z_i = a_k q_i + x_i, \quad \text{con } 0 \leq x_i \leq a_k - 1,$$

per $i = 1, 2, \ldots k - 1$. Poniamo

$$x_k = z_k + \sum_{i=1}^{k-1} a_i q_i.$$

Allora $x_k \in \mathbb{Z}$ e si ha

$$\begin{aligned} b &= \sum_i a_i z_i \\ &= a_1(a_k q_1 + x_1) + \ldots + a_{k-1}(a_k q_{k-1} + x_{k-1}) + a_k z_k \\ &= a_1 x_1 + \ldots + a_{k-1} x_{k-1} + a_k (z_k + \sum_{i=1}^{k-1} a_i q_i) \\ &= \sum_{i=1}^{k} a_i x_i. \end{aligned}$$

Infine,

$$(a_k - 1) \sum_{i=1}^{k-1} a_i \leq b = \sum_{i=1}^{k} a_i x_i \leq (a_k - 1) \sum_{i=1}^{k-1} a_i + a_k x_k$$

implica $a_k x_k \geq 0$ e dunque anche $x_k \geq 0$. ■

Algoritmo di Euclide

Questo algoritmo consente di determinare, con un numero finito di operazioni, il massimo comun divisore (positivo) di due interi non nulli a e b.

Siano quindi a e b due numeri naturali non nulli, e possiamo assumere $b \geq 1$.

Si pone $a_0 = a$ e $a_1 = b$. Il primo passo è dividere a_0 per a_1:

$$a_0 = q_1 a_1 + a_2 \quad \text{con} \quad 0 \leq a_2 < a_1,$$

quindi, se $a_2 \neq 0$, si divide a_1 per a_2, ottenendo un resto a_3 con $0 \leq a_3 < a_2$. Si prosegue quindi con tale catena di divisioni successive; ovvero, arrivati ad a_i si definisce a_{i+1} come il resto della divisione di a_{i-1} per a_i :

$$\begin{aligned} a_0 &= q_1 a_1 + a_2 \\ a_1 &= q_2 a_2 + a_3 \\ a_2 &= q_3 a_3 + a_4 \\ &\ldots\ldots \\ a_{i-1} &= q_i a_i + a_{i+1} \\ &\ldots\ldots \end{aligned}$$

In questo modo, si ottiene una sequenza strettamente decrescente di resti positivi

$$b = a_1 > a_2 > \cdots > a_i > a_{i+1} > \ldots$$

Questa sequenza, costituita da numeri naturali, arriva a zero dopo un numero finito di passi. Detto n il più piccolo intero per cui $a_{n+1} = 0$, l'ultimo resto non nullo, a_n, è il massimo comun divisore positivo tra a e b. Cosa che si dimostra facilmente utilizzando induttivamente la seguente osservazione

Lemma 1.1.4 *Siano a e b interi non nulli, e sia r il resto della divisione di a per b. Allora $(a,b) = (b,r)$.*

DIMOSTRAZIONE. Si vedano ad esempio le dispense del corso di Algebra 1 [7]. ■

Osserviamo che l'algoritmo di Euclide, oltre a determinare (a,b), fornisce (ripercorso a ritroso) i coefficienti u, v come nella Proposizione 1.1.2, tali che $(a,b) = ua + vb$.

Esempio 1.1.1 Siano $a = 6468$ e $b = 2275$. Si ha

$$\begin{aligned}
6468 &= 2 \cdot 2275 + 1918 \\
2275 &= 1 \cdot 1918 + 357 \\
1918 &= 5 \cdot 357 + 133 \\
357 &= 2 \cdot 133 + 91 \\
133 &= 1 \cdot 91 + 42 \\
91 &= 2 \cdot 42 + 7 \\
42 &= 6 \cdot 7 + 0
\end{aligned}$$

Quindi $(6468, 2275) = 7$. Ora

$$\begin{aligned}
7 \quad &= 91 - 2 \cdot 42 = 91 - 2(133 - 91) = 3 \cdot 91 - 2 \cdot 133 = \\
&= 3(357 - 2 \cdot 133) - 2 \cdot 133 = -8 \cdot 133 + 3 \cdot 357 = \\
&= 43 \cdot 357 - 8 \cdot 1918 = \\
&= -51 \cdot 1918 + 43 \cdot 2275 = \\
&= -51 \cdot 6468 + 145 \cdot 2275.
\end{aligned}$$

FATTORIZZAZIONI

Un numero intero p si dice *primo* se $p \neq 0, 1, -1$ e l'insieme dei divisori di p è $\{1, -1, p, -p\}$; in caso contrario, il numero si dice *composto*. La proprietà fondamentale dei numeri primi è espressa nella seguente Proposizione.

Proposizione 1.2.1 *Siano $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $(a,b) = 1$, allora $a|c$. In particolare se p è un numero primo e $p|bc$, allora $p|b$ oppure $p|c$.*

DIMOSTRAZIONE. Siano $a, b, c \in \mathbb{Z}$ con $a|bc$ e $(a,b) = 1$. La seconda condizione implica che a e b non sono entrambi nulli, quindi per la formula di Bezout (Proposizione 1.1.2), esistono $u, w \in \mathbb{Z}$ tali che $1 = ua + wb$. Moltiplicando per c, si ha $c = uac + wbc$ e siccome a divide sia uac che wbc si conclude che a divide c.
Ora, sia p un primo e $p|bc$. Se p non divide b allora (essendo p primo) $(p,b) = 1$ e dunque p divide c per quanto appena provato. ■

A partire dalla Proposizione 1.2.1 si prova facilmente per induzione il seguente Lemma.

Lemma 1.2.2 *Sia n un numero intero diverso da $0, 1, -1$. Allora esiste un numero primo che divide n. Inoltre, se n è un numero naturale composto, esiste un primo $p < \sqrt{n}$ che divide n.*

Dimostrazione. Esercizio. ■

Utilizzando questo Lemma si dimostra poi agevolmente che ogni intero (diverso da $0, 1, -1$) ammette una fattorizzazione essenzialmente unica come prodotto di numeri primi.

Teorema 1.2.3 (Teorema Fondamentale dell'Aritmetica) *Sia $a \in \mathbb{Z}$, $a \neq 0, 1, -1$. Allora esistono un intero positivo s ed s numeri primi $p_1, p_2, \ldots, p_s$ tali che*

$$a = p_1 p_2 \cdots p_s \, .$$

Se inoltre $q_1, q_2, \ldots, q_t$ sono primi tali che $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_s$, allora $s = t$ ed esiste una permutazione σ di $\{1, 2, \ldots, s\}$ tale che, per ogni $i = 1, 2, \ldots, s$, $q_i = \pm p_{\sigma(i)}$.

Dimostrazione. Si rimanda a [7]. ■

Denotiamo con $\mathbb{P}$ l'insieme di tutti i numeri primi positivi. Dal Teorema precedente segue che ogni intero $n \neq 0$ si scrive come il prodotto

$$n = \pm \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

dove $p^{v_p(n)} \| n$ per ogni $p \in \mathbb{P}$. I $v_p(n)$ sono numeri naturali univocamente determinati da n, e quasi tutti nulli, cioè $v_p(n) \neq 0$ solo per un numero finito di primi p. La funzione $v_p(n)$ ($n \in \mathbb{N}^*$) viene detta *valore p-adico* ed è *completamente additiva*, nel senso che per ogni $n, m \in \mathbb{N}^*$ vale

$$v_p(mn) = v_p(m) + v_p(n).$$

Teorema 1.2.4 (Euclide) *Esistono infiniti numeri primi.*

Dimostrazione. Supponiamo, per assurdo, che l'insieme dei numeri primi sia finito, e che $p_1, p_2, \ldots, p_k$ siano tutti i numeri primi distinti. Consideriamo $n = p_1 p_2 \cdots p_k$. Per il Lemma 1.2.2, il numero intero $n + 1$ ammette un divisore primo, che deve essere pertanto uno dei p_i (con $i \in \{1, 2, \ldots, k\}$). Ma allora si avrebbe che tale primo divide sia n che $n + 1$, il che è chiaramente impossibile. ■

PRIMI DI FERMAT E DI MERSENNE

Introduciamo in questa sezione due classi importanti di numeri primi, i cosiddetti *primi di Fermat* e *di Mersenne*.

Lemma 1.3.1 *Siano $a, n, m \in \mathbb{N}^*$, con $a \neq 1$. Allora*

$$(a^n - 1, a^m - 1) = a^{(n,m)} - 1 \, .$$

DIMOSTRAZIONE. Siano $d = (a^n - 1, a^m - 1)$ e $c = (n, m)$. Allora, $a^c - 1$ divide d per una ben nota e facile proprietà delle somme di serie geometriche:

$$a^n - 1 = (a^c - 1)(a^{c(n'-1)} + a^{c(n'-2)} + \dots a^c + 1),$$

se $n = cn'$. Similmente per m.

Viceversa, siano $u, -v \in \mathbb{Z}$, tali che $c = un + (-v)m = un - vm$. Allora, scambiando eventualmente n ed m, possiamo supporre u, v sono positivi. Ancora per le proprietà delle serie geometriche, abbiamo che d divide $a^{nu} - 1$ e $a^{mv} - 1$. Quindi d divide la diffrenza di questi, $a^{nu} - a^{mv} = a^{mv}(a^{nu-mv} - 1) = a^{mv}(a^c - 1)$. Poichè chiaramente d e a sono coprimi, si conclude che d divide $a^c - 1$. ∎

Proposizione 1.3.2 *Sia n un numero naturale maggiore di 1.*

1. *Sia p un primo; se $p^n + 1$ è un primo, allora $p = 2$ e $n = 2^m$ per qualche $m \in \mathbb{N}^*$.*
2. *Sia $a \in \mathbb{N}^*$; se $a^n - 1$ è un primo, allora $a = 2$ e n è un primo.*

DIMOSTRAZIONE. 1. Se $p^n + 1$ è primo allora deve essere dispari e quindi $p = 2$. Supponiamo che n abbia un divisore primo dispari q, e scriviamo $n = tq$. Allora

$$2^n + 1 = (2^t + 1)(2^{t(q-1)} - 2^{t(q-2)} + \cdots - 2^t + 1)$$

non è primo. Dunque, se $2^n + 1$ è primo, n deve essere una potenza di 2.

2. Poichè $a^n - 1 = (a - 1)(a^{n-1} + \cdots + a + 1)$, se $a^n - 1$ è primo allora $a = 2$ e, per la stessa considerazione, n è primo. ∎

I numeri primi del tipo 1. sono detti primi di Fermat. In generale, per $m \in \mathbb{N}$, l'intero $F_m = 2^{2^m} + 1$ è detto *m-esimo numero di Fermat*. I primi cinque numeri di Fermat

$$F_0 = 3, \; F_1 = 5, \; F_2 = 17, \; F_3 = 257, \; F_4 = 65537$$

sono numeri primi. Sulla base di questa osservazione, P. Fermat affermò che ogni intero di questo tipo è primo. Fu L. Eulero a scoprire come il termine successivo $F_5 = 2^{32} + 1$ non è primo (vedi Proposizione seguente). Di fatto, oltre ai cinque numeri di sopra, nessun altro primo di Fermat è stato tutt'oggi trovato, anzi, sembrerebbe che questi cinque siano gli unici numeri di Fermat ad essere primi.

Un sorprendente risultato di K. D. Boklan e J. H. Conway [6] del 2016 prova che la probabiltà che esista un ulteriore primo di Fermat è $\leq 10^{-9}$.

Proposizione 1.3.3 (Eulero) *F_5 non è un numero primo.*

DIMOSTRAZIONE. Proviamo che $641|F_5$. Infatti,

$$641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1,$$

dunque

$$\begin{aligned} 2^{32} &= 2^4 \cdot 2^{28} = (641 - 5^4) \cdot 2^{28} \\ &= 641 \cdot 2^{28} - (641 - 1)^4 \end{aligned}$$

e quindi esiste un intero positivo t tale che $2^{32} = 641t - 1$, cioè $641|2^{32} + 1 = F_5$

(si verifica che $F_5 = 641 \cdot 6700417$, e 641 e 6700417 sono numeri primi). ■

I numeri della forma $M_p = 2^p - 1$ (con p primo) sono detti *numeri di Mersenne*. Anch'essi non sono tutti primi. Il più piccolo numero di Mersenne a non essere primo è $M_{11} = 23 \cdot 89$. Anche in questo caso non è tuttora noto se esistano infiniti primi di Mersenne.

Al gennaio 2016, risultano noti 49 primi di Mersenne, il maggiore dei quali è M_p con $p = 74.207.281$, questo è anche il più grande numero primo noto [11]. Per "visualizzarlo" in base 10, occorrono 5.957 pagine con 75 cifre per riga e 50 righe per pagina. Per dettagli ed aggiornamenti: https://mersenne.org/

EQUAZIONI DIOFANTEE

Col termine di *equazione diofantea* (dal matematico alessandrino Diofanto, IV sec. d.C.) si intende genericamente una equazione algebrica le cui soluzioni sono cercate in prefissate classi di numeri; in particolare numeri interi. Allo studio della risolubilità (e delle soluzioni) di particolari equazioni diofantee è riconducibile una considerevole parte della teoria dei numeri, così come sono molteplici gli strumenti sviluppati nel corso dei secoli per affrontare simili questioni. Un esempio è la terza e ultima parte di questi appunti, dove studieremo la possibilità di rappresentare i numeri naturali come somme di quadrati.

Un primo facile caso di equazione diofantea è collegato alla Proposizione 1.1.2.

Proposizione 1.4.1 *Siano a, b ed n numeri interi (con a e b non entrambi nulli); allora l'equazione*

$$ax + by = n$$

ammette soluzioni in $\mathbb{Z}$ se e solo se (a, b) divide n. In generale, se $a_1, a_2, \ldots, a_k$ sono interi non tutti nulli, l'equazione $a_1x_1 + a_2x_2 + \cdots + a_kx_k = n$ ammette soluzioni intere se e solo se $(a_1, a_2, \ldots, a_k)$ divide n.

DIMOSTRAZIONE. Vedi [7]. ■

Un poco più complicata è la situazione in cui si richiede l'esistenza di soluzioni non negative. Anche la dimostrazione del seguente risultato è lasciata per esercizio.

Proposizione 1.4.2 *Siano $a, b \in \mathbb{N}^*$ tali che $(a, b) = 1$. Se $n \geq a(b-1)$, allora esistono interi non negativi x, y tali che $ax + by = n$.*

Un esempio assai famoso di equazione diofantea è il cosiddetto *"ultimo teorema di Fermat"*, che fu enunciato da P. de Fermat nel 1637. Fermat scrisse di averne trovato una dimostrazione "mirabile", ma di non avere lo spazio per riportarla (egli stava appunto annotando un testo di Diofanto). Dopo secoli di sforzi (inefficaci a dimostrare l'asserzione di Fermat, ma importantissimi per lo sviluppo di molte idee matematiche), l'ultimo teorema di Fermat è stato finalmente dimostrato da Andrew Wiles (e Richard Taylor) nel 1997 ([66] e [58]), utilizzando metodi assai profondi di geometria algebrica.

Teorema 1.4.3 (P. de Fermat - A. Wiles). *Sia n un numero naturale. Se $n \geq 3$, non esistono soluzioni intere dell'equazione*

$$x^n + y^n = z^n$$

tali che $xyz \neq 0$.

Il caso invece in cui l'esponente n è uguale a 2 è del tutto elementare.

Proposizione 1.4.4 *Ogni soluzione intera non banale dell'equazione*

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

si scrive nella forma $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$, dove $k, n, m \in \mathbb{N}^*$ e $(m, n) = 1$.

Dimostrazione. Si verifica facilmente che per ogni $k, n, m \in \mathbb{N}^*$, con $(n, m) = 1$, la terna $x = k(m^2 - n^2)$, $y = 2kmn$ e $z = k(m^2 + n^2)$ è una soluzione dell'equazione data (ed è detta, per ovvî motivi, *terna pitagorica*).

Viceversa, siano $x, y, z \in \mathbb{N}^*$ tali che $x^2 + y^2 = z^2$, e sia $k = (x, y)$. Osserviamo che allora $k = (x, z) = (y, z)$. Siano $a, b, c \in \mathbb{N}^*$, con

$$x = ka, \quad y = kb, \quad z = kc.$$

Allora $(a, b) = (a, c) = (b, c) = 1$ e $a^2 + b^2 = c^2$. Dunque

$$c^2 = a^2 + b^2 = (a + b)^2 - 2ab.$$

a e b non sono entrambi pari. Se fossero entrambi dispari, allora $a + b$ e c sarebbero pari, e quindi $4|c^2$ e $4|(a + b)^2$, da cui segue la contraddizione $4|2ab$. Possiamo quindi assumere che a sia dispari e b sia pari (e quindi c è dispari). Sia $d = (c + a, c - a)$; allora $2|d$, ed inoltre $d|(c + a) + (c - a) = 2c$ (analogamente $d|2a$), e dunque, poiché a e c sono coprimi, $d = 2$. Siano ora $u, v \in \mathbb{N}^*$ tali che

$$c + a = 2u \qquad c - a = 2v.$$

Per quanto appena osservato $(u, v) = 1$. Inoltre

$$b^2 = c^2 - a^2 = (c + a)(c - a) = 4uv\ ;$$

e dunque u e v sono quadrati: sia $u = m^2$ e $v = n^2$. Allora,

- $b^2 = 4m^2n^2$, e quindi $b = 2mn$, e $y = 2kmn$.
- $2c = 2(u + v) = 2(m^2 + n^2)$, e quindi $c = m^2 + n^2$, e $z = k(m^2 + n^2)$.
- $2a = 2(u - v) = 2(m^2 - n^2)$, e quindi $a = m^2 - n^2$, e $x = k(m^2 - n^2)$

il che conclude la dimostrazione. ■

L'importanza delle equazione diofantee non risiede tanto nella loro applicabilità "pratica" (anche all'interno della matematica stessa), quanto nel profluvio di idee - a volte molto sofisticate - a cui il loro studio ha dato e dà luogo (ad esempio la teoria degli anelli e degli ideali è nata da un tentativo di attaccare la congettura di Fermat), e nella suggestione esercitata da problemi i cui enunciati sono comprensibili anche ad un livello assolutamente elementare.

Un esempio curioso è la celebre congettura di Catalan, che è stata recentemente dimostrata dopo oltre 250 anni.

Nell'aprile del 2002, il matematico romeno P. Mihăilescu ha provato questa congettura (si veda [44] e [43]).

Congettura di Catalan: *Siano* $2 \leq n, m \in \mathbb{N}^*$. *La sola soluzione non banale intera dell'equazione*

$$x^n = y^m - 1$$

si ha per $x^n = 2^3$ e $y^m = 3^2$.

Ovvero i soli numeri naturali consecutivi che sono potenze non banali di numeri interi sono 8 e 9. Chi fosse interessato, oltre agli articoli segnalati in nota, può consultare il testo di P. Ribenboim "Catalan's Conjecture" [54].

APPENDICE

Dimostrazioni alternative del Teorema di Euclide

Esistono svariate dimostrazioni dell'esistenza di infiniti numeri primi. Il lettore interessato può consultare la pagina web `http://www.cut-the-knot.org/proofs/primes.shtml`, dove ne vengono riportate circa una ventina. Di seguito proponiamo due dimostrazioni tra le più note.

Una dimostrazione analitica

(Leonard Eulero, 1737)
Supponiamo che l'insieme dei primi positivi sia $\mathbb{P} = \{p_1, p_2, \dots, p_k\}$. Per il Teorema Fondamentale dell'Aritmetica (Teorema 1.2.3), abbiamo allora che

$$\mathbb{N}^* = \left\{ p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} | a_1, a_2, \dots a_k \geq 0 \right\}.$$

Ora, per ogni $s \in \mathbb{R}$, sfruttando le somme geometriche, si ha che:

$$\begin{aligned}
\sum_{n\geq 1} \frac{1}{n^s} &= \sum_{a_1,a_1,\dots,a_k\geq 0} \frac{1}{(p_1^{a_1} p_2^{a_2} \dots p_k^{a_k})^s} \\
&= \left(\sum_{a_1\geq 0} \frac{1}{(p_1^{a_1})^s} \right) \left(\sum_{a_2\geq 0} \frac{1}{(p_2^{a_2})^s} \right) \dots \left(\sum_{a_k\geq 0} \frac{1}{(p_k^{a_k})^s} \right) \\
&= \left(\sum_{a_1\geq 0} \frac{1}{(p_1^s)^{a_1}} \right) \left(\sum_{a_2\geq 0} \frac{1}{(p_2^s)^{a_2}} \right) \dots \left(\sum_{a_k\geq 0} \frac{1}{(p_k^s)^{a_k}} \right) \\
&= \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^s} \right)^{-1},
\end{aligned}$$

ovvero

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{i=1}^{k} \left(1 - \frac{1}{p_i^s} \right)^{-1},$$

che, ad esempio, per $s = 1$ fornisce una contraddizione, poiché il termine a destra è uguale a qualche numero razionale, mentre a sinistra c'è una serie divergente.

Si noti che, ripercorrendo i passaggi di sopra senza l'ipotesi d'assurdo che $\mathbb{P}$ sia finito, si prova che, per ogni $s \in \mathbb{R}_{>1}$:

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^s} \right)^{-1} \tag{1}$$

formula che riprenderemo in esame nel Capitolo 4.

Una dimostrazione topologica

(Hillel Fürstenberg, 1955, [20])
Dati $a, b \in \mathbb{Z}$, con $b \geq 1$, sia

$$N_{a,b} = \{\ a + zb \mid z \in \mathbb{Z}\ \}.$$

Definiamo una topologia in $\mathbb{Z}$, definendo gli insiemi aperti non vuoti come i sottoinsiemi A di $\mathbb{Z}$ tali che per ogni $a \in A$ esiste $b \geq 1$ tale che $N_{a,b} \subseteq A$. Si verifica facilmente che ciò definisce una topologia su $\mathbb{Z}$. In questa topologia è immediato verificare che

- ogni insieme aperto non vuoto è infinito;

- ogni insieme $N_{a,b}$ è chiuso.

La prima è ovvia dalla definizione. Per la seconda basta osservare che

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}.$$

Ora, poiché ogni numero intero diverso da $1, -1$ ha almeno un divisore primo, si ha che

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Se, per assurdo $\mathbb{P}$ fosse finito, si avrebbe che $\mathbb{Z} \setminus \{1, -1\}$ sarebbe una unione finita di insiemi chiusi, e quindi esso stesso chiuso. Di conseguenza $\{1, -1\}$ sarebbe aperto, contro quanto osservato sopra.

La serie $\sum_{p \in \mathbb{P}} \frac{1}{p}$ diverge

La seguente dimostrazione è di Paul Erdös.

Sia $p_1, p_2, p_3, \ldots$ la successione di tutti i numeri primi positivi in ordine crescente, e supponiamo per assurdo che la serie $\sum_{p \in \mathbb{P}} \frac{1}{p}$ sia convergente. Allora esiste un k tale che $\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}$; quindi, per un qualunque numero intero $N \geq 1$,

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}.$$

Dato $N \geq 1$, sia N_0 il numero di interi positivi $n \leq N$ che sono divisibili per almeno un primo p_j con $j \geq k+1$, e sia N_1 il numero di numeri di interi positivi $n \leq N$ che sono divisibili solo da primi p_t con $t \leq k$. Chiaramente, per definizione, $N_0 + N_1 = N$.

Osserviamo che il numero di interi $1 \leq n \leq N$ che sono multipli del primo p_i è al più $\frac{N}{p_i}$. Quindi

$$N_0 \leq \sum_{j \geq k+1} \frac{N}{p_j} < \frac{N}{2}.$$

Stimiamo ora N_1. Osserviamo che ogni numero naturale n può essere scritto in modo univoco come $n = a_n b_n^2$, dove b_n^2 è il massimo quadrato che divide n, e a_n è un prodotto di primi *distinti*. Ora, se i divisori primi di $n \leq N$ sono tutti compresi tra $p_1, p_2, \ldots, p_k$, si ha che il numero di possibili fattori a_n per tali interi n, è 2^k. D'altra parte, sempre per tali n, $b_n \leq \sqrt{n} \leq \sqrt{N}$, e dunque ci sono al più $\sqrt{N}$ possibilità per il fattore b_n. In conclusione,

$$N_1 \leq 2^k \sqrt{N}.$$

Poiché $N = N_0 + N_1$ vale per ogni $N \geq 1$, si ha

$$N < \frac{N}{2} + 2^k\sqrt{N}.$$

Ma tale relazione è falsa per $N \geq 2^{2k+2}$, e questa contraddizione dimostra che la serie $\sum_{p\in\mathbb{P}} \frac{1}{p}$ deve essere divergente.

L'equazione diofantea $x^2 + 2 = y^3$.

Proviamo che 26 è l'unico numero naturale successivo ad un quadrato (25) e precedente ad un cubo (27); ovvero:

Proposizione *L'equazione diofantea*

$$x^2 + 2 = y^3 \tag{2}$$

ammette un'unica soluzione in $\mathbb{N}^2$*:* $(x_0, y_0) = (5, 3)$.

Dimostrazione. Incominciamo con l'osservare che una soluzione (x_0, y_0) dell'equazione (2) è costituita da coppie di numeri entrambi dispari (se infatti x_0 fosse pari, allora anche y_0^3 lo è e, conseguentemente anche y_0, ma ciò implicherebbe che $x_0^2 \equiv 2 \pmod 4$, il che è assurdo).

Osserviamo ora che l'equazione (2) si fattorizza nel PID $\mathbb{Z}[i\sqrt{2}]$ come

$$(x + i\sqrt{2})(x - i\sqrt{2}) = y^3. \tag{3}$$

Sia $d = (x_0 + i\sqrt{2}, x_0 - i\sqrt{2}) \in \mathbb{Z}[i\sqrt{2}]$, e proviamo che d è associato ad 1. Detto α un eventuale fattore irriducibile di d, poiché $i\sqrt{2}$ è irriducibile e

$$\alpha | x_0 + i\sqrt{2} - (x_0 - i\sqrt{2}) = -(i\sqrt{2})^3$$

avremmo che α è associato a $i\sqrt{2}$. Pertanto $i\sqrt{2}|(x_0 + i\sqrt{2})$ e conseguentemente $i\sqrt{2}|x_0$, il che però è assurdo, perché altrimenti avremmo che $N(i\sqrt{2}) = 2$ divide x_0^2 in $\mathbb{Z}$, mentre x_0 è dispari. Ne segue che $x_0 + i\sqrt{2}$ e $x_0 - i\sqrt{2}$ sono due elementi coprimi in $\mathbb{Z}[i\sqrt{2}]$. Da (3) segue allora che $x_0 + i\sqrt{2}$ è un cubo di $\mathbb{Z}[i\sqrt{2}]$, ovvero esiste $z = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ tale che

$$x_0 + i\sqrt{2} = z^3 = (a + ib\sqrt{2})^3. \tag{4}$$

separando parte reale e parte immaginaria tale equazione è equivalente al sistema

$$\begin{cases} x_0 = a^3 - 6ab^2 \\ 1 = b(3a^2 - 2b^2) \end{cases}$$

il quale è facile vedere che ammette come uniche soluzioni intere $(a, b) = (\pm 1, 1)$. Abbiamo pertanto che $(x_0, y_0) = (5, 3)$ è l'unica coppia di numeri naturali che soddisfa l'equazione (2). ∎

Un test di primalità per i numeri di Mersenne

Descriviamo un test di primalità per numeri di Mersenne che fu trovato da D. H. Lehmer nel 1930, ed è tuttora utilizzato nelle computazioni. Esso è una applicazione di una tecnica più generale, quella delle *sequenze di Lucas* (si veda l'interessante testo di P. Ribenboim, *The Book of Prime Number Records*, [55]).

Cominciamo col definire induttivamente una successione $(S_i)_{i\in\mathbb{N}^*}$ di numeri naturali, ponendo

$$S_1 = 4 \qquad \text{e} \qquad S_{n+1} = S_n^2 - 2\ .$$

Denotiamo l'n-esimo numero di Mersenne con $M_n = 2^n - 1$.

Test di Lucas-Lehmer. Sia $n \geq 3$. Allora M_n *è primo se e solo se* $S_{n-1} \equiv 0\,(mod\, M_n)$.

Dimostrazione. In questa appendice ci limitiamo a provare la sufficienza (che è poi quella che interessa maggiormente), ovvero: se M_n divide S_{n-1}, allora M_n è un numero primo. Nell'Appendice del Capitolo 3 proveremo invece che la condizione è anche necessaria.

Incominciamo con l'osservare che la sequenza $\{S_n\}_n$ è costituita da soli numeri interi e pertanto ha senso considerare la riduzione di ogni S_n modulo un arbitrario primo q; indicheremo tale riduzione semplicemente con $\overline{S_n}$.

Supponiamo per assurdo, che M_n non sia primo e prendiamo q primo che divide M_n e tale che $q \leq \sqrt{M_n}$. Poniamo $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ il campo con q elementi e prendiamo una radice α del polinomio $x^2 - 3 \in \mathbb{F}_q[x]$. Sia inoltre $\mathbb{E}$ l'estensione $\mathbb{E} = \mathbb{F}_q[\alpha]$. Poiché $\left|\mathbb{E} : \mathbb{F}_q\right| \leq 2$, abbiamo che $\mathbb{E}$ è un campo finito d'ordine al più q^2. Detto $G = \mathbb{E}^*$, il gruppo moltiplicativo dei suoi elementi non nulli, allora $|G| \leq q^2 - 1$.

Siano $u = \overline{2} + \alpha$ e $v = \overline{2} - \alpha$. Allora u, v sono due elementi di $\mathbb{E}^*$ e vale $uv = \overline{1}$. Inoltre per ogni naturale $n \geq 2$,

$$\overline{S_n} = u^{2^{n-1}} + v^{2^{n-1}}$$

(lo si verifichi per induzione). Quindi, se M_n divide S_{n-1}, allora anche $q|S_{n-1}$, ovvero $\overline{S_{n-1}} = \overline{0}$, cioè

$$u^{2^{n-2}} + v^{2^{n-2}} = \overline{0}.$$

Moltiplicando per $u^{2^{n-2}}$ e sottraendo $\overline{1}$, si ha

$$u^{2^{n-1}} = -\overline{1}\ , \tag{5}$$

ed elevando al quadrato,

$$u^{2^n} = \overline{1}\ . \tag{6}$$

Ciò ci dice esattamente che l'elemento u del gruppo G ha proprio ordine 2^n. Pertanto

$$2^n \leq |G| \leq q^2 - 1 < M_n = 2^n - 1$$

e questa è una contraddizione. ■

ESERCIZI

Esercizio 1.1 *Siano a, b numeri interi, con $b \geq 1$. Si provi che esistono unici interi t, s tali che $a = bt + s$ e $-\frac{b}{2} < s \leq \frac{b}{2}$.*

Esercizio 1.2 *Siano $a_1, a_2, \ldots, a_s$ numeri interi non tutti nulli. Si dimostri che $(a_1, a_2, \ldots, a_s) = 1$ se e solo se esistono interi $x_1, x_2, \ldots, x_s$ tali che*

$$a_1x_1 + a_2x_2 + \cdots + a_sx_s = 1.$$

Esercizio 1.3 *Provare che v_p è completamente additiva.*

Esercizio 1.4 *Siano $a, n \in \mathbb{N}^*$. Provare che $\sqrt[n]{a} \in \mathbb{Q}$ se e solo se $\sqrt[n]{a} \in \mathbb{N}$.*

Esercizio 1.5 *Siano $a, b \in \mathbb{N}^*$ tali che $\sqrt{a} + \sqrt{b} \in \mathbb{Q}$. Provare che a e b sono quadrati in $\mathbb{N}$.*

Esercizio 1.6 *Sia $1 < n \in \mathbb{N}$. Si provi che*

$$u = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

non è un numero intero.

Esercizio 1.7 *Sia $1 < n \in \mathbb{N}$. Si provi che*

$$v = 1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$$

non è un numero intero.

Esercizio 1.8 *Per $n \in \mathbb{N}$, sia $F_n = 2^{2^n} + 1$. Si provi che se $n \neq m$ allora $(F_n, F_m) = 1$ (si osservi che, se $n < m$, allora F_n divide $F_m - 2$).*

Esercizio 1.9 *Sia $n \in \mathbb{N}$. Si provi che n, $n+2$, $n+4$ sono primi se e solo se $n = 3$. Si dimostri che la stessa conclusione vale assumendo che n, $n+4$, $n+8$ siano primi.*

Esercizio 1.10 *Si provi che l'insieme $S = \{\log p | p \in \mathbb{P}\}$ consiste di numeri reali che sono linearmente indipendenti su $\mathbb{Q}$.*

Esercizio 1.11 *Sia $f(x) \in \mathbb{Z}[x]$ un polinomio non costante. Allora l'insieme*

$$T = \{p \in \mathbb{P} | p | f(n) \text{ per qualche } n \in \mathbb{N}^*\}$$

è infinito.

Esercizio 1.12 *Siano $n, k \in \mathbb{N}$, con $k \geq 3$. Si provi che se $n,\ n+k,\ n+2k, \ldots, n+(k-2)k$ sono tutti numeri primi, allora $n = k-1$.*

Esercizio 1.13 *Sia $n \in \mathbb{N}^*$ e siano a, b interi non nulli tali che $(a,b)|n$. Sia (x_o, y_o) una soluzione dell'equazione diofantea $ax + by = n$. Si provi che l'insieme delle soluzioni di tale equazione è*

$$\left\{ \left(x_o + t\frac{b}{(a,b)},\ y_o - t\frac{a}{(a,b)} \right) \ \middle|\ t \in \mathbb{Z} \right\}.$$

Esercizio 1.14 *Provare che l'equazione $x^4 + y^4 = z^2$ non ha soluzioni intere non banali (cioè tali che $xyz \neq 0$). In particolare, quindi, il Teorema di Fermat è vero per l'esponente $n = 4$.*

Esercizio 1.15 *Si provi che le sole soluzioni intere, con $x \geq 2$, dell'equazione*

$$(x-1)! = x^y - 1$$

sono $(x,y) \in \{(2,1), (3,1), (5,2)\}$.

Esercizio 1.16 *La successione di Fibonacci è definita da:*

$$u_0 = 0,\ u_1 = 1,\ \text{ e } \ u_{n+2} = u_{n+1} + u_n$$

(i primi termini di essa sono $0, 1, 1, 2, 3, 5, 8, 13, 21, 33 \ldots$). Provare i seguenti fatti.

1) *Se $x = (1+\sqrt{5})/2$ e $y = (1-\sqrt{5})/2$, allora $u_n\sqrt{5} = x^n - y^n$ (x, y sono le radici reali dell'equazione $t^2 - t - 1$);*
2) *$(u_n, u_{n+1}) = 1$;*
3) *$u_{m+n} = u_{n-1}u_m + u_n u_{m+1}$;*
4) *se $r \in \mathbb{N}^*$, allora u_n divide u_{nr};*
5) *se $(m,n) = d$, allora $(u_m, u_n) = u_d$.*

Esercizio 1.17 *Sia $n \in \mathbb{N}^*$. Si provi che l'equazione diofantea $x + 2xy + y = n$ ha soluzioni non banali (cioè $x \neq 0 \neq y$) se e solo se $2n+1$ non è un numero primo.*

"Que- sta
tomba rac- chiude al suo
interno Diofanto. Oh, meraviglia! Essa
dice ad arte quanto egli ha vissuto. Dio
gli accordò il sesto della sua vita
per l'infanzia e aggiunse un
dodicesimo perché le sue guance
si coprissero della peluria dell'a-
dolescenza. Per un settimo
fece eziandio brillare per
lui la fiamma d'Imene, e
dopo cinque anni di matri-
monio gli die- de un figlio:
Ahimè! unico ed infelice
bambino, al quale la Parca
non concesse di vedere che
la metà della vita di suo
padre. Du- rante quattro
anni ancora, consolando il
suo dolore con lo studio delle
cifre, Diofanto raggiunse infine
il termine della sua vi-
ta." *([21])*

2 CONGRUENZE

Per questo Capitolo vale quanto già detto all'inizio del Capitolo 1. Dopo un rapido richiamo dei fondamenti algebrici della teoria delle congruenze, ci soffermeremo sulle congruenze modulo un numero composto, dimostrando un importante Lemma di Hensel.

PROPRIETÀ GENERALI

Sia $n \in \mathbb{N}^*$. Due interi a e b si dicono *congrui modulo* n se n divide $a - b$. In tal caso si scrive

$$a \equiv b \ (mod\, n).$$

Per ogni $n \in \mathbb{N}^*$, la congruenza modulo n è una relazione d'equivalenza su $\mathbb{Z}$. Per ogni $a \in \mathbb{Z}$ la classe di equivalenza di a (detta *classe di congruenza* di a modulo n) è l'insieme

$$a + n\mathbb{Z} = \{\ a + nz \mid z \in \mathbb{Z}\ \}$$

che, se non ci sono ambiguità sul valore di n, in questo Capitolo, indicheremo di solito anche con la scrittura $\overline{a}$.

L'insieme di tutte la classi di congruenza modulo n (ovvero l'insieme quoziente) si denota con

$$\frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Usando la divisione euclidea si verifica facilmente che ogni intero a è congruo modulo n al resto della divisione di a per n. Da ciò segue subito che il quoziente $\mathbb{Z}/n\mathbb{Z}$ contiene esattamente n elementi, e che gli interi $0, 1, 2, \ldots, n-1$ costituiscono un insieme di rappresentanti delle classi di congruenza modulo n; ovvero

$$\begin{aligned}\frac{\mathbb{Z}}{n\mathbb{Z}} &= \{\ 0 + n\mathbb{Z},\ 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\ \} \\ &= \{\overline{0},\ \overline{1}, \ldots, \overline{n-1}\}.\end{aligned}$$

Inoltre, l'insieme $n\mathbb{Z}$ è un ideale dell'anello $\mathbb{Z}$, e quindi il quoziente $\mathbb{Z}/n\mathbb{Z}$ è un anello rispetto alle operazioni (che si verificano essere ben definite):

$$\overline{a} + \overline{b} = \overline{a + b}$$

$$\overline{a} \cdot \overline{b} = \overline{ab}\ ;$$

in cui lo zero è $\overline{0}$, e l'elemento identico è $\overline{1}$.

Indichiamo con

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

l'insieme degli elementi *invertibili* dell'anello $\mathbb{Z}/n\mathbb{Z}$, ovvero l'insieme delle classi di congruenza $\overline{a}$ modulo n per cui esiste $b \in \mathbb{Z}$ con $\overline{a}\overline{b} = \overline{1}$. Questo insieme è un gruppo rispetto alla moltiplicazione in $\mathbb{Z}/n\mathbb{Z}$. I suoi elementi sono facilmente descritti.

Lemma 2.1.1 *Sia $2 \leq n \in \mathbb{N}$, e sia $a \in \mathbb{Z}$. Allora $\overline{a} = a + n\mathbb{Z}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se e solo se $(a, n) = 1$.*

Dimostrazione. Dopo aver osservato che $\overline{a}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se e solo se esiste un $b \in \mathbb{Z}$ tale che $ab \equiv 1\,(mod\, n)$; cioè se e solo se esiste anche un $c \in \mathbb{Z}$ per cui $ab = 1 + cn$, l'enunciato segue facilmente dalla Proposizione 1.1.2. ■

Poiché possiamo scegliere come insieme di rappresentanti di $\mathbb{Z}/n\mathbb{Z}$ gli elementi $0, 1, 2, \ldots, n-1$, una conseguenza immediata del Lemma 2.1.1 è che il numero di elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$ è uguale al numero di interi compresi tra 1 e n che sono coprimi con n. Tale numero si denota con $\phi(n)$. La funzione ϕ viene chiamata *funzione (totient) di Eulero* e sarà trattata in dettaglio nel Capitolo 4. Abbiamo pertanto che

$$\left|\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*\right| = \phi(n). \tag{7}$$

Esempio 2.1.1 Gli interi $1 \leq a \leq 12$ che sono coprimi con 12, sono $1, 5, 7, 11$. Quindi $(\mathbb{Z}/12\mathbb{Z})^* = \{\ \overline{1}, \overline{5}, \overline{7}, \overline{11}\ \}$.

Ricordiamo ora che se G è un gruppo moltiplicativo finito di ordine k, allora per ogni $g \in G$, risulta $g^k = 1_G$. Ora, $(\mathbb{Z}/n\mathbb{Z})^*$ è un gruppo moltiplicativo di ordine $\phi(n)$, e quindi, per ogni $\overline{a}$ in $(\mathbb{Z}/n\mathbb{Z})^*$, si ha $\overline{a^{\phi(n)}} = \overline{a}^{\phi(n)} = \overline{1}$, ovvero

$$a^{\phi(n)} \equiv 1\ (mod\, n).$$

Siccome gli elementi di $(\mathbb{Z}/n\mathbb{Z})^*$ sono le classi di congruenza degli interi a coprimi con n, ricaviamo il seguente

Teorema 2.1.2 (L. Eulero) *Sia $n \in \mathbb{N}^*$, e sia a un numero intero tale che $(n, a) = 1$. Allora n divide $a^{\phi(n)} - 1$, ovvero*

$$a^{\phi(n)} \equiv 1\,(mod\, n).$$

Il caso particolare in cui $n = p$ è un numero primo, è il cosiddetto "piccolo teorema di Fermat".

Corollario 2.1.3 (P. de Fermat) *Sia p un numero primo, e sia $a \in \mathbb{Z}$. Se p non divide a,*

$$a^{p-1} \equiv 1 \,(mod\, p).$$

In ogni caso, $a^p \equiv a \,(mod\, p)$.

Infatti, è possibile rendere del tutto esplicita la struttura algebrica del gruppo degli invertibili di $\mathbb{Z}/m\mathbb{Z}$. Per il momento, ci limitiamo al caso in cui $m = p$ è un numero primo. In tal caso ogni elemento non nullo di $\mathbb{Z}/p\mathbb{Z}$ è invertibile, e quindi $\mathbb{Z}/p\mathbb{Z}$ è un *campo*.

Lemma 2.1.4 *Per ogni numero naturale $n \geq 1$,*

$$\sum_{m|n} \phi(m) = n.$$

Dimostrazione. Poniamo $A = \{1, 2, \ldots, n\}$ e $\Delta_n = \{1 \leq m \leq n | m \text{ divide } n\}$. Definiamo una applicazione $c : A \to \Delta_n$ ponendo, per ogni $a \in A$, $c(a) = (a, n)$. Allora, chiaramente

$$n = \sum_{m|n} |c^{-1}(m)|.$$

D'altra parte, per ogni $m \in \Delta_n$,

$$\begin{aligned} |c^{-1}(m)| &= |\{a \in A \,;\, (a, n) = m\}| \\ &= |\{1 \leq a' \leq n/m \,;\, (a', n/m) = 1\}| \\ &= \phi(n/m). \end{aligned}$$

Dunque

$$\sum_{m|n} \phi(m) = \sum_{m|n} \phi(n/m) = \sum_{m|n} |c^{-1}(m)| = n$$

e la dimostrazione è completata. ∎

Teorema 2.1.5 *Sia p un numero primo. Allora $(\mathbb{Z}/p\mathbb{Z})^*$ è un gruppo (moltiplicativo) ciclico di ordine $p - 1$.*

Dimostrazione. Poniamo $G = (\mathbb{Z}/p\mathbb{Z})^*$. Allora $|G| = p - 1$. Per un fatto già ricordato precedentemente, ogni elemento di G ha ordine che divide $p - 1$. Per ogni divisore m di $p - 1$, denotiamo con $\psi(m)$ il numero di elementi di G che hanno ordine esattamente m. Allora

$$\sum_{m|p-1} \psi(m) = |G| = p - 1.$$

Se $\psi(m) \neq 0$, esiste un elemento a di G tale che il sottogruppo ciclico $\langle a \rangle$ ha ordine m. Ogni elemento $g \in \langle a \rangle$ è tale che $g^m = 1$, e quindi è una radice in $\mathbb{Z}/p\mathbb{Z}$ del polinomio $x^m - 1$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un campo,

il numero di tali elementi è al più m; quindi $\langle a \rangle$ è l'insieme di tutte le radici di $x^m - 1$.

Ora, $\langle a \rangle$ ammette $\phi(m)$ generatori distinti, tutti di ordine m.

In conclusione, per ogni $m|p-1$,

$$\psi(m) = 0 \text{ oppure } \psi(m) \leq \phi(m).$$

Applicando ciò, ed il Lemma 2.1.4, si ottiene

$$p - 1 = \sum_{m|p-1} \psi(m) \leq \sum_{m|p-1} \phi(m) = p - 1.$$

Dunque, deve essere $\psi(m) = \phi(m)$ per ogni divisore m di $p-1$. In particolare, $\psi(p-1) \neq 0$, e quindi esiste un elemento in G di ordine $p-1$. Il gruppo ciclico generato da tale elemento è tutto G. ∎

Un generatore del gruppo ciclico $(\mathbb{Z}/p\mathbb{Z})^*$ viene chiamato *elemento primitivo* di $(\mathbb{Z}/p\mathbb{Z})$.

Proviamo ora un risultato classico interessante.

Teorema 2.1.6 (Wilson) *Sia p un numero primo. Allora*

$$(p-1)! \equiv -1 \, (mod\, p).$$

DIMOSTRAZIONE. Se $p = 2$ l'affermazione è banale. Sia $p > 2$. Osserviamo che $\overline{1}, \overline{2}, \overline{3}, \ldots, \overline{p-1}$ sono tutti gli elementi non nulli del campo $\mathbb{Z}/p\mathbb{Z}$. Per il piccolo Teorema di Fermat (Corollario 2.1.3) queste sono tutte e sole le radici nel campo $\mathbb{Z}/p\mathbb{Z}$ del polinomio $x^{p-1} - \overline{1}$. Quindi

$$(x - \overline{1})(x - \overline{2}) \ldots (x - \overline{p-1}) = x^{p-1} - \overline{1}.$$

Dal confronto dei termini noti, si ottiene

$$\overline{(p-1)!} = \overline{1} \cdot \overline{2} \cdots \overline{p-1} = -\overline{1} = \overline{-1}$$

che significa proprio $(p-1)! \equiv -1 \, (mod\, p)$. ∎

(Per una diversa dimostrazione si veda l'esercizio 2.5)

CONGRUENZE

Sia $f(x)$ un polinomio a coefficienti interi, e sia $n \in \mathbb{N}^*$. Siamo interessati a stabilire la risolubilità (ed eventualmente a determinare le "soluzioni") di congruenze del tipo

$$f(x) \equiv 0 \pmod{n}. \tag{8}$$

Con "soluzione" di una tale congruenza si intende ovviamente un intero $a \in \mathbb{Z}$ tale che $f(a) \equiv 0 \pmod{n}$. Osserviamo subito che, poiché $f(x)$ ha coefficienti interi, se a è una soluzione di (8), e b è un altro intero congruo ad $a \pmod{n}$, allora anche b è una soluzione di (8). Dunque, se esistono, le soluzioni di (8) sono infinite, ma corrispondono tuttavia ad un numero finito di classi di congruenza. Quindi potremo riferirci al *numero di soluzioni* di una congruenza del tipo (8), intendendo con ciò il numero di classi di congruenza distinte i cui elementi sono soluzioni vere e proprie (in altri termini, il numero di interi $0 \leq a \leq n-1$ tali che $f(a) \equiv 0 \pmod{n}$).

Una maniera spesso conveniente di trattare una congruenza del tipo (8) è quella di interpretarla come una "equazione" su un opportuno anello. Infatti, posto $A = \mathbb{Z}/n\mathbb{Z}$, al polinomio intero $f(x) = a_o + a_1 x + \cdots + a_k x^k$ possiamo univocamente associare la sua *riduzione modulo* n, $\overline{f}(x) = \overline{a_o} + \overline{a_1} x + \cdots + \overline{a_k} x^k$ (dove, per ogni $1 \leq i \leq k$, $\overline{a_i} = a_i + n\mathbb{Z}$), che è un polinomio in $A[x]$. È allora immediato osservare che se a è una soluzione della congruenza (8), allora $\overline{a} = a + n\mathbb{Z}$ è una radice in A del polinomio ridotto $\overline{f}(x)$ (ovvero, in termini più impropri ma usuali, è una "soluzione" in A dell'equazione $\overline{f}(x) = \overline{0}$). Viceversa, se $\overline{a}$ è una radice in A del polinomio ridotto $\overline{f}(x)$, allora ogni intero appartenente alla classe di congruenza $\overline{a}$ (cioè ogni $b \equiv a \pmod{n}$) è una soluzione della congruenza (8).

Questo approccio risulta particolarmente adatto quando il modulo n è un numero primo, poiché in tal caso $\mathbb{Z}/n\mathbb{Z}$ è un campo, e la teoria delle radici di un polinomio a coefficienti su un campo è molto più agevole. Nelle sezioni successive vedremo come sia sempre possibile, mediante il teorema cinese del resto (Teorema 2.3.3) ed il lemma di Hensel (Lemma 2.4.4), ricondursi a questa situazione; per il momento vediamo alcune osservazioni di carattere generale.

Il caso in cui $f(x)$ è lineare (cioè $f(x) = ax + b$, con $a, b \in \mathbb{Z}$) è relativamente semplice, ed è sostanzialmente contenuto nella Proposizione 1.4.1.

Proposizione 2.2.1 *Sia $1 \leq n \in \mathbb{N}$, e siano $a, b \in \mathbb{Z}$. La congruenza $ax \equiv b \pmod{n}$ ammette soluzioni se e solo se $(a, n) | b$.*

Corollario 2.2.2 *Siano p un numero primo e $a, b \in \mathbb{Z}$. Allora la congruenza $ax \equiv b \pmod{p}$ ammette soluzioni se e solo se $p | b$ oppure $p \nmid a$, e nel secondo caso la soluzione è una sola.*

Per risolvere congruenze di questo tipo si può adoperare l'algoritmo di Euclide. Supponiamo, ad esempio, di voler risolvere la congruenza

$$57x \equiv 21 \pmod{12}.$$

Si trova, $57 = 4 \cdot 12 + 9$, e $12 = 1 \cdot 9 + 3$; dunque, andando a ritroso,

$$(57, 6) = 3 = (-1) \cdot 57 + 5 \cdot 12.$$

Ora $21 = 3 \cdot 7$ e pertanto si ha

$$21 = 7 \cdot 3 = 7 \cdot ((-1) \cdot 57 + 5 \cdot 12) = 57 \cdot (-7) + 12 \cdot 35.$$

Dunque -7 è una soluzione cercata, ed ogni intero ad essa congruo modulo 12 è tale. Ad esempio, 5 è una soluzione. Le altre eventuali soluzioni (si intende, come abbiamo spiegato sopra, modulo 12) si possono determinare mediante una applicazione dell'esercizio 1.13 del Capitolo 1 (vedi esercizio seguente). Esse sono date da

$$5 + t\frac{12}{(57, 12)} = 5 + t \cdot 4$$

con $0 \leq t < 3$, ovvero sono 5, $5 + 4 = 9$ e $5 + 8 = 13$. In conclusione, le soluzioni della congruenza di partenza sono tutti e soli i numeri interi a tali che $a \equiv 1, 5, 9 \pmod{12}$.

Vediamo ora come il Corollario 2.2.2 si può agevolmente interpretare mediante la riduzione modulo p. Siano quindi p un numero primo ed $a, b \in \mathbb{Z}$. Risolvere la congruenza $ax \equiv b \pmod{p}$ equivale a trovare le radici nel campo $\mathbb{Z}/p\mathbb{Z}$ del polinomio $\overline{a}x - \overline{b}$. Supponiamo che p non divida a. Allora la classe di congruenza $\overline{a} = a + p\mathbb{Z}$ è un elemento invertibile del campo $\mathbb{Z}/p\mathbb{Z}$, dunque ammette un inverso $\overline{a}^{-1}$, e $\overline{b}\overline{a}^{-1}$ è un elemento di $\mathbb{Z}/p\mathbb{Z}$ (cioè una classe di congruennza modulo p) che è una radice del polinomio $\overline{a}x - \overline{b}$. Se $c \in \mathbb{Z}$ è un qualsiasi elemento della classe $\overline{ba^{-1}}$, allora $\overline{c} = \overline{b}\overline{a}^{-1}$, e quindi $\overline{ac} = \overline{b}$. Dunque c è una soluzione della congruenza $ax \equiv b \pmod{p}$. L'unicità degli inversi in un campo (ovvero il fatto che $\overline{a}x - \overline{b}$ abbia un'unica radice) assicura che la congruenza ha una sola soluzione.

In linea di principio, per ogni congruenza del tipo che stiamo considerando è possibile determinare le eventuali soluzioni: se n è il modulo e $f(x)$ il polinomio intero, "basta" valutare $f(x)$ per tutti gli interi compresi tra 0 e $n - 1$. Tuttavia, sia dal punto di vista astratto sia da quello pratico, ciò è tutt'altro che soddisfacente. Da un lato si vorrebbero risultati generali che garantiscano la risolubilità (e possibilmente la determinazione delle soluzioni, come la Proposizione 2.2.1) di ampie classi di congruenze, senza dover "fare i conti", dall'altro la computazione diretta si rivela presto estremamente laboriosa. Questo vale già per le congruenze di secondo grado, che saranno l'argomento del prossimo capitolo, centrato sul famoso teorema di reciprocità quadratica di Gauss (Teorema 3.2.1). Per il momento vediamo un altro risultato di esistenza, che nella sostanza ci dice, dati un primo p ed un intero positivo n, quante radice n-esime dell'unità sono contenute nel campo $\mathbb{Z}/p\mathbb{Z}$. Ne diamo due dimostrazioni, la seconda della quale adotta un approccio gruppale.

Proposizione 2.2.3 *Sia p un primo, $n \in \mathbb{N}$ e $d = (n, p - 1)$. Allora la soluzioni della congruenza*

$$x^n \equiv 1 \pmod{p}$$

coincidono con quelle di $x^d \equiv 1 \pmod{p}$. *Inoltre queste sono esattamente* d *classi.*

DIMOSTRAZIONE. Osserviamo preliminarmente che le soluzioni della congruenza $x^n \equiv 1 \pmod{p}$ sono tutte e sole quelle della congruenza $x^d \equiv 1 \pmod{p}$. Infatti, è chiaro che le soluzioni della seconda sono anche soluzioni della prima. Viceversa sia $a \in \mathbb{Z}$ tale che $a^n \equiv 1 \pmod{p}$, e siano $u, v \in \mathbb{Z}$ con $d = nu + (p-1)v$. Poiché p non divide a, applicando il piccolo teorema di Fermat (Corollario 2.1.3) si ha

$$a^d = a^{nu+(p-1)v} = a^{nu}a^{(p-1)v} \equiv (a^n)^u(a^{p-1})^v \equiv 1 \pmod{p}$$

(osserviamo che in questo calcolo abbiamo usato il fatto che, essendo $\mathbb{Z}/p\mathbb{Z}$ un campo ha senso elevare con esponente negativo - si veda anche l'esercizio 2.14). Quindi a è soluzione di $x^d \equiv 1 \pmod{p}$.

Mostriamo ora che la congruenza $x^d \equiv 1 \pmod{p}$ (con d un divisore di $p-1$) ha esattamente d soluzioni.

(Prima dimostrazione) Consideriamo il polinomio intero $f(x) = x^d - 1$. Allora a è soluzione della congruenza di sopra se e solo se $\overline{a} = a + p\mathbb{Z}$ è radice del polinomio (ridotto modulo p) $\overline{f}(x) = x^d - \overline{1} \in (\mathbb{Z}/p\mathbb{Z})[x]$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un campo, tale polinomio ammette al più d radici. Sia ora $e \in \mathbb{N}$ tale che $p - 1 = de$. Allora

$$x^{p-1} - \overline{1} = (x^d - \overline{1})\overline{g}(x)$$

dove $g(x) = x^{d(e-1)} + \cdots + x^d + 1$. Ora, per il Corollario 2.1.3, $x^{p-1} - \overline{1}$ ha esattamente $p-1$ soluzioni in $\mathbb{Z}/p\mathbb{Z}$. Poiché le soluzioni di $\overline{g}(x) = \overline{0}$ sono al piú $d(e-1) = p-1-d$, ne segue che $x^d - \overline{1}$ ha almeno d radici. Dunque $x^d - \overline{1} = \overline{0}$ ha esattamente d soluzioni in $\mathbb{Z}/p\mathbb{Z}$, e questo prova l'asserto.

(Seconda dimostrazione) Sappiamo che il gruppo moltiplicativo $\mathbb{F}^* = (\mathbb{Z}/p\mathbb{Z})^*$ è ciclico di ordine $p-1$. Sia $\overline{u}$ un suo generatore, e sia $p - 1 = de$. Allora $\langle \overline{u}^e \rangle$ è un sottogruppo di $\mathbb{F}^*$ di ordine esattamente d. Se $\overline{a} \in \langle \overline{u}^e \rangle$; allora $\overline{a}^d = \overline{1}$, cioè $\overline{a}$ è radice di $x^d - \overline{1}$. Poiché $x^d - \overline{1}$ ha al più d radici, si conclude che $\langle \overline{u}^e \rangle$ è l'insieme di esse e, siccome $\langle \overline{u}^e \rangle$ contiene esattamente d elementi, la dimostrazione è conclusa. ∎

Notiamo come la (seconda) dimostrazione della Proposizione 2.2.3, oltre a determinare il numero di soluzioni della congruenza, sembra anche fornire un metodo per trovarle. Da un punto di vista computazionale, questo è abbastanza apparente: la ragione è che non è noto alcun algoritmo efficiente che, dato un primo p, trovi un generatore del gruppo moltiplicativo $(\mathbb{Z}/p\mathbb{Z})^*$, ovvero un elemento primitivo di $\mathbb{Z}/p\mathbb{Z}$.

Il solo caso veramente facile è quando $n = 2$.

Lemma 2.2.4 *Sia p un numero primo dispari. Allora le radici in $\mathbb{Z}/p\mathbb{Z}$ di $x^2 - \overline{1}$ sono $\overline{1}$ e $-\overline{1}$. Equivalentemente, se $a \in \mathbb{Z}$ si ha $a^2 \equiv 1 \pmod{p}$ se e solo se $a \equiv \pm 1 \pmod{p}$.*

Sia $n \geq 1$ e $a \in \mathbb{Z}$ tale che $(a, n) = 1$. Allora $\overline{a} = a + n\mathbb{Z}$ è un invertibile nell'anello $\mathbb{Z}/n\mathbb{Z}$, e quindi è un elemento del gruppo moltiplicativo $(\mathbb{Z}/n\mathbb{Z})^*$. L'ordine di $\overline{a}$ in tale gruppo si dice *ordine di a modulo n*. Esso è il minimo intero $\zeta \geq 1$ tale che $a^\zeta \equiv 1 \pmod{n}$. Per il Teorema di Lagrange (vedi [8]), l'ordine di a modulo n è un divisore dell'ordine del gruppo $(\mathbb{Z}/n\mathbb{Z})^*$, pertanto è un divisore di $\phi(n)$.

È chiaro che l'ordine di un intero modulo n dipende solo dalla sua classe di congruenza modulo n. Calcoliamo, ad esempio, l'ordine di 54 modulo 7. Posssiamo sostituire 54 con 5, dato che sono congrui modulo 7. Inoltre $\phi(7) = 6$, e quindi è sufficiente considerare come esponenti i divisori di 6. Poiché $5^2 = 25 \equiv 4 \pmod{7}$, e $5^3 = 125 \equiv 6 \pmod{7}$, deduciamo che l'ordine di 5 (e quindi di 54) modulo 7 è 6.

IL TEOREMA CINESE DEL RESTO

Il Teorema cinese del resto (così chiamato perché nella sostanza appare noto ad antichi matematici cinesi - come Sun Tze, vissuto nel I secolo d.C.) consente di ridurre le congruenze al caso in cui il modulo sia una potenza di un numero primo. Iniziamo vedendone una formulazione "astratta".

Teorema 2.3.1 *Siano $m_1, m_2, \ldots, m_s$ elementi di $\mathbb{N}^*$ a due a due coprimi, e sia $n = m_1 m_2 \cdots m_s$. Allora l'applicazione definita da, per ogni $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$,*

$$a + n\mathbb{Z} \;\mapsto\; (a + m_1\mathbb{Z},\, a + m_2\mathbb{Z},\, \ldots,\, a + m_s\mathbb{Z})$$

è ben definita e stabilisce un isomorfismo di anelli:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_s\mathbb{Z}}.$$

Dimostrazione. Con le notazioni dell'enunciato, denotiamo con f l'applicazione data. Verifichiamo che f è ben definita. Siano $a, b \in \mathbb{Z}$ tali che $a + n\mathbb{Z} = b + n\mathbb{Z}$. Allora $n|a - b$, e quindi per ogni $i = 1, 2, \ldots, s$, $m_i|a - b$, e di conseguenza $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$, provando che secondo la definizione $f(a + n\mathbb{Z}) = f(b + n\mathbb{Z})$.

Il fatto che f sia un omomorfismo d'anelli segue immediatamente dalla definizione degli anelli quoziente $\mathbb{Z}/k\mathbb{Z}$.

Proviamo che f è iniettiva. Siano $a + n\mathbb{Z}, b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, tali che $f(a + n\mathbb{Z}) = f(b + n\mathbb{Z})$. Allora, per ogni $i = 1, 2, \ldots, s$, $a + m_i\mathbb{Z} = b + m_i\mathbb{Z}$; e quindi m_i divide $a - b$. Poiché gli interi m_i sono a due a

due coprimi, da ciò segue che $n = m_1 m_2 \cdots m_s$ divide $a - b$, e dunque che $a + n\mathbb{Z} = b + n\mathbb{Z}$, provando l'iniettività di f.

Per la suriettività, si osservi che

$$\left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| = n = \left|\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right| \times \cdots \times \left|\frac{\mathbb{Z}}{m_s\mathbb{Z}}\right| = \left|\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{m_s\mathbb{Z}}\right|.$$

Dunque f è una applicazione iniettiva tra insiemi finiti dello stesso ordine, e pertanto è anche suriettiva. ■

Corollario 2.3.2 *Con le stesse ipotesi del Teorema precedente, il gruppo degli elementi invertibili di* $\frac{\mathbb{Z}}{n\mathbb{Z}}$ *è isomorfo a:*

$$\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^* \simeq \left(\frac{\mathbb{Z}}{m_1\mathbb{Z}}\right)^* \times \left(\frac{\mathbb{Z}}{m_2\mathbb{Z}}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{m_s\mathbb{Z}}\right)^*.$$

Il Teorema 2.3.1 si può riformulare in termini di congruenze nel modo classico.

Teorema 2.3.3 (Cinese del resto) *Siano* $m_1, m_2, \ldots, m_s$ *elementi di* $\mathbb{N}^*$ *a due a due coprimi, e sia* $n = m_1 m_2 \cdots m_s$. *Per ogni* $i = 1, 2, \ldots, s$ *siano dati* $a_i, b_i \in \mathbb{Z}$. *Allora, il sistema di congruenze*

$$\begin{cases} a_1 x \equiv b_1 \ (mod\, m_1) \\ a_2 x \equiv b_2 \ (mod\, m_2) \\ \ldots \\ a_s x \equiv b_s \ (mod\, m_s) \end{cases}$$

ammette soluzioni in $\mathbb{Z}$ *se e solo se ciascuna congruenza* $a_i x \equiv b_i \ (mod\, m_i)$ *ammette soluzioni.*

Dimostrazione. Supponiamo che, per ciascuno degli $i = 1, 2, \ldots, s$, la congruenza $a_i x \equiv b_i (mod\, m_i)$ ammetta soluzioni, e sia x_i una sua soluzione. Per il teorema 2.3.1 (la suriettività dell'applicazione nell'enunciato), esiste un intero y tale che

$$(y + m_1\mathbb{Z}, y + m_2\mathbb{Z}, \ldots, y + m_s\mathbb{Z}) = \\ = (x_1 + m_1\mathbb{Z}, x_2 + m_2\mathbb{Z}, \ldots, x_s + m_s\mathbb{Z}),$$

ovvero $y \equiv x_i (mod\, m_i)$, per ogni $i = 1, 2, \ldots, s$. Tale y è una soluzione del sistema delle congruenze. ■

La dimostrazione che abbiamo dato del teorema cinese del resto è elegante ma astratta. In particolare non sembra suggerire un metodo per trovere le soluzioni del sistema (a partire da quelle delle singole congruenze). Non sarebbe difficile dare una dimostrazione più diretta e costruttiva, che tuttavia lasciamo per esercizio.

Assumendo le ipotesi e le notazioni dell'enunciato del Teorema 2.3.3, vediamo come è possibile ricavare una soluzione del sistema

a partire dalle soluzioni x_i di ciascuna congruenza. Per ogni m_i, poniamo $m_i' = n/m_i$. Osserviamo che le ipotesi sugli m_i assicurano che, per ogni $i = 1, \ldots, s$, si ha $(m_i, m_i') = 1$ e $m_i' \equiv 0 \pmod{m_j}$ se $i \neq j$. Mediante l'algoritmo di Euclide, per ogni indice i, si trovano quindi interi u_i, c_i tali che $u_i m_i + c_i m_i' = 1$ (ovvero, $c_i m_i' \equiv 1 \pmod{m_i}$). Se $x_1, x_2, \ldots, x_s$ sono soluzioni delle singole congruenze, si pone

$$y = x_1 m_1' c_1 + x_2 m_2' c_2 + \cdots + x_s m_s' c_s.$$

Per la definizione degli m_i' e la scelta dei c_i, si ha che, per ogni $i = 1, \ldots, s$,

$$y \equiv x_i m_i' c_i \equiv x_i \pmod{m_i}.$$

Dunque y è una soluzione del sistema di congruenze.

A sua volta il Teorema cinese del resto può essere enunciato in termini (apparentemente) più generali (la dimostrazione è lasciata per esercizio).

Teorema 2.3.4 *Siano $m_1, m_2, \ldots, m_s$ elementi di $\mathbb{N}^*$ a due a due coprimi, e sia $n = m_1 m_2 \cdots m_s$. Sia g un polinomio non nullo a coefficienti in $\mathbb{Z}$. Le seguenti asserzioni sono equivalenti*

1. *è risolubile in $\mathbb{Z}$ la congruenza*

$$g(x) \equiv 0 \ (mod\, n).$$

2. *Per ogni $i = 1, 2, \ldots, s$, è risolubile in $\mathbb{Z}$ la congruenza*

$$g(x) \equiv 0 \ (mod\, m_i).$$

CONGRUENZE MODULO UN NUMERO COMPOSTO

Sia $f = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio non nullo (a coefficienti in un campo $\mathbb{F}$). Il *polinomio derivato* di f è:

$$f' = a_1 + 2a_2 x + 3a_3 x^2 \cdots + n a_n x^{n-1}.$$

A volte, per rendere la notazione più agevole scriveremo $f' = D(f)$. Inoltre, come consuetudine, si pone $f^{(0)} = f$ e induttivamente, per $k \geq 2$, $f^{(k)} = (f^{(k-1)})'$. La seguente regola per il prodotto si verifica immediatamente.

Siano f, g, polinomi su un campo $\mathbb{F}$. Allora $(fg)' = f'g + fg'$.

Lemma 2.4.1 *Sia $f = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio non nullo in $\mathbb{Z}[x]$, e sia $k \geq 1$. Allora*

$$f^{(k)} = k! \sum_{i=0}^{n-k} \binom{k+i}{i} a_{k+i} x^i.$$

In particolare, $\frac{1}{k!} f^{(n)} \in \mathbb{Z}[x]$.

DIMOSTRAZIONE. Procediamo per induzione su k. Se $k = 1$, la cosa è immediata per definizione. Sia $k \geq 1$; allora, applicando l'ipotesi induttiva,

$$\begin{aligned} f^{(k+1)} = (f^{(k)})' &= D\left(k! \sum_{i=0}^{n-k} \binom{k+i}{i} a_{k+i} x^i\right) \\ &= k! \sum_{i=1}^{n-k} i \binom{k+i}{i} a_{k+i} x^{i-1}. \end{aligned}$$

Ponendo $j = i - 1$, si ha

$$\begin{aligned} f^{(k+1)} &= (k+1)! \sum_{j=0}^{n-k-1} \frac{j+1}{k+1} \binom{k+1+j}{j+1} a_{k+1+j} x^j \\ &= (k+1)! \sum_{j=0}^{n-(k+1)} \binom{(k+1)+j}{j} a_{(k+1)+j} x^j. \end{aligned}$$

Il lemma è quindi provato. ■

Il Lemma che segue non è che un caso particolare della formula di Taylor.

Lemma 2.4.2 *Sia $f(x)$ un polinomio non nullo in $\mathbb{Z}[x]$, e sia $b \in \mathbb{Z}$. Allora*

$$f(x+b) = \sum_{k=0}^{n} \frac{b^k f^{(k)}(x)}{k!}.$$

In particolare, $f(x+b) = f(x) + f'(x)b + s_b(x)b^2$, dove $s_b(x)$ è un polinomio a coefficienti interi.

DIMOSTRAZIONE. Sia $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ un polinomio non nullo in $\mathbb{Z}[x]$. Sviluppando mediante la formula di Newton ciascun binomio $(x+b)^k$, per $0 \leq k \leq n$, ed applicando il Lemma 2.4.1, si ottiene

$$\begin{aligned} f(x+b) = \sum_{i=0}^{n} a_i (x+b)^i &= \sum_{i=0}^{n} a_i \left(\sum_{k=0}^{i} \binom{i}{k} x^{i-k} b^k\right) \\ &= \sum_{k=0}^{n} b^k \left(\sum_{i=k}^{n} \binom{i}{k} a_i x^{i-k}\right) = \sum_{k=0}^{n} b^k \left(\sum_{j=0}^{n-k} \binom{k+j}{k} a_{k+j} x^j\right) \\ &= \sum_{k=0}^{n} \left(b^k \sum_{j=0}^{n-k} \binom{k+j}{j} a_{k+j} x^j\right) = \sum_{k=0}^{n} \frac{b^k f^{(k)}(x)}{k!}, \end{aligned}$$

ed il Lemma è dimostrato. ■

Corollario 2.4.3 *Siano $f(x) \in \mathbb{Z}[x]$, p un primo e $x_0 \in \mathbb{Z}$ tale che $f'(x_0) \equiv 0 \pmod{p}$. Allora x_0 è soluzione di $f(x) \equiv 0 \pmod{p^2}$ se e solo se ogni $x_0 + tp$, con $0 \leq t \leq p-1$, lo è.*

Teorema 2.4.4 (Lemma di Hensel) *Sia p un primo e $f \in \mathbb{Z}[x]$ un polinomio il cui coefficiente direttivo non sia multiplo di p. Supponiamo che esista un intero z_1 tale che*

$$\begin{cases} f(z_1) \equiv 0 \pmod{p} \\ f'(z_1) \not\equiv 0 \pmod{p} \end{cases}$$

Allora, per ogni $n \geq 1$ esiste un intero z_n tale che:

$$\begin{cases} f(z_n) \equiv 0 \pmod{p^n} \\ z_{n+1} \equiv z_n \pmod{p^n} \\ f'(z_n) \not\equiv 0 \pmod{p} \end{cases}$$

Dimostrazione. Siano f e z_1 come nell'enunciato. Procedendo per induzione su n, proviamo l'esistenza di $z_n \in \mathbb{Z}$ con le proprietà desiderate.

Il passo $n = 1$ è soddisfatto se definiamo

$$z_2 = z_1 + t_1 p,$$

dove $0 \leq t_1 \leq p-1$ è tale che $f'(z_1)t_1 \equiv -\frac{f(z_1)}{p} \pmod{p}$.

Supponiamo, per ipotesi induttiva di aver già costruito $z_1, z_2, \ldots, z_n$. Sia t un numero intero arbitrario. Allora, per il Lemma 2.4.2, esiste un polinomio intero $s(x)$, tale che

$$f(z_n + tp^n) = f(z_n) + f'(z_n)tp^n + s(z_n)t^2p^{2n}.$$

Quindi, in particolare,

$$f(z_n + tp^n) \equiv f(z_n) + f'(z_n)tp^n \pmod{p^{n+1}}.$$

Ora, siccome, per ipotesi induttiva, $f(z_n) \equiv 0 \pmod{p^n}$, $f(z_n)/p^n$ è un numero intero. Inoltre, $f'(z_n) \not\equiv 0 \pmod{p}$, e dunque esiste un $0 \leq t_n \leq p-1$ tale che

$$f'(z_n)t_n \equiv -\frac{f(z_n)}{p^n} \pmod{p}.$$

Ponendo $z_{n+1} = z_n + t_n p^n$, si ha subito $z_{n+1} \equiv z_n \pmod{p^n}$. Inoltre, sostituendo nella congruenza di sopra, si ottiene

$$f(z_{n+1}) \equiv f(z_n) + f'(z_n)t_n p^n \equiv 0 \pmod{p^{n+1}}.$$

Resta da provare che $f'(z_{n+1}) \not\equiv 0 \pmod{p}$. Ma questo è immediato dal fatto che $z_{n+1} \equiv z_n \pmod{p}$, e che $f'(z_n) \not\equiv 0 \pmod{p}$. ∎

Vediamo ora come la combinazione del Lemma di Hensel con il Teorema cinese del resto, consente di ricondurre la soluzione di congruenze modulo un intero generico a congruenze modulo un numero primo.

Supponiamo dunque di voler risolvere la congruenza

$$f(x) \equiv 0 \pmod{n}$$

con $f(x) \in \mathbb{Z}[x]$, e $n \geq 2$. Per il Teorema cinese del resto (nella versione 2.3.4) possiamo supporre che $n = p^k$ sia la potenza di un numero primo p; il problema si è quindi ricondotto a risolvere la seguente congruenza

$$f(x) \equiv 0 \pmod{p^k}. \tag{9}$$

Si considera allora $f(x) \equiv 0 \pmod{p}$. Se questa non ammette soluzioni, allora chiaramente neppure la (9) ne ha. Supponiamo quindi che $f(x) \equiv 0 \pmod{p}$ sia risolubile e sia $x_1, x_2, \ldots, x_s$ (con $s \leq p$) un sistema di rappresentanti delle soluzioni di essa (i cui elementi sono a due a due non congrui modulo p, e che anzi possiamo prendere compresi tra 0 e $p-1$). Per ogni $i = 1, \ldots, s$, si calcola $f'(x_i)$.

- Se $f'(x_i) \not\equiv 0 \pmod{p}$, allora per il Lemma di Hensel è possibile trovare soluzioni della congruenza (15refpp) che sono congrue a x_i modulo p. Di fatto, in un primo passo, si trovano quelle della congruenza modulo p^2: la dimostrazione del Teorema 2.4.4 mostra che (modulo p^2) ce n'è una sola, e suggerisce anche come calcolarla.

- Se $f'(x_i) \equiv 0 \pmod{p}$, allora per il Lemma 2.4.2, per ogni intero t,

$$f(x_i + tp) \equiv f(x_i) \pmod{p^2};$$

dunque, è possibile sollevare la soluzione x_i ad una soluzione di $f(x) \equiv 0 \pmod{p^2}$ se e soltanto se x_i è già una soluzione di questa (vd. Corollario 2.4.3). In tal caso, tutti gli interi $x_i + tp$ con $0 \leq t \leq p-1$ sono soluzioni della congruenza modulo p^2.

In questo modo, dopo aver applicato la procedura descritta a tutti gli $x_1, \ldots, x_s$ si sarà trovato un sistema completo di rappresentanti delle soluzioni della congruenza $f(x) \equiv 0 \pmod{p^2}$ (detto un sollevamento di quello modulo p). Da questo, con lo stesso procedimento, si risale alle soluzioni modulo p^3, e così via, sino al modulo p^k desiderato.

L'esempio che segue chiarirà forse meglio l'algoritmo.

Esempio 2.4.1 Determinare le soluzioni della congruenza

$$x^3 - 2x^2 + 3x + 9 \equiv 0 \pmod{27}.$$

Posto $f(x) = x^3 - 2x^2 + 3x + 9$, si ha $f'(x) = 3x^2 - 4x + 3$. Un sistema di rappresentanti delle soluzioni di $f(x) \equiv 0 \pmod{3}$ è dato da $x_1 = 0$, $x_2 = 2$. A partire da queste si determinano le soluzioni modulo 3^2.

- Per $x_1 = 0$, si ha $f'(0) = 3 \equiv 0 \pmod{3}$. Poiché $f(0) = 9 \equiv 0 \pmod{3^2}$, si ha che $y_1 = 0$, $y_2 = 0 + 3 = 3$, $y_3 = 0 + 6 = 6$ sono soluzioni della congruenza $f(x) \equiv 0 \pmod{3^2}$.

- Per $x_2 = 2$, si ha $f(2) = 15$, e $f'(2) = 7 \not\equiv 0 \pmod 3$. Per il lemma di Hensel x_2 si può sollevare ad un'unica soluzione modulo 3^2, che è data da $2 + 3t_0$, dove t_0 è la soluzione di

$$f'(2)t_0 \equiv -\frac{f(2)}{3} \pmod 3.$$

Cioè $7t_0 \equiv -5 \pmod 3$, da cui si ricava $t_0 = 1$. Quindi la soluzione modulo 3^2, associata (cioè ad essa congrua modulo 3) a $x_2 = 2$ è $y_4 = x_2 + 3 \cdot 1 = 5$.

Pertanto, un sistema completo di rappresentanti delle soluzioni di $f(x) \equiv 0 \pmod{3^2}$ è $y_1 = 0$, $y_2 = 3$, $y_3 = 6$, $y_4 = 5$. Ad ognuna di queste si riapplica il procedimento.

- Per $y_1 = 0$. Si ha $f'(0) = 3 \equiv 0 \pmod 3$, ma $f(0) = 9 \not\equiv 0 \pmod{3^3}$. Quindi, 0 non si solleva ad alcuna soluzione modulo 3^3.
- Per $y_2 = 3$. Si ha $f'(3) = 18 \equiv 0 \pmod 3$, e $f(3) = 27 \equiv 0 \pmod{3^3}$. Quindi, $y_2 = 3$ si solleva alle soluzioni $z_1 = 3$, $z_2 = 3 + 9 = 12$ e $z_3 = 3 + 18 = 21$, di $f(x) \equiv 0 \pmod{3^3}$.
- Per $y_3 = 6$. Si ha $f'(6) = 87 \equiv 0 \pmod 3$, ma $f(6) = 171 \not\equiv 0 \pmod{3^3}$. Quindi, 6 non si solleva ad alcuna soluzione modulo 3^3.
- Per $y_4 = 5$. Si ha $f'(5) = 58 \not\equiv 0 \pmod 3$, e $f(5) = 99$. Per il Lemma di Hensel, $y_4 = 5$ si solleva alla soluzione $z_4 = 5 + 9t_1$, dove t_1 è tale che $58t_1 \equiv -\frac{99}{9} \pmod 3$; ovvero $t_1 = 1$. La soluzione di $f(x) \equiv 0 \pmod{3^3}$ associata a y_4 è dunque $z_4 = 5 + 9 = 14$.

In conclusione, un sistema completo di rappresentanti delle soluzioni della congruenza $x^3 - 2x^2 + 3x + 9 \equiv 0 \pmod{27}$ è dato da 3, 12, 14, 21.

APPENDICE

Una formula per p_n

Esistono diverse formule, tutte estremamente inefficienti dal punto di vista computazionale, per calcolare l'n-esimo numero primo, p_n, in termini di n e dei primi precedenti.

Una fra le prime trovate è dovuta ad G. H. Hardy e E. M. Wright e fa uso della seguente conseguenza del Teorema 2.1.6 di Wilson (Esercizio 2.24).

Esercizio *Per ogni $n \in \mathbb{N}^*$ sia*

$$F(n) = \left\lfloor \cos^2\left(\pi \frac{(n-1)! + 1}{n}\right) \right\rfloor$$

Si provi che $F(n) = \begin{cases} 1 & \text{se } n = 1 \text{ o } n \text{ è primo,} \\ 0 & \text{altrimenti.} \end{cases}$

Proposizione 2.5.1 (Hardy, Wright)

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left\lfloor \frac{n}{\sum_{j=1}^{m} F(j)} \right\rfloor^{1/n} \right\rfloor$$

Chi fosse interessato alla dimostrazione può consultare [26, Theorem 419] o [22].

Pseudoprimi e numeri di Carmichael

Sia n un intero positivo e supponiamo di voler determinare se n è un numero primo oppure è composto (questo è un problema pratico che si presenta in modo importante in molte applicazioni, ad esempio in alcuni sistemi crittografici). La procedura più diretta è quella di applicare il crivello di Eratostene (Lemma 1.2.2), ovvero dividere n per tutti gli interi positivi minori o uguali alla sua radice quadrata; n è un numero primo se e solo se nessuno di essi è un divisore di n. Questo può anche andar bene se n è piccolo, ma per numeri grandi questo semplice algoritmo si rivela del tutto inefficiente (a causa della crescita esponenziale del tempo necessario a svolgere tutte le operazioni). Il piccolo teorema di Fermat (Corollario 2.1.3) fornisce un criterio *necessario* affinché un intero $n \geq 2$ sia un numero primo: per ogni intero b con $(n, b) = 1$ deve essere

$$b^{n-1} \equiv 1 \pmod{n}. \tag{10}$$

Quindi se, dato un intero positivo n, troviamo un altro intero (detto base) b con $(b, n) = 1$ per cui la congruenza (10) non è soddisfatta, allora n è necessariamente un numero composto.

Una singola verifica di questo tipo è computazionalmente abbastanza agevole (perché moltiplicare è più facile che dividere). Vediamo, ad esempio che 319 non è un numero primo. Una procedura conveniente è quella di scrivere $319 - 1 = 318$ in base 2; si ha

$$318 = 2^8 + 2^5 + 2^4 + 2^3 + 2^2 + 2.$$

Quindi, tenendo conto che $b^{2^{k+1}} = (b^{2^k})^2$, e prendendo come base $b = 2$, otteniamo

$$\begin{aligned}
2^2 &= 4 \\
2^{2^2} &= 16 \\
2^{2^3} &= 256 \\
2^{2^4} &= 65536 \equiv 141 \pmod{319} \\
2^{2^5} &\equiv 141^2 = 19881 \equiv 103 \pmod{319} \\
2^{2^6} &\equiv 103^2 \equiv 82 \pmod{319} \\
2^{2^7} &\equiv 82^2 \equiv 25 \pmod{319} \\
2^{2^8} &\equiv 25^2 \equiv 306 \pmod{319}.
\end{aligned}$$

Dunque,

$$\begin{aligned} 2^{318} &= 2^{2^8}2^{2^5}2^{2^4}2^{2^3}2^{2^2}2^2 \equiv 306 \cdot 103 \cdot 141 \cdot 256 \cdot 16 \cdot 4 \\ &\equiv 193 \not\equiv 1 \pmod{319}, \end{aligned}$$

e pertanto 319 non è un numero primo (infatti $319 = 11 \cdot 29$).

Sia $b \in \mathbb{N}^*$; un intero $n \geq 2$ si dice *pseudoprimo* rispetto alla base b se $(n, b) = 1$ e la congruenza (10) è verificata.

Vediamo, ad esempio che $n = 341$ è uno pseudoprimo rispetto alla base $b = 2$ (per fare questo usiamo il fatto di conoscere già la fattorizzazione di $341 = 11 \cdot 31$ (cosa che facilita i calcoli, e che nel caso di sopra non sarebbe stata leale). Ora, $2^5 = 32 \equiv 1 \pmod{31}$, e quindi

$$2^{340} = (2^5)^{68} \equiv 1 \pmod{31}.$$

Inoltre, $2^5 \equiv -1 \pmod{11}$, dunque $2^{10} \equiv 1 \pmod{11}$, e

$$2^{340} = (2^{10})^{34} \equiv 1 \pmod{11}.$$

Poiché 11 e 31 sono coprimi si conclude che

$$2^{340} \equiv 1 \pmod{341}$$

e quindi che 341 è uno pseudoprimo rispetto alla base 2. Non è invece uno pseudoprimo rispetto alla base 3. Infatti, se, per assurdo fosse $3^{340} \equiv 1 \pmod{341}$, allora in particolare $3^{340} \equiv 1 \pmod{31}$, e dunque l'ordine di 3 modulo 31 sarebbe un divisore di 340; ma l'ordine di 3 modulo 31 è un divisore di $\phi(31) = 30$; poiché $(340, 30) = 10$, si dovrebbe avere $3^{10} \equiv 1 \pmod{31}$. Ma, da $3^5 = 243 \equiv 26 \equiv -5 \pmod{31}$ segue

$$3^{10} \equiv (-5)^2 \equiv 25 \pmod{31},$$

e dunque un assurdo.

A questo punto viene naturale congetturare che la condizione espressa dal teorema di Fermat sia anche sufficiente a ché n sia un numero primo; ovvero che se n è uno pseudoprimo rispetto ad ogni base b (con $(n, b) = 1$) allora n è un primo. Tuttavia, le cose non stanno così. Esistono cioè numeri composti che sono pseudoprimi rispetto a qualunque base ad essi coprima. Tali interi sono denominati *numeri di Carmichael*.

Un esempio è il numero $n = 1105$. Infatti, $n = 5 \cdot 13 \cdot 17$, e $n - 1 = 1104 = 2^4 \cdot 3 \cdot 23$; osserviamo quindi che $n - 1$ è un multiplo comune di $\phi(5) = 4$, $\phi(13) = 12$ e $\phi(17) = 16$. Sia b un intero coprimo con 1105, allora, per il Teorema di Fermat b^{1104} è congruo ad 1 modulo 5, 13 e 17. Poiché questi sono coprimi si conclude che

$$b^{1104} \equiv 1 \pmod{1105}$$

e dunque 1105 è un numero di Carmichael.

Nel 1939 J. Chernick ha provato che ogni numero della forma $(6k+1)(12k+1)(18k+1)$ è di Carmichael se e solo se ciascuno dei tre fattori è un numero primo ([10]). Se esistano infiniti numeri di Carmichael siffatti è tuttora una questione aperta. Il fatto che i numeri di Carmichael siano comunque infiniti è garantito da un notevole risultato di W. R. Alford, A. Granville e C. Pomerance. Nel 1994 i tre autori hanno infatti dimostrato che per n sufficientemente grande, ci sono almeno $n^{2/7}$ numeri di Carmichael compresi tra 1 ed n (si veda [2]).

Un criterio di primalità

Recentemente i matematici Agrawal, Kayal e Saxena [1] hanno proposto un algoritmo che testa la primalità di un intero positivo n in un tempo polinomiale (rispetto ad n) risolvendo così un importante problema aperto. Il loro algoritmo (chi fosse interessato può consultare anche il sito `http://fatphil.org/maths/AKS/`) si basa sul seguente ed elementare criterio di primalità.

Teorema 2.5.2 *Sia n un intero positivo, e sia a un numero naturale coprimo con n. Allora n è un numero primo se e solo se per ogni $x \in \mathbb{Z}$*

$$(x-a)^n \equiv x^n - a \pmod{n}.$$

DIMOSTRAZIONE. Sviluppando mediante la formula del binomio di Newton, si trova che, per $1 \leq i \leq n-1$, il coefficiente di x^i in $(x-a)^n - (x^n - a)$ è

$$(-1)^i \binom{n}{i} a^{n-i}.$$

Supponiamo che n sia un numero primo. Ricordo che allora, per ogni $1 \leq i \leq n-1$, n divide $\binom{n}{i}$; dunque il coefficiente di x^i in $(x-a)^n - (x^n - a)$ è un multiplo di n. Da ciò segue che

$$(x-a)^n \equiv x^n - a \pmod{n}.$$

Viceversa, supponiamo che n sia un numero composto, e sia q un divisore primo di n. Se q^k è la massima potenza di q che divide n, cioè $q^k \| n$, scritto $n = q^k b$ con $(q, b) = 1$, allora q^k è coprimo con a^{n-q} e non divide

$$\binom{n}{q} = \frac{q^k b(q^k b - 1) \cdots (q^k b - q + 1)}{1 \cdot 2 \cdot 3 \cdots q}.$$

Da ciò segue che il coefficiente di x^q in $(x-a)^n - (x^n - a)$ non è un multiplo di n e dunque (lo si dimostri) il polinomio $(x-a)^n - (x^n - a)$ non assume valori identicamente uguali a zero modulo n. ∎

ESERCIZI

Esercizio 2.1 *Determinare l'ultima cifra decimale di* 7^{139}*, e quella di* 13^{2001}.

Esercizio 2.2 *Siano* a, m *numeri interi. Si provi che se* $(a, m) = 1 = (a-1, m)$*, allora*

$$1 + a + a^2 = \cdots + a^{\phi(m)-1} \equiv 0 \,(mod\ m).$$

Esercizio 2.3 *Siano* n, m *numeri interi. Si provi che se* $(m, n) = 1$ *allora*

$$m^{\phi(n)} + n^{\phi(m)} \equiv 1 \,(mod\ mn).$$

Esercizio 2.4 *Provare che se* $m > 1$ *e* $(m-1)! \equiv -1 \,(mod\ m)$*, allora* m *è primo.*

Esercizio 2.5 *Sia* $G = \langle g \rangle$ *un gruppo ciclico (moltiplicativo) di ordine pari* n*, e sia* $a = 1 \cdot g \cdot g^2 \cdots g^{n-1}$*. Si provi che* $a \neq 1_G$ *e che* $a^2 = 1$*. Si usi questo fatto ed il teorema 2.1.5 per dare una dimostrazione alternativa del Teorema di Wilson.*

Esercizio 2.6 *Per* $n \in \mathbb{N}$*, sia* $F_n = 2^{2^n} + 1$ *l'*n*-esimo numero di Fermat. Si provi che ogni divisore primo di* F_n *è del tipo* $2^{n+1}k + 1$*. Applicando l'esercizio 1.8 del Capitolo 1, si deduca che, per ogni* $n \geq 1$*, esistono infiniti numeri primi congrui a* 1 *modulo* 2^n.

Esercizio 2.7 *Si provi che un intero positivo è divisibile per* 11 *se e solo se la somma delle sue cifre decimali di posto pari è congrua alla somma di quelle di posto dispari modulo* 11.

Esercizio 2.8 *Sia* n *un intero naturale e sia* $n = \sum_{i=0}^{k} n_i \cdot 10^i$ *la sua scrittura in base* 10*. Definiamo* $g(n) = \left(\sum_{i=1}^{k} n_i \cdot 10^{i-1}\right) - 2n_0$*. Si provi che* n *è divisibile per* 7 *se e solo se lo è* $g(n)$.

Esercizio 2.9 *Provare che* $(712)! + 1$ *non è primo.*

Esercizio 2.10 *Nelle ipotesi della Proposizione 2.2.1, sia* a_o *una soluzione della congruenza. Si provi che un sistema completo di rappresentanti modulo* n *di tutte le soluzioni è dato dagli interi*

$$a_o + t\frac{n}{(a,n)}, \qquad con \quad 0 \leq t < (a, n).$$

In particolare, il numero di soluzioni è (a, n).

Esercizio 2.11 *Si determinino le soluzioni della congruenza*

$$39x \equiv 5 \pmod{14}.$$

Esercizio 2.12 *Si risolva il seguente sistema di congruenze:*

$$\begin{cases} 4x - y \equiv 3 \,(mod\ 13) \\ \\ 7x + 2y \equiv 5 \,(mod\ 13) \end{cases}$$

Esercizio 2.13 *Si dica per quali $x \in \mathbb{N}$ si ha $2^x \equiv 2 \pmod 7$.*

Esercizio 2.14 *Siano p un primo, $n \in \mathbb{N}$ e $d = (n, p-1)$. Sia $q = n/d$. Utilizzando la fattorizzazione*

$$x^n - 1 = (x^d - 1)(x^{d(q-1)} + \cdots + x^d + 1)$$

si provi che le soluzioni di $x^n \equiv 1 \pmod p$ coincidono con quelle di $x^d \equiv 1 \pmod p$.

Esercizio 2.15 *Si calcoli l'ordine di 53 modulo, rispettivamente 3, 12, 15, 19.*

Esercizio 2.16 *Sia $n \geq 3$. Si provi che, l'ordine di ogni numero dispari modulo 2^n è un divisore di 2^{n-2} (si deduca che il gruppo $(\mathbb{Z}/2^n\mathbb{Z})^*$ non è ciclico). Si provi quindi che l'ordine di 5 modulo 2^n è 2^{n-2}.*

Esercizio 2.17 *Si risolvano i seguenti sistemi di congruenze:*

$$\begin{cases} x \equiv 3 \,(mod\ 6) \\ x \equiv 5 \,(mod\ 35) \\ x \equiv 7 \,(mod\ 143) \\ x \equiv 3 \,(mod\ 323) \end{cases}$$

$$\begin{cases} x \equiv 5 \,(mod\ 6) \\ 7x \equiv 5 \,(mod\ 12) \\ 17x \equiv 19 \,(mod\ 30) \end{cases}$$

Esercizio 2.18 *Si provi che il sistema di congruenze*

$$\begin{cases} x \equiv a \,(mod\ n) \\ x \equiv b \,(mod\ m) \end{cases}$$

ha soluzioni se e solo se $(n, m)|b - a$, e che in tal caso la soluzione è unica modulo m.c.m.(m, n).

Esercizio 2.19 *Sia $n \geq 1$ e siano $p_1, p_2, \ldots, p_n$ primi distinti assegnati. Si provi che esistono n interi naturali consecutivi $a_1, a_2 = a_1 + 1, \ldots, a_n = a_1 + (n-1)$ tali che $p_i|a_i$ per ogni $i = 1, \ldots, n$.*

Esercizio 2.20 *Provare che esiste una successione strettamente crescente $a_1, a_2, \ldots$ di numeri naturali tale che per ogni $k \geq 0$ l'insieme $\{a_n + k | n \geq 1\}$ contiene al più un numero finito di primi.*

Esercizio 2.21 *Sia p un primo dispari, e sia $a \in \mathbb{Z}$ tale che p non divide a. Supponiamo che esista un intero b tale che $b^2 \equiv a \pmod{p}$. Si provi che, per ogni $s \geq 1$, la congruenza $x^2 \equiv a \pmod{p^s}$ ammette soluzioni.*

Esercizio 2.22 *Dire quale condizione deve essere soddisfatta dal primo p affinché la proprietà analoga a quella dell'esercizio precedente valga con la potenza terza, invece del quadrato.*

Esercizio 2.23 *Si risolvano le seguenti congruenze.*

$$x^4 - 3x^2 + 11 \equiv 0 \pmod{5^3},$$

$$x^4 - 2x^2 + x - 3 \equiv 0 \pmod{5^3}.$$

Esercizio 2.24 *Per ogni $n \in \mathbb{N}^*$ sia*

$$F(n) = \left\lfloor \cos^2\left(\pi \frac{(n-1)! + 1}{n}\right) \right\rfloor$$

Si provi che $F(n) = \begin{cases} 1 & \text{se } n = 1 \text{ o } n \text{ è primo,} \\ 0 & \text{altrimenti.} \end{cases}$

Esercizio 2.25 *Si provi che 561 e 1729 sono numeri di Carmichael.*

Esercizio 2.26 *Sia $n = p_1 p_2 \cdots p_s$ un prodotto di almeno due primi distinti, tale che, per ogni $i = 1, \ldots, s$, il numero $p_i - 1$ divide $n - 1$. Si provi che n è un numero di Carmichael.*

Two times two is four! Two times four is eight! Two times eight is sixteen And the hour is getting late! Two times sixteen is thirty-two, Twice that is sixty-four; Next comes a hundred twenty-eight, And do you want to hear more? Keep doubling ten generations, You can have a million. Keep doubling another million, You can have another billion. Keep doubling another billion, You are going to have quadrillion. Either people get smaller Or the world's going to get bigger; Or there's a couple other possibilities, I'll leave it to you to figure.

([57])

3 RESIDUI QUADRATICI

Sia p un primo dispari, e siano $a, b, c \in \mathbb{Z}$ con $p \nmid a$. Risolvere la congruenza quadratica

$$ax^2 + bx + c \equiv 0 \pmod{p} \tag{11}$$

equivale a risolvere nel campo $\mathbb{Z}/p\mathbb{Z}$ l'equazione di secondo grado

$$\overline{a}x^2 + \overline{b}x + \overline{c} = \overline{0} \tag{12}$$

(dove il soprassegno indica, come usuale, la classe di congruenza modulo p del numero intero sottostante). Ora, le eventuali soluzioni della (12) soddisfano alla medesima formula che si usa per risolvere equazioni reali di secondo grado. Quindi, la (12) è risolubile in $\mathbb{Z}/p\mathbb{Z}$ (e pertanto la congruenza (11) è risolubile in $\mathbb{Z}$) se e soltanto se il *discriminante* $\Delta = \overline{b}^2 - 4\overline{a} \cdot \overline{c}$ è un quadrato in $\mathbb{Z}/p\mathbb{Z}$, ovvero se e soltanto se la congruenza

$$x^2 \equiv \Delta \pmod{p} \tag{13}$$

è risolubile. Questo Capitolo è dedicato a risultati classici che riguardano tali congruenze quadratiche. Vedremo in particolare la famosa Legge di Reciprocità Quadratica che regola congruenze del tipo (13) per coppie di moduli primi p e q diversi.

IL SIMBOLO DI LEGENDRE

Definizione 3.1.1 *Siano $a, b \in \mathbb{Z}$, con $b \neq 1$. a si dice un* residuo quadratico (R.Q.) modulo b *se esiste un $c \in \mathbb{Z}$ tale che*

$$c^2 \equiv a \pmod{b},$$

ovvero se $\overline{a} = a + b\mathbb{Z}$ è un quadrato nell'anello $\mathbb{Z}/b\mathbb{Z}$.

Il caso in cui $b = p$ è un numero primo è particolarmente interessante. Se $p = 2$, allora ogni elemento di $\mathbb{Z}/2\mathbb{Z}$ è un quadrato, e quindi ogni intero è un residuo quadratico modulo 2. Se invece p è un primo dispari le cose sono più complicate, ed è conveniente introdurre il seguente

Definizione 3.1.2 SIMBOLO DI LEGENDRE. *Siano p un numero primo dispari ed a un intero. Si pone*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p|a; \\ 1 & \text{se } p \nmid a \text{ ed } a \text{ è un R.Q. modulo } p; \\ -1 & \text{se } a \text{ non è un R.Q. modulo } p. \end{cases}$$

Sia p un primo dispari, e sia $a \in \mathbb{Z}$. Per definizione a è un R.Q. modulo p se e soltanto se la classe di congruenza, $\overline{a}$, di a modulo p è un quadrato nel campo $\mathbb{Z}/p\mathbb{Z}$. Ora, siccome p è dispari, per ogni $0 \neq \overline{a}$ in $\mathbb{Z}/p\mathbb{Z}$, si ha $-\overline{a} \neq \overline{a}$ e $(-\overline{a})^2 = \overline{a}^2$. Ne segue che esattamente la metà degli elementi non nulli di $\mathbb{Z}/p\mathbb{Z}$ è un quadrato. Ovvero, contando anche lo 0, il numero di quadrati in $\mathbb{Z}/p\mathbb{Z}$ è

$$1 + (p-1)/2 = (p+1)/2.$$

Una maniera più astratta (e forse migliore) di provare questo semplice fatto, consiste nell'osservare che, per il Teorema 2.1.5, il gruppo moltiplicativo $G = (\mathbb{Z}/p\mathbb{Z})^*$ è ciclico di ordine $p-1$; sia α un suo generatore. Poiché $2|p-1$, il sottogruppo $Q = \langle \alpha^2 \rangle$ è un sottogruppo di G, di ordine $\frac{p-1}{2}$. Se $x \in Q$, allora, per qualche $0 \leq n \leq p-2$,

$$x = (\alpha^2)^n = (\alpha^n)^2$$

e dunque x è un quadrato. Viceversa, sia $y \neq 0$ un quadrato in $\mathbb{Z}/p\mathbb{Z}$. Allora y è il quadrato di un elemento in G, e quindi, per qualche m intero $y = (\alpha^m)^2 = (\alpha^2)^m \in Q$. Dunque, Q è l'insieme dei quadrati non nulli di $\mathbb{Z}/p\mathbb{Z}$, e si ritrova la formula di sopra.

Prima di vedere un'importante applicazione di questa osservazione alla teoria dei residui quadratici, dimostriamo un Lemma che ci sarà utile nei capitoli successivi.

Lemma 3.1.1 *Sia p un numero primo. Allora ogni elemento del campo $\mathbb{Z}/p\mathbb{Z}$ è una somma di due quadrati.*

Dimostrazione. Se $p = 2$ non c'e nulla da dimostrare. Sia dunque p un primo dispari, e sia Q_0 l'insieme dei quadrati di $\mathbb{Z}/p\mathbb{Z}$. Per quanto visto sopra $|Q_0| = (p+1)/2$.

Sia $a \in \mathbb{Z}/p\mathbb{Z}$. Consideriamo l'applicazione σ_a da Q_0 in $\mathbb{Z}/p\mathbb{Z}$, definita da

$$\sigma_a(y) = a - y$$

per ogni $y \in Q_0$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un gruppo additivo, σ_a è iniettiva, e quindi, posto $Q_1 = \sigma_a(Q_0)$, si ha $|Q_1| = |Q_0| = \frac{p+1}{2}$. D'altra parte Q_0 e Q_1 sono sottoinsiemi di $\mathbb{Z}/p\mathbb{Z}$, e quindi $|Q_0 \cup Q_1| \leq |\mathbb{Z}/p\mathbb{Z}| = p$. Dunque

$$p \geq |Q_0 \cup Q_1| = |Q_0| + |Q_1| - |Q_0 \cap Q_1| = p + 1 - |Q_0 \cap Q_1|;$$

da cui segue che l'intersezione $Q_0 \cap Q_1$ non è vuota. Dunque esiste un $y \in Q_0$ tale che $\sigma_a(y) = a - y \in Q_0 \cap Q_1$, provando che $a = y + (a-y)$ è una somma di due quadrati. ∎

Torniamo ora al nostro argomento principale, provando il cosiddetto *Criterio di Eulero*.

Proposizione 3.1.2 (criterio di Eulero) *Siano p un primo dispari, ed $a \in \mathbb{Z}$, con $(a, p) = 1$. Allora*

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

Dimostrazione. Dal Teoream di Fermat (Corollario 2.1.3) segue che $a^{\frac{p-1}{2}}$ è una soluzione dell'equazione

$$x^2 \equiv 1 \pmod{p},$$

e poiché tale equazione ha esattamente due soluzioni modulo p, che sono 1 e -1 si ha

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

Se $\left(\frac{a}{p}\right) = 1$, a è un R.Q. modulo p, cioè esiste $c \in \mathbb{Z}$ tale che $c^2 \equiv a \pmod{p}$. Ma allora, ancora per il Corollario 2.1.3,

$$a^{\frac{p-1}{2}} \equiv c^{p-1} \equiv 1 \pmod{p}.$$

Viceversa sia $\left(\frac{a}{p}\right) = -1$. Per quanto osservato in precedenza, il numero di quadrati non nulli modulo p è esattamente $\frac{p-1}{2}$; e quindi essi sono tutte e sole le soluzioni dell'equazione

$$x^{\frac{p-1}{2}} = \overline{1} \tag{14}$$

in $\mathbb{Z}/p\mathbb{Z}$ (si ricordi che, poichè $\mathbb{Z}/p\mathbb{Z}$ è un campo l'equazione di sopra ha al più $\frac{p-1}{2}$ soluzioni). Dunque, se $a \in \mathbb{Z}$ (con $(a, p) = 1$) non è un R.Q. modulo p, allora $\overline{a}$ non è una soluzione dell'equazione (14), quindi, per quanto prima osservato, deve essere

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

provando così la Proposizione. ■

Non è ora difficile verificare che valgono le seguenti proprietà elementari.

Lemma 3.1.3 *Sia p un primo dispari, e siano $a, b \in \mathbb{Z}$. Allora*

1. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *se* $a \equiv b \pmod{p}$;
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
3. $\left(\frac{a^2}{p}\right) = 1$ *(se* $p \nmid a$*)*;
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

DIMOSTRAZIONE. I punti 1. e 3. discendono immediatamente dalle definizioni.

Per il punto 2., la cosa è ovvia se p divide ab. Altrimenti, per il criterio di Eulero,

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$$

provando così l'affermazione (essendo p dispari).

Anche il punto 4. segue dal criterio di Eulero; infatti

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

e quindi l'asserto. ■

Osserviamo che se p è un primo dispari, allora $p \equiv 1, 3 \pmod 4$. Il punto 4. del Lemma precedente può quindi essere riformulato affermando che, per un primo dispari p,

$$\left(\frac{-1}{p}\right) = 1 \quad \Leftrightarrow \quad p \equiv 1 \pmod 4.$$

Sia $n \in \mathbb{N}^*$. L'insieme dei numeri interi x con $-n/2 < x \leq n/2$ è un sistema di rappresentanti delle classi di congruenza modulo n.

Definizione 3.1.3 *Dato un intero a chiamiamo* residuo assoluto *di a modulo n quell'unico intero $-n/2 < b \leq n/2$ tale che $a \equiv b \pmod n$.*

Lemma 3.1.4 (Lemma di Gauss) *Sia p un primo dispari, e sia $a \in \mathbb{N}^*$ tale che $(a, p) = 1$. Sia t il numero di elementi nell'insieme*

$$S = \{\, a, 2a, \ldots, ((p-1)/2)a \,\}$$

il cui residuo assoluto modulo p è negativo. Allora

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

DIMOSTRAZIONE. Osserviamo che, poiché $(a, p) = 1$, gli elementi di S sono a due a due non congrui modulo p.

Sia $k = \frac{p-1}{2} - t$. Siano $r_1, r_2, \ldots, r_k$ i residui assoluti positivi degli elementi di S, e siano $-s_1, -s_2, \ldots, -s_t$ quelli negativi. Supponiamo che esistano $1 \leq i \leq k$ e $1 \leq j \leq t$ tali che $r_i \equiv s_j \pmod p$. Ora, esistono $1 \leq n_i, n_j \leq (p-1)/2$, tali che $an_i \equiv r_i \pmod p$ e $an_j \equiv -s_j \pmod p$. Ma allora

$$a(n_i + n_j) \equiv 0 \pmod p$$

e quindi p divide $n_i + n_j$, il che è impossibile. Dunque gli elementi dell'insieme $R = \{r_1, \ldots, r_k, s_1, \ldots, s_t\}$ sono a due a due non congrui

modulo p, e di conseguenza $R = \{1, 2, \ldots, (p-1)/2\}$. Da ciò segue che

$$\begin{aligned} a^{\frac{p-1}{2}}((p-1)/2)! &= a \cdot 2a \cdots ((p-1)/2)a \\ &\equiv \prod_{i=1}^{k} r_i \cdot \prod_{j=1}^{t}(-s_j) \\ &\equiv (-1)^t \prod_{i=1}^{k} r_i \cdot \prod_{j=1}^{t} s_j \\ &\equiv (-1)^t((p-1)/2)! \pmod{p}; \end{aligned}$$

e quindi, poiché p non divide $((p-1)/2)!$,

$$a^{\frac{p-1}{2}} \equiv (-1)^t \pmod{p}$$

e la dimostrazione si completa applicando il criterio di Eulero, e tenendo conto del fatto che $\left(\frac{a}{p}\right) \in \{1, -1\}$. ■

Il Lemma di Gauss può essere impiegato per calcolare il valore del simbolo di Legendre. Ad esempio, determiniamo $\left(\frac{5}{13}\right)$.

	res. ass. (mod 13)
$1 \cdot 5 = 5$	5
$2 \cdot 5 = 10$	-3
$3 \cdot 5 = 15$	2
$4 \cdot 5 = 20$	-6
$5 \cdot 5 = 25$	-1
$6 \cdot 5 = 30$	4

quindi il numero t di residui assoluti negativi per i multipli di 5 da considerare è 3 e pertanto, per il Lemma di Gauss,

$$\left(\frac{3}{13}\right) = (-1)^3 = -1.$$

Proposizione 3.1.5 *Sia p un primo dispari. Allora*

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

Dimostrazione. Applichiamo il Lemma di Gauss (Lemma 3.1.4) con $a = 2$, e quindi $Q = \{2, 4, \ldots, p-1\}$. In questo caso, gli elementi di Q il cui residuo assoluto modulo p è negativo sono quelli maggiori di $p/2$, ovvero (in ordine decrescente)

$$p-1,\ p-3,\ \ldots,\ p-(2t-1)$$

dove quindi t è il massimo tale che $p-(2t-1) > p/2$, e cioè

$$t = \left\lfloor \frac{p+2}{4} \right\rfloor.$$

Se $p \equiv \pm 1 \pmod 8$, allora $\frac{p^2-1}{8}$ è pari; inoltre, per qualche k, $p = 8k \pm 1$, e quindi

$$t = \left\lfloor \frac{p+2}{4} \right\rfloor = 2k$$

è pari, e dunque

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

Se invece $p \equiv 3,5 \pmod 8$, allora $\frac{p^2-1}{8}$ è dispari, $p = 8k+3$ oppure $p = 8k+5$, e quindi

$$t = \left\lfloor \frac{p+2}{4} \right\rfloor = 2k+1$$

è dispari, e dunque

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

concludendo la dimostrazione. ■

Vediamo una applicazione di quest'ultimo risultato ai numeri di Mersenne.

Proposizione 3.1.6 (L. Eulero) *Sia $1 \leq k \in \mathbb{N}$, tale che $p = 4k+3$ sia un numero primo. Allora*

1. *$2p+1$ è primo $\Leftrightarrow$ $2^p \equiv 1 \pmod{2p+1}$.*
2. *Se $p > 3$ e $2p+1$ è primo, allora $M_p = 2^p - 1$ non è un numero primo.*

Dimostrazione. 1. Osserviamo che $2p+1 \equiv 7 \pmod 8$. Se $2p+1$ è un primo, allora, per la Proposizione 3.1.5,

$$\left(\frac{2}{2p+1}\right) = (-1)^{\frac{(2p+1)^2-1}{8}} = (-1)^{\frac{49-1}{8}} = 1,$$

e quindi, dal criterio di Eulero,

$$2^p = 2^{\frac{(2p+1)-1}{2}} \equiv 1 \pmod{(2p+1)}.$$

Viceversa, supponiamo che $2^p \equiv 1 \pmod{(2p+1)}$. Allora, poiché $(2, 2p+1) = 1$, si ha che p è l'ordine di 2 modulo $2p+1$, e quindi scritto $2p+1 = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$ con p_i primi distinti,

$$p \,\Big|\, \phi(2p+1) = \prod_{i=1}^{s} p_i^{a_i-1}(p_i-1)$$

(si veda il Teorema 4.2.7 a pagina 73). Poiché $p \nmid 2p+1$, si ha che $p \neq p_i$, per ogni $i = 1, 2, \ldots, s$. Ne segue che $p | p_i - 1$ per qualche i. Ma allora, essendo $p \geq 3$ e $p_i - 1$ pari, $2p \leq p_i - 1$ e quindi $2p+1 \leq p_i \leq 2p+1$, ovvero $2p+1 = p_i$ è un primo.

2. Segue subito dal punto 1., tenendo conto che, poiché $p > 3$, $2p+1 < 2^p - 1$. ■

I primi p tali che $2p+1$ è ancora un numero primo, vengono chiamati *primi di Sophie Germain*, in onore della matematica Marie-Sophie Germain. Si congettura che questi numeri primi siano infiniti.

LA LEGGE DI RECIPROCITÀ QUADRATICA

Siano p e q due numeri primi dispari distinti. Allora, p è un residuo quadratico modulo q se la congruenza

$$x^2 \equiv p \pmod{q}$$

è risolubile. A prima vista, la risolubilità di tale congruenza non ha molto legame con la risolubilità di quella che si ottiene scambiando p con q, ovvero $x^2 \equiv q \pmod{p}$. Invece, esiste un legame molto stretto, stabilito dal Teorema seguente, che deve considerarsi come uno dei vertici della teoria dei numeri classica.

Teorema 3.2.1 (Legge di reciprocità quadratica di Gauss) *Siano p e q due numeri primi dispari distinti. Allora*

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

cioè

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right) & \text{se } p \equiv 1 \pmod 4 \text{ o } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right) & \text{se } p, q \equiv 3 \pmod 4. \end{cases}$$

Esempio 3.2.1 Proviamo che la congruenza $x^2 \equiv 257 \pmod{269}$ non ha soluzioni. Infatti, $269 = 257 + 12$; inoltre 257 e 259 sono numeri primi e possiamo applicare il Teorema di Reciprocità Quadratica, ottenendo

$$\begin{aligned}\left(\frac{257}{269}\right) = \left(\frac{269}{257}\right) = \left(\frac{12}{257}\right) = \left(\frac{3}{257}\right)\left(\frac{4}{257}\right) \\ = \left(\frac{3}{257}\right) = \left(\frac{257}{3}\right) = \left(\frac{2}{3}\right) = -1.\end{aligned}$$

Esistono diverse dimostrazioni del Teorema di reciprocità quadratica; lo stesso Gauss ne fornì sette. Quella che vedremo è prossima

Il libro di F. Lemmermeyer "Reciprocity Laws: From Euler to Eisenstein", [37], contiene 196 dimostrazioni differenti.

ad una delle dimostrazioni di Gauss; pur non essendo forse la più accessibile, dato che richiede qualche prerequisito algebrico non banale (una dimostrazione di carattere più elementare si trova nell'appendice del Capitolo), è piuttosto elegante, e fornisce delle indicazioni sulle possibili generalizzazioni (reciprocità biquadratica, cubica, etc.).

Lemma 3.2.2 *Sia p un primo dispari, e sia A un sistema di rappresentanti delle classi di congruenza modulo p. Allora*

$$\sum_{a\in A}\left(\frac{a}{p}\right)=0.$$

Dimostrazione. Il Lemma discende immediatamente dal fatto che, essendo p dispari, esattamente la metà degli elementi di $(\mathbb{Z}/p\mathbb{Z})^*$ è un quadrato (e contribuisce con 1 alla somma), e l'altra metà non lo è (e contribuisce con -1), mentre il contributo alla somma del rappresentante in A della classe nulla è zero. ∎

Dimostrazione del Teorema 3.2.1.
Siano p e q due primi dispari distinti, e sia $\mathbb{E}$ un campo di caratteristica q che contenga le radici p-esime dell'unità (ad esempio, si può prendere come $\mathbb{E}$ il campo di spezzamento del polinomio x^p-1 sul campo $\mathbb{Z}/q\mathbb{Z}$), e sia $\omega\in\mathbb{E}$ una radice primitiva p-esima. Quindi, $\{1,\omega,\omega^2,\dots,\omega^{p-1}\}$ sono tutte le radici (distinte) del polinomio $x^p-1=(x-1)(x^{p-1}+\cdots+x+1)$ nel campo $\mathbb{E}$. In particolare ω è radice del fattore di destra, e quindi

$$1+\omega+\omega^2+\cdots+\omega^{p-1}=0. \tag{15}$$

Osserviamo che per ogni $z\in\mathbb{Z}$, il valore ω^z dipende solo dalla classe di congruenza di z modulo p. Quindi ha senso definire la potenza ω^a per ogni $a\in\mathbb{Z}/p\mathbb{Z}$ (nel corso di questa dimostrazione, evitiamo di usare il soprassegno per non appesantire le notazioni). Se $0\neq a\in\mathbb{Z}/p\mathbb{Z}$, allora l'applicazione $x\mapsto ax$ al variare di $x\in(\mathbb{Z}/p\mathbb{Z})^*$ è una permutazione di $(\mathbb{Z}/p\mathbb{Z})^*$. Dalla formula (15) segue pertanto che, per ogni $a\in(\mathbb{Z}/p\mathbb{Z})^*$,

$$\sum_{x\in(\mathbb{Z}/p\mathbb{Z})^*}\omega^{ax}=\sum_{x\in(\mathbb{Z}/p\mathbb{Z})^*}\omega^{x}=\omega+\omega^2+\cdots+\omega^{p-1}=-1. \tag{16}$$

Definiamo ora l'applicazione $\tau:\mathbb{Z}/p\mathbb{Z}\longrightarrow\mathbb{E}$, ponendo, per ogni $a\in\mathbb{Z}/p\mathbb{Z}$,

$$\tau(a)=\sum_{x\in(\mathbb{Z}/p\mathbb{Z})^*}\left(\frac{x}{p}\right)\omega^{ax}.$$

Nel seguito indicheremo semplicemente con $\mathbb{F}$ il campo $\mathbb{Z}/p\mathbb{Z}$. Proviamo che, per ogni $a\in\mathbb{F}^*$,

$$\tau(a)=\left(\frac{a}{p}\right)\tau(1). \tag{17}$$

Infatti,

$$\begin{aligned}\tau(a) &= \sum_{x\in\mathbb{F}^*}\left(\frac{x}{p}\right)\omega^{ax} = \sum_{x\in\mathbb{F}^*}\left(\frac{a^{-1}ax}{p}\right)\omega^{ax}\\ &= \left(\frac{a^{-1}}{p}\right)\sum_{x\in\mathbb{F}^*}\left(\frac{ax}{p}\right)\omega^{ax} = \left(\frac{a}{p}\right)\sum_{t\in\mathbb{F}^*}\left(\frac{t}{p}\right)\omega^{t}\\ &= \left(\frac{a}{p}\right)\tau(1).\end{aligned}$$

Ora, dimostriamo che

$$\tau(1)^2 = (-1)^{(p-1)/2}p. \tag{18}$$

Applicando la formula (17), si ha

$$\begin{aligned}\tau(1)^2 &= \tau(1)\sum_{x\in\mathbb{F}^*}\left(\frac{x}{p}\right)\omega^{x} = \sum_{x\in\mathbb{F}^*}\tau(x)\omega^{x}\\ &= \sum_{x\in\mathbb{F}^*}\left[\sum_{y\in\mathbb{F}^*}\left(\frac{y}{p}\right)\omega^{xy}\right]\omega^{x} = \sum_{x\in\mathbb{F}^*}\sum_{y\in\mathbb{F}^*}\left(\frac{y}{p}\right)\omega^{x(y+1)}\\ &= \sum_{y\in\mathbb{F}^*}\left[\left(\frac{y}{p}\right)\sum_{x\in\mathbb{F}^*}\omega^{x(y+1)}\right];\end{aligned}$$

Ora, per la formula (16), se $y \in \mathbb{F}^*$ e $y+1 \neq 0$, si ha

$$\sum_{x\in\mathbb{F}^*}\omega^{x(y+1)} = -1.$$

Quindi, applicando il Lemma 3.2.2 ed il Lemma 3.1.3,

$$\begin{aligned}\tau(1)^2 &= -\sum_{\substack{y\in\mathbb{F}^*\\ y\neq -1}}\left(\frac{y}{p}\right) + \left(\frac{-1}{p}\right)\sum_{x\in\mathbb{F}^*}\omega^{0}\\ &= -\sum_{y\in\mathbb{F}^*}\left(\frac{y}{p}\right) + \left(\frac{-1}{p}\right) + \left(\frac{-1}{p}\right)\sum_{x\in\mathbb{F}^*}\omega^{0}\\ &= \left(\frac{-1}{p}\right)(1+(p-1))\\ &= \left(\frac{-1}{p}\right)p = (-1)^{\frac{p-1}{2}}p.\end{aligned}$$

Completiamo ora la dimostrazione del Teorema. Applicando la formula (18), sia ha

$$\tau(1)^{q-1} = (\tau(1)^2)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}p^{\frac{q-1}{2}}$$

e quindi, per il criterio di Eulero (tenendo conto che in $\mathbb{E}$ moltiplicare per q dà zero),

$$\tau(1)^{q-1} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right). \tag{19}$$

D'altra parte, poichè $\mathbb{E}$ è un campo di caratteristica q, l'elevazione alla q-esima potenza è un omomorfismo di $\mathbb{E}$ in se stesso. In particolare,

$$\tau(1)^q = \left(\sum_{x\in\mathbb{F}^*}\left(\frac{x}{p}\right)\omega^x\right)^q = \sum_{x\in\mathbb{F}^*}\left(\frac{x}{p}\right)^q\omega^{qx} = \tau(q).$$

Confrontando quest'ultima eguaglianza (nel campo $\mathbb{E}$) con la (19), ed applicando la formula (17), si ricava

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) = \tau(1)^{q-1} = \tau(q)\tau(1)^{-1} = \left(\frac{q}{p}\right) \tag{20}$$

Questa è un'uguaglianza nel campo $\mathbb{E}$, nella quale quindi gli interi vanno intesi come multipli dell'identità. D'altra parte, i simboli di Legendre $\left(\frac{p}{q}\right)$ e $\left(\frac{q}{p}\right)$ appartengono a $\{-1, 1\}$ e, siccome q (che è la caratteristica di $\mathbb{E}$) è dispari, in $\mathbb{E}$, $-1 \neq 1$. Ne segue che dalla uguaglianza (20) deriva l'uguaglianza in $\mathbb{Z}$

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

concludendo così la dimostrazione del Teorema. ■

IL SIMBOLO DI JACOBI

Il *simbolo di Jacobi* estende al caso dei numeri dispari il simbolo di Legendre per i numeri primi.

Definizione 3.3.1 *Sia $1 < b$ un intero dispari, e sia $b = p_1p_2p_3\cdots p_k$, come prodotto di numeri primi (non necessariamente distinti). Per ogni $a \in \mathbb{Z}$ si pone*

$$\left(\frac{a}{b}\right)_J = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{a}{p_3}\right)\cdots\left(\frac{a}{p_k}\right),$$

dove, per ogni $i = 1, 2, \ldots, k$, $\left(\frac{a}{p_i}\right)$ è l'usuale simbolo di Legendre definito a pagina 45.

Osserviamo subito che, diversamente dal simbolo di Legendre, il simbolo di Jacobi non individua i residui quadratici modulo b. Infatti, se a è un R.Q. modulo b, allora a è un R.Q. modulo ogni primo p_i e dunque

$$\left(\frac{a}{b}\right)_J = 1;$$

ma è possibile che il simbolo di Jacobi calcolato in a sia uguale ad 1 senza che a sia un R.Q. modulo b. Ad esempio, se $b = 9$, ed $a = -1$,

$$\left(\frac{-1}{9}\right)_J = \left(\frac{-1}{3}\right)\left(\frac{-1}{3}\right) = (-1)(-1) = 1$$

mentre -1 non è un R.Q. modulo 9.

Tuttavia, il simbolo di Jacobi è utile per semplificare diversi argomenti. Ne vedremo un esempio con il Teorema 3.3.3. Prima elenchiamo alcune immediate proprietà del simbolo di Jacobi; esse discendono dalla definizione e dalle analoghe proprietà del simbolo di Legendre (Lemma 3.1.3).

Lemma 3.3.1 *Siano b, b_1, b_2 numeri naturali dispari maggiori di 1, e siano a, a_1, a_2 interi. Allora*

1. $\left(\frac{a_1}{b}\right)_J = \left(\frac{a_2}{b}\right)_J$ *se* $a_1 \equiv a_2 \pmod{b}$,
2. $\left(\frac{a_1 a_2}{b}\right)_J = \left(\frac{a_1}{b}\right)_J \left(\frac{a_2}{b}\right)_J$,
3. $\left(\frac{a}{b_1}\right)_J \left(\frac{a}{b_2}\right)_J = \left(\frac{a}{b_1 b_2}\right)_J$,
4. $\left(\frac{-1}{b}\right)_J = (-1)^{\frac{b-1}{2}}$,
5. $\left(\frac{2}{b}\right)_J = (-1)^{\frac{b^2-1}{8}}$.

Dimostrazione. I punti 1., 2. e 3. si deducono immediatamente dalla definizione di simbolo di Jacobi e dalla moltiplicatività del simbolo di Legendre.

Per i rimanenti punti osserviamo preliminarmente che se m e n sono numeri naturali dispari allora

$$mn - 1 \equiv (m-1) + (n-1) \pmod{4}$$

e quindi

$$\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod{2}.$$

Dunque, se $b = p_1 p_2 \cdots p_k$, per il Lemma 3.1.3,

$$\begin{aligned}\left(\frac{-1}{b}\right)_J &= \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_k}\right) = \prod_{i=1}^{k}(-1)^{\frac{p_i-1}{2}} = (-1)^{\sum \frac{p_i-1}{2}} \\ &= (-1)^{\frac{b-1}{2}}\end{aligned}$$

provando il punto 4. Dalla stessa osservazione di sopra segue anche che, se n e m sono dispari

$$\frac{m^2n^2-1}{8} \equiv \frac{m^2-1}{8} + \frac{n^2-1}{8} \pmod{2}.$$

Dunque, per la Proposizione 3.1.5,

$$\begin{aligned}\left(\frac{2}{b}\right)_J &= \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_k}\right) = \prod_{i=1}^{k}(-1)^{\frac{p_i^2-1}{8}} = (-1)^{\sum \frac{p_i^2-1}{8}} \\ &= (-1)^{\frac{b^2-1}{8}}\end{aligned}$$

provando il punto 5. ■

Dal teorema di reciprocità quadratica di Gauss discende inoltre un analogo risultato per il simbolo di Jacobi.

Teorema 3.3.2 (Legge di Reciprocità per i simboli di Jacobi) *Siano m, n due interi positivi dispari. Allora*

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

cioè

$$\left(\frac{m}{n}\right)_J = \begin{cases} -\left(\frac{n}{m}\right)_J & \text{se } m \equiv n \equiv 3 \pmod 4 \\ \left(\frac{n}{m}\right)_J & \text{altrimenti.} \end{cases}$$

Dimostrazione. Osserviamo innanzitutto che se m ed n hanno un fattore in comune, allora, per come è definito il simbolo di Legendre, i simboli di Jacobi $\left(\frac{m}{n}\right)_J$ e $\left(\frac{n}{m}\right)_J$ sono entrambi nulli. Supponiamo pertanto che m ed n siano coprimi e scriviamo rispettivamente

$$m = \prod_{i=1}^{r} p_i \quad \text{e} \quad n = \prod_{j=1}^{s} q_j$$

come prodotto di primi (non necessariamente distinti). Per convertire $\left(\frac{m}{n}\right)_J = \prod_{i,j}\left(\frac{p_i}{q_j}\right)$ in $\left(\frac{n}{m}\right)_J = \prod_{i,j}\left(\frac{q_j}{p_i}\right)$, dobbiamo applicare il Teorema 3.2.1 esattamente rs volte. Il numero di fattori (-1) che si generano coincide con il numero di volte che sia p_i che q_j sono congrui a 3 modulo 4, questo è esattamente il prodotto di numeri primi $\equiv 3 \pmod 4$ nelle fattorizzazioni di m ed n. Pertanto $\left(\frac{m}{n}\right)_J = \left(\frac{n}{m}\right)_J$, a meno che ci sia un numero dispari di primi $\equiv 3 \pmod 4$ in entrambe le fattorizzazioni di m ed n, nel cui caso si ha $\left(\frac{m}{n}\right)_J = -\left(\frac{n}{m}\right)_J$. Ora, un prodotto di primi dispari, come lo sono m ed n, è $\equiv 3 \pmod 4$ se e solo se contiene un numero dispari di primi $\equiv 3 \pmod 4$. Si conclude che $\left(\frac{m}{n}\right)_J = \left(\frac{n}{m}\right)_J$, a meno che entrambi m ed n siano $\equiv 3 \pmod 4$. ■

Esempio 3.3.1 Consideriamo $b = 803 = 11 \cdot 73$;

$$\begin{aligned}\left(\frac{403}{803}\right)_J &= -\left(\frac{803}{403}\right)_J = -\left(\frac{-3}{403}\right)_J = \left(\frac{3}{403}\right)_J \\ &= -\left(\frac{403}{3}\right)_J = -\left(\frac{1}{3}\right)_J = -1.\end{aligned}$$

Teorema 3.3.3 *Un numero intero a è un quadrato in $\mathbb{Z}$ se e solo se $\left(\frac{a}{p}\right) = 1$ per ogni primo dispari p che non divide a.*

Dimostrazione. Se a è un quadrato in $\mathbb{Z}$, allora è ovvio che è un R.Q. modulo ogni primo dispari che non lo divide.

Viceversa, proviamo che se a non è un quadrato in $\mathbb{Z}$, allora esiste un primo p con $(a,p) = 1$, tale che a non è un R.Q. modulo p. Distinguiamo tre casi.

(1) $a = -b^2$ per qualche $b \in \mathbb{N}$.
È sempre possibile scegliere un intero $k > 0$ tale che $(b,k) = 1$ e $k \equiv 3 \pmod 4$ (lo si provi per esercizio!). Applicando il lemma 3.3.1,

$$\left(\frac{a}{k}\right)_J = \left(\frac{-b^2}{k}\right)_J = \left(\frac{-1}{k}\right)_J = (-1)^{\frac{k-1}{2}} = -1$$

e quindi, per la definizione del simbolo di Jacobi, esiste un divisore primo p di k tale che $\left(\frac{a}{p}\right) = -1$, cioè a non è un R.Q. modulo p.

(2) $a = \pm 2^t b$, con t e b numeri naturali dispari.
Per il Teorema cinese del resto, esiste un intero positivo k tale che

$$\begin{cases} k \equiv 5 \pmod 8 \\ k \equiv 1 \pmod b. \end{cases}$$

Per tale k si ha, essendo t dispari,

$$\left(\frac{2^t}{k}\right)_J = \left(\frac{-2^t}{k}\right)_J = -1,$$

ed anche, applicando il Lemma 3.3.2,

$$\left(\frac{b}{k}\right)_J = \left(\frac{k}{b}\right)_J = \left(\frac{1}{b}\right)_J = 1.$$

Quindi

$$\left(\frac{a}{k}\right)_J = \left(\frac{\pm 2^t}{k}\right)_J \left(\frac{b}{k}\right)_J = -1,$$

e dunque esiste un divisore primo di k, rispetto al quale a non è un R.Q.

(3) $a = \pm 2^{2n} q^t b$, con b numero naturale dispari, q un primo dispari tale che $(q,b) = 1$, e $t \geq 1$.

Poiché q è dispari, esiste un naturale c tale che $\left(\frac{c}{q}\right) = -1$. Per il Teorema cinese del resto, esiste un intero positivo k tale che

$$\begin{cases} k \equiv 1 \pmod{4b} \\ k \equiv c \pmod q. \end{cases}$$

Per tale intero k si ha

$$\left(\frac{2^{2n}}{k}\right)_J = \left(\frac{-2^{2n}}{k}\right)_J = 1,$$

e, applicando il Lemma 3.3.2,

$$\left(\frac{b}{k}\right)_J = \left(\frac{k}{b}\right)_J = \left(\frac{1}{b}\right)_J = 1,$$

inoltre, poiché t è dispari,

$$\left(\frac{q^t}{k}\right)_J = \left(\frac{q}{k}\right)_J = \left(\frac{k}{q}\right)_J = \left(\frac{c}{q}\right)_J = \left(\frac{c}{q}\right) = -1.$$

Quindi

$$\left(\frac{a}{k}\right)_J = \left(\frac{\pm 2^t}{k}\right)_J \left(\frac{b}{k}\right)_J \left(\frac{q^t}{k}\right)_J = -1,$$

e dunque esiste un divisore primo di k, rispetto al quale a non è un R.Q.

Poiché ogni intero a rientra in uno dei tre casi (1), (2), (3), il Teorema è dimostrato. ■

APPENDICE

Un'altra dimostrazione della Legge di Reciprocità Quadratica

Quella che vediamo è una dimostrazione di carattere più elementare di quella fornita sopra, ed è sostanzialmente la terza delle dimostrazioni proposte da Gauss.

Dimostrazione del Teorema 3.2.1.
Siano quindi p e q numeri primi dispari distinti. Poniamo

$$P = \{1, 2, \ldots, (p-1)/2\} \qquad \text{e} \qquad Q = \{1, 2, \ldots, (q-1)/2\}.$$

Sia s il numero di elementi dell'insieme $Pq = \{xq \mid x \in P\}$ il cui residuo assoluto modulo p è negativo, e sia t il numero di elementi dell'insieme $Qp = \{xp \mid x \in Q\}$ il cui residuo assoluto modulo q è negativo. Per il Lemma di Gauss (Lemma 3.1.4),

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

La Legge di reciprocità quadratica equivale quindi ad affernare che

$$s + t \text{ è dispari} \quad \Leftrightarrow \quad p \equiv q \equiv 3 \pmod 4.$$

Consideriamo l'insieme N di tutte le coppie $(u, v) \in P \times Q$ tali che

$$-q/2 < vp - uq < 0. \tag{21}$$

Queste sono i punti a coordinata intera che (in un usuale piano cartesiano) giacciono all'interno del trapezio di coordinate

$$A_0 = (0,0),\ A_1 = (p/2, q/2),\ B_1 = (0, 1/2),\ B_2 = (p/2, q(p-1)/2p).$$

La condizione (21) implica che se $(u, v) \in N$, allora il residuo assoluto di vp modulo q è negativo. Pertanto $|N| \leq t$.

Viceversa, se $j \in Q$ è tale che il residuo assoluto di jp modulo q è negativo, allora esiste un intero k tale che $-q/2 < jp - kq < 0$. Quindi, $jp < kq < jp + q/2$; siccome $1 \leq j \leq (q-1)/2$ si ha che

$$p < kq < \frac{(q-1)p}{2} + \frac{q}{2},$$

da cui segue,

$$\frac{p}{q} < k < \frac{q-1}{q} \cdot \frac{p}{2} + \frac{1}{2} < \frac{p+1}{2},$$

ed essendo k intero e p dispari,

$$1 \leq k \leq (p-1)/2,$$

ovvero $k \in P$. In conclusione per ogni $j \in Q$ tale che il residuo assoluto di jp modulo q è negativo esiste uno ed un solo punto $(j, k) \in N$. Pertanto $|N| \geq t$, e dunque $|N| = t$.

Allo stesso modo si prova che il numero di coppie $(u, v) \in P \times Q$ tali che

$$-p/2 < uq - vp < 0 \tag{22}$$

è uguale a s. In questo caso si tratta dei punti a coordinate intere che giacciono all'interno del trapezio di vertici

$$A_0 = (0,0),\ A_1 = (p/2, q/2),\ C_1 = (0,0),\ C_2 = (p/2, p(q-1)/2q).$$

Quindi, $s + t$ è uguale alla cardinalità dell'insieme U di tutti i punti a coordinata intera che giacciono all'interno dell'esagono di vertici A_0, B_1, B_2, A_1, C_2, C_1.

Ora, si verifica facilmente che $X = (x_0, y_0) \in U$ se e solo se $\sigma(X) = (x_1, y_1) \in U$, dove

$$\begin{cases} x_1 = \frac{p+1}{2} - x_0 \\ \\ y_1 = \frac{q+1}{2} - y_0. \end{cases}$$

Dunque, σ definisce una biezione involutoria su U (cioè $\sigma(\sigma(X)) = X$ per ogni $X \in U$).

Supponiamo che $X = (x_0, y_0)$ sia un punto fisso per σ (ovvero $\sigma(X) = X$). Allora

$$\begin{cases} 2x_0 = \frac{p+1}{2} \\ \\ 2y_0 = \frac{q+1}{2} \end{cases}$$

Ne segue, in particolare, che esiste al più un punto fisso per σ. Siccome σ è una involuzione, il numero di elementi di U che non sono fissati da σ è pari. Quindi, un punto fisso esiste se e solo se $|U| = s + t$ è dispari. D'altra parte, dalle due equazioni che lo caratterizzano, si

conclude che, essendo x_0 e y_0 numeri interi, un punto fisso per σ esiste se e solo se $p \equiv q \equiv 3 \pmod 4$. ■

Ancora sul test di Lucas-Lehmer

Come anticipato a pagina 17, nell'Appendice al Capitolo 1, completiamo la dimostrazione del test di Lucas-Lehmer. Ricordiamo che per ogni $n \geq 1$ abbiamo chiamato $M_n = 2^n - 1$ l'n-esimo numero di Mersenne e definito la sequenza

$$S_1 = 4 \qquad \text{e} \qquad S_{n+1} = S_n^2 - 2.$$

Proviamo quindi che:

Se $n \geq 3$ ed M_n è un numero primo, allora M_n divide S_{n-1}.

Dimostrazione. Per semplicità poniamo $q = M_n$ e ricordiamo che essendo q un primo, necessariamente anche n lo è, in particolare (tenedo conto dell'ipotesi iniziale) n è dispari. Abbiamo allora che

$$\begin{aligned} q = 2^n - 1 = 2 \cdot 2^{2l} - 1 &\equiv 3 \pmod 4 \\ &\equiv 1 \pmod 3 \end{aligned}$$

Quindi $q \equiv 7 \pmod{12}$. Ora, per la Legge di reciprocità quadratica, si ha

$$\left(\frac{3}{q}\right) = (-1)^{\frac{3-1}{2}\frac{q-1}{2}} \left(\frac{q}{3}\right) = -\left(\frac{q}{3}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Inoltre $2^n \equiv 1 \pmod q$ e quindi $2 \equiv 2^{n+1} \equiv (2^{\frac{n+1}{2}})^2 \pmod q$, cioè

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

per il criterio di Eulero. Ne segue che

$$24^{\frac{q-1}{2}} = \left(2^{\frac{q-1}{2}}\right)^3 \cdot \left(3^{\frac{q-1}{2}}\right) \equiv -1 \pmod q. \tag{23}$$

Chiamiamo ora $\mathbb{F} = \mathbb{Z}_q$ ed $\mathbb{E} = \mathbb{F}[\alpha]$ dove α è una radice del polinomio $x^2 - 3 \in \mathbb{F}[x]$. Poichè $\left(\frac{3}{q}\right) = -1$, $\alpha \notin \mathbb{F}$, quindi $x^2 - 3$ è irriducibile in $\mathbb{F}[x]$ ed $\mathbb{E}$ ha grado due su $\mathbb{F}$. Ricordo inoltre che posti $u = 2 + \alpha$ e $v = 2 - \alpha$, nel campo $\mathbb{E}$ si ha

$$uv = 1 \text{ e } u^{2^{n-1}} + v^{2^{n-1}} = S_n.$$

Chiamiamo $\sigma = 2\alpha$ e calcoliamo

$$\begin{aligned} (6+\sigma)^q &= 6^q + \sigma^q = 6^q + 2^q\alpha^q \\ &= 6 + 2\alpha^q = 6 + 2 \cdot (\alpha^2)^{\frac{q-1}{2}} \cdot \alpha \\ &= 6 + 2 \cdot (3)^{\frac{q-1}{2}} \cdot \alpha = 6 + 2 \cdot \left(\frac{3}{q}\right) \cdot \alpha \\ &= 6 - 2\alpha = 6 - \sigma \end{aligned}$$

dove si sono usati il morfismo di Frobenius, il Teorema di Fermat ed il criterio di Eulero. Abbiamo cioè provato che

$$(6+\sigma)^q = 6-\sigma. \tag{24}$$

Inoltre

$$\frac{(6+\sigma)^2}{24} = 2+\alpha = u$$

e pertanto, usando (23) e (24) si ottiene che

$$\begin{aligned} u^{\frac{q+1}{2}} &= \frac{(6+\sigma)^{q+1}}{24^{\frac{q+1}{2}}} = \frac{(6+\sigma)(6+\sigma)^q}{24\cdot 24^{\frac{q-1}{2}}} \\ &= \frac{6+\sigma}{24}\cdot\frac{6-\sigma}{-1} = -\frac{36-\sigma^2}{24} = -1. \end{aligned}$$

Moltiplicando ambo i menbri di questa equazione per $v^{\frac{q+1}{4}}$ e tenendo conto che $uv = 1$, otteniamo

$$u^{\frac{q+1}{2}} v^{\frac{q+1}{4}} = -v^{\frac{q+1}{4}}$$

$$(uv)^{\frac{q+1}{4}} \cdot u^{\frac{q+1}{4}} + v^{\frac{q+1}{4}} = 0$$

$$u^{\frac{q+1}{4}} + v^{\frac{q+1}{4}} = 0$$

cioè

$$u^{2^{n-2}} + v^{2^{n-2}} = 0$$

ovvero $S_{n-1} = 0$ in $\mathbb{E}$, che significa M_n divide S_{n-1}. ■

ESERCIZI

Esercizio 3.1 *Calcolare, usando il Lemma di Gauss,* $\left(\frac{7}{17}\right)$ *e* $\left(\frac{3}{23}\right)$.

Esercizio 3.2 *Sia* $F_n = 2^{2^n}+1$ *l'n-esimo numero di Fermat, e sia* p *un suo divisore primo. Nell'esercizio 2.6 del Capitolo 2 si è provato che* $p \equiv 1 \pmod{2^{n+1}}$. *Usando tale fatto, e la Proposizione 3.1.5, si provi che se* $n \geq 2$, *allora esiste un intero* a *tale che*

$$a^{2^{n+1}} \equiv -1 \pmod{p}$$

e si deduca da questo che $p \equiv 1 \pmod{2^{n+2}}$.

Esercizio 3.3 *Si dica se la congruenza*

$$17x^2 + 28x - 11 \equiv 0 \pmod{503}$$

ammette soluzioni.

Esercizio 3.4 *Si dica se la congruenza*

$$7x^2 + 12x - 19 \equiv 0 \pmod{1067}$$

ammette soluzioni (si faccia attenzione che 1067 *non è un numero primo).*

Esercizio 3.5 *Sia p un primo dispari. Si provi che* 3 *è un residuo quadratico modulo p se e solo se $p \equiv \pm 1 \pmod{12}$.*

Esercizio 3.6 *Si caratterizzino tutti i primi dispari p, tali che* 5 *è un residuo quadratico modulo p.*

Esercizio 3.7 *Si provi che la congruenza*

$$(x^2 - 5)(x^2 - 6) \equiv 0 \pmod{p}$$

è risolubile per ogni primo p.

Esercizio 3.8 *Sia p un primo dispari. Si provi che la congruenza*

$$3x^2 + y^2 \equiv 0 \pmod{p}$$

ha soluzioni non banali (cioè con $x, y \not\equiv 0 \pmod{p}$) se e solo se $p \equiv 1 \pmod{3}$.

Esercizio 3.9 *Siano p un primo dispari ed a un intero non divisibile per p. Si provi che, per ogni $n \geq 1$, a è un R.Q. modulo p^n se e solo se a è un R.Q. modulo p.*

Esercizio 3.10 *Questo esercizio caratterizza i numeri interi positivi n tali che -1 è un R.Q. modulo n. Sia $2 \leq n \in \mathbb{N}$, e denotiamo con $\nu(n)$ il numero di soluzioni distinte (modulo n) della congruenza*

$$x^2 \equiv -1 \pmod{n}.$$

Si provi che $\nu(n) = 0$ se $4|n$ oppure n ha un divisore primo p con $p \equiv 3 \pmod{4}$. Se invece $n = 2^e p_1^{a_1} \cdots p_s^{a_s}$, con $e = 0, 1$, e p_i primi distinti e tali che $p \equiv 1 \pmod{4}$, allora $\nu(n) = 2^s$.

Parte II.

Teoria moltiplicativa

"Fu allora che vidi il Pendolo. La sfera, mobile all'estremità di un lungo filo fissato alla volta del coro, descriveva le sue ampie oscillazioni con isocrona maestà. Io sapevo - ma chiunque avrebbe dovuto avvertire nell'incanto di quel placido respiro - che il periodo era regolato dal rapporto tra la radice quadrata della lunghezza del filo e quel numero π che, irrazionale alle lunari, vina ragione tra le più sure, l'unità del punto di so- una astratta dimensione, la il tetragono segreto del- zione del cerchio."

men- ti sub- ga ne- mente

ra- zionali per di- ferenza

numerazionali per digione necessaria- di tutti

la circon- sibili -

al diametro po di quel

i cerchi pos- sfera dal-

così che il tem- lo era effet-

vagare di una to

l'uno all'altro po-

di una arcana cospi-

intemporali delle mi-

spensione, la dualità di

natura ternaria di π,

la radice, la perfe-

([15])

4 FUNZIONI ARITMETICHE

Nella Matematica, ed in particolare per quanto riguarda la Teoria dei Numeri, siamo spesso interessati a studiare successioni di numeri reali o complessi. Tali successioni vengono semplicemente chiamate *funzioni aritmetiche*.

Inizieremo questo Capitolo definendo l'ambiente di lavoro, ovvero la struttura di anello delle funzioni aritmetiche (dotate dell'usuale somma e del prodotto di convoluzione di Dirichlet). Introdurremo in seguito le funzioni moltiplicative, ed esamineremo in dettaglio le principali funzioni che giocano un ruolo significativo nella divisibilità fra interi e nella distribuzione dei numeri primi.

L'ANELLO DELLE FUNZIONI ARITMETICHE

Definizione 4.1.1 *Una funzione che ha per dominio l'insieme* $\mathbb{N}^*$ *dei numeri naturali positivi e codominio il campo* $\mathbb{C}$ *viene detta* funzione aritmetica.

Indicheremo con $\mathbb{C}^{\mathbb{N}^*}$ l'insieme di tutte le funzioni aritmetiche. Se f e g sono due arbitrari elementi di $\mathbb{C}^{\mathbb{N}^*}$, è possibile definire due nuove funzioni aritmetiche (dette rispettivamente *somma* e *prodotto di convoluzione*), ponendo per ogni $n \in \mathbb{N}^*$,

$$(f+g)(n) = f(n) + g(n),$$
$$(f*g)(n) = \sum_{m|n} f(m)g(n/m).$$

dove la sommatoria viene fatta su tutti i divisori positivi di n.
Introduciamo anche la seguente notazione per indicare le funzioni costanti. Se $z \in \mathbb{C}$, la scrittura in grassetto $\mathbf{z}$ sta a indicare la funzione costante uguale a z. Sia inoltre, δ la funzione di Dirac così definita, per ogni $n \in \mathbb{N}^*$:

$$\delta(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n \geq 2 \end{cases}$$

Riserveremo invece il simbolo id per indicare la funzione identità, $id(n) = n$, per ogni $n \in \mathbb{N}^*$.
È routine provare il seguente

Teorema 4.1.1 *L'insieme delle funzioni aritmetiche* $\mathbb{C}^{\mathbb{N}^*}$*, dotato delle operazioni di somma e prodotto di convoluzione, è un anello commutativo con zero* $\mathbf{0}$ *e unità* δ.

DIMOSTRAZIONE. Esercizio (oppure si veda [4]). ■

Proposizione 4.1.2 *L'insieme degli elementi invertibili di* $\mathbb{C}^{\mathbb{N}^*}$ *è*

$$U(\mathbb{C}^{\mathbb{N}^*}) = \{f \in \mathbb{C}^{\mathbb{N}^*} | f(1) \neq 0\}.$$

DIMOSTRAZIONE. Dal fatto che $f(1)f^{-1}(1) = (f * f^{-1})(1) = \delta(1) = 1$, segue immediatamente l'inclusione $U(\mathbb{C}^{\mathbb{N}^*}) \subseteq \{f | f(1) \neq 0\}$.

Viceversa, supponiamo che f sia una funzione aritmetica tale che $f(1) \neq 0$. Definiamo f^{-1} ricorsivamente.
Poniamo $f^{-1}(1) = 1/f(1)$ e supponiamo che siano definiti i valori $f^{-1}(k)$ per ogni $1 \leq k < n$. L'equazione

$$(f * f^{-1})(n) = \delta(n) = 0$$

può essere scritta come

$$\sum_{m|n} f(n/m)f^{-1}(m) = f(1)f^{-1}(n) + \sum_{\substack{m|n \\ m<n}} f(n/m)f^{-1}(m) = 0.$$

Essendo noti i valori di $f^{-1}(m)$ per ogni $m < n$, esiste un unico valore per $f^{-1}(n)$ ed è dato da

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{\substack{m|n \\ m<n}} f(n/m)f^{-1}(m).$$

Questo ragionamento induttivo prova l'esistenza (e l'unicità) della funzione inversa f^{-1}. ■

FUNZIONI MOLTIPLICATIVE

Definizione 4.2.1 *Una funzione aritmetica* f *si dice* moltiplicativa *se* $f \neq \mathbf{0}$ *e per ogni* $n, m \in \mathbb{N}^*$

$$(m, n) = 1 \quad \textit{implica} \quad f(mn) = f(m)f(n).$$

La moltiplicatività di una funzione consente di determinarne i valori a partire da quelli che assume sulle potenze dei numeri primi. Infatti, se f è una funzione moltiplicativa, e $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, dove i p_i sono primi distinti e gli a_i interi maggiori o uguali a 1, allora chiaramente

$$f(n) = \prod_{i=1}^{k} f(p_i^{a_i}).$$

Osserviamo che se f è una funzione moltiplicativa, allora $f(1) = 1$. Infatti, essendo $f \neq \mathbf{0}$, preso un intero positivo n tale che $f(n) \neq 0$ si ha $f(n) = f(n \cdot 1) = f(n)f(1)$, da cui segue $f(1) = 1$. In particolare, per la Proposizione 4.1.2, ogni funzione moltiplicativa è un elemento invertibile dell'anello $\mathbb{C}^{\mathbb{N}^*}$.

Esempio 4.2.1 Per ogni $z \in \mathbb{C}$, la funzione *potenza* z-esima, definita da

$$f_z(n) = n^z, \quad \forall n \in \mathbb{N}^*$$

è una funzione moltiplicativa.[1]
Si noti che $f_0 = \mathbf{1}$ e $f_1 = id$.

Un fatto estremamente importante è che il prodotto di convoluzione di funzioni moltiplicative è ancora una funzione moltiplicativa.

Teorema 4.2.1 *L'insieme delle funzioni moltiplicative, rispetto al prodotto di convoluzione, è un gruppo (un sottogruppo di $U(\mathbb{C}^{\mathbb{N}^*})$).*
In particolare, se f e g sono due funzioni moltiplicative, allora anche f^{-1} e $f * g$ sono funzioni moltiplicative.

DIMOSTRAZIONE. È banale osservare che δ è una funzione moltiplicativa.
Siano f e g due funzioni moltiplicative e chiamiamo $h = f * g$. Siano inoltre m ed n due interi positivi coprimi. Allora ogni divisore c di mn è della forma $c = ab$ con $a|m$ e $b|n$. Essendo $(a, b) = 1 = (m/a, n/b)$ esiste una corrispondenza biunivoca tra i divisori c di mn e i prodotti ab di questa forma. Pertanto

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m \\ b|n}} f(ab)g(mn/ab) = \sum_{\substack{a|m \\ b|n}} f(a)f(b)g(m/a)g(n/b) \\ &= \sum_{a|m} f(a)g(m/a) \sum_{b|n} f(b)g(n/b) = h(m)h(n). \end{aligned}$$

Sia ora f moltiplicativa e, per assurdo, supponiamo che la sua inversa f^{-1} non sia moltiplicativa. Scegliamo una coppia *minimale* (m, n) di interi positivi coprimi per cui valga

$$f^{-1}(mn) \neq f^{-1}(m)f^{-1}(n). \tag{25}$$

Osserviamo che $mn > 1$. Infatti, essendo f moltiplicativa, si ha che $f(1) = 1$ e quindi da $1 = \delta(1) = f^{-1}(1)f(1)$ segue $f^{-1}(1) = \frac{1}{f(1)} = 1$.
Per la scelta minimale di m, n, per ogni coppia di interi coprimi a, b, con $ab < mn$, vale $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$. Ne segue che

$$\begin{aligned} 0 = \delta(mn) &= \sum_{\substack{a|m \\ b|n \\ ab<mn}} f^{-1}(ab) f\left(\frac{mn}{ab}\right) + f^{-1}(mn)f(1) \\ &= \sum_{\substack{a|m \\ b|n \\ ab<mn}} f^{-1}(a)f^{-1}(b) f\left(\frac{m}{a}\right) f\left(\frac{n}{b}\right) + f^{-1}(mn) \\ &= \sum_{a|m} f^{-1}(a) f\left(\frac{m}{a}\right) \sum_{b|n} f^{-1}(b) f\left(\frac{n}{b}\right) - f^{-1}(m)f^{-1}(n) + f^{-1}(mn) \\ &= \delta(m)\delta(n) - f^{-1}(m)f^{-1}(n) + f^{-1}(mn) \\ &= -f^{-1}(m)f^{-1}(n) + f^{-1}(mn), \end{aligned}$$

1 Si ricorda che se $z = a + ib$ (con $a, b \in \mathbb{R}$) allora $n^z = n^a \cdot (\cos(b \ln n) + i \sin(b \ln n))$.

che contraddice la (25). ■

Le funzioni d e σ

Per ogni numero complesso z definiamo la funzione $\sigma_z = f_z * \mathbf{1}$, ovvero

$$\sigma_z(n) = \sum_{m|n} m^z,$$

per ogni $n \in \mathbb{N}^*$.

In virtù dell'Esempio 4.2.1 e del Teorema 4.2.1, ogni σ_z è una funzione moltiplicativa.

Due casi particolari meritano menzione. Per $z = 0$, la funzione σ_0 viene denotata comunemente con d (o con τ) , ed il valore $d(n)$ rappresenta il numero di divisori positivi di n. Per $z = 1$, la funzione $\sigma := \sigma_1$ rappresenta invece la somma di tutti i divisori positivi di n.

Si osserva che se p è un primo e $a \in \mathbb{N}^*$, allora:

$$d(p^a) = 1 + a \quad \text{e} \quad \sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1}.$$

Possiamo dunque concludere con la seguente

Proposizione 4.2.2 *Sia $n \in \mathbb{N}^*$, e sia $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ la fattorizzazione in primi di n; allora*

$$d(n) = \prod_{i=1}^{k} (1 + a_i) \quad e \quad \sigma(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Numeri perfetti

Un numero $n \in \mathbb{N}^*$ si dice *perfetto* se è uguale alla somma dei suoi divisori *propri*. In altri termini, n è perfetto se e solo se $2n = \sigma(n)$.

Teorema 4.2.3 *[L. Eulero] Un numero pari n è perfetto se e solo se $n = 2^{p-1}(2^p - 1)$, dove p e $2^p - 1$ sono primi.*

Dimostrazione. Supponiamo che sia $n = 2^{p-1}(2^p - 1)$, con p e $2^p - 1$ numeri primi. Allora

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^{p-1+1} - 1}{2 - 1} \cdot (2^p - 1 + 1) = (2^p - 1)2^p = 2n,$$

e dunque n è perfetto.

Viceversa, sia n un numero perfetto pari. Allora $n = 2^{k-1}m$ con $k \geq 2$ e m dispari. Inoltre

$$2^k m = 2n = \sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m). \tag{26}$$

Quindi, $2^k - 1$ divide m. Posto $m = (2^k - 1)m'$, da (26) abbiamo che

$$\sigma(m) = \frac{2^k m}{2^k - 1} = 2^k m' .$$

Poichè m e m' sono distinti ed entrambi dividono m si ha

$$\sigma(m) \geq m + m' = (2^k - 1)m' + m' = 2^k m' = \sigma(m)$$

da cui segue che $m' = 1$ ed $m = 2^k - 1$ è primo; si vede poi facilmente (Proposizione 1.3.2 (2)) che ciò può essere vero solo se $k = p$ è primo. ■

Il Teorema precedente (parzialmente già noto ai matematici greci, e provato definitivamente da Eulero) riconduce quindi la descrizione dei numeri perfetti pari alla determinazione dei primi di Mersenne (ovvero della forma $2^p - 1$, di cui abbiamo parlato nel Capitolo 1, sezione 1.3). In particolare se il numero di primi di Mersenne è finito, allora i numeri perfetti pari sono finiti. Il problema dell'esistenza di numeri perfetti dispari è invece tuttora aperto, anche se la congettura prevalente è che non ve ne siano.

Al giugno 2017, sono stati testati tutti i numeri dispari fino a 10^{15000}. Ochem e Rao [49] e Nielsen [47] hanno provato che un eventuale numero perfetto dispari ammette almeno 101 fattori primi, di cui almeno dieci distinti.

La funzione μ di Möbius

La *funzione di Möbius* (classica) è l'applicazione

$$\mu : \mathbb{N}^* \longrightarrow \{0, 1, -1\} \subset \mathbb{Z}$$

definita nel modo seguente

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se esiste un primo } p \text{ tale che } p^2 | n, \\ (-1)^s & \text{se } n = p_1 p_2 \dots p_s \text{ con i } p_i \text{ primi distinti.} \end{cases}$$

La funzione di Möbius può essere generalizzata in modo da venire definita su insiemi parzialmente ordinati (quella che abbiamo esposto è la versione classica, in cui l'insieme parzialmente ordinato è $\mathbb{N}^*$ con la relazione di divisibilità.)

Dalla definizione, segue immediatamente che μ è una funzione moltiplicativa (ed in particolare invertibile in $(\mathbb{C}^{\mathbb{N}^*}, +, *)$).

Lemma 4.2.4

$$\sum_{m|n} \mu(m) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } n > 1 \end{cases}$$

ovvero:

$$\mu * \mathbf{1} = \delta,$$

cioè l'inversa di μ nell'anello $(\mathbb{C}^{\mathbb{N}^*}, +, *)$ è la funzione costante $\mathbf{1}$.

DIMOSTRAZIONE. Poniamo $g(n) = \sum_{d|n} \mu(d)$. Allora $g = \mu * \mathbf{1}$ è moltiplicativa per il Teorema 4.2.1 e pertanto $g(1) = 1$. Siano p un numero primo e $a \geq 1$; allora

$$\begin{aligned} g(p^a) &= \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^a) \\ &= \mu(1) + \mu(p) = 1 - 1 = 0; \end{aligned}$$

poichè g è moltiplicativa, si conclude che, per ogni $n > 1$, $g(n) = 0$. Pertanto $g = \delta$. ■

L'importanza della funzione di Möbius risiede principalmente nella **Formula di Inversione di Möbius**, la cui dimostrazione, in virtù delle proprietà dell'anello $(\mathbb{C}^{\mathbb{N}^*}, +, *)$, è ora immediata.

Teorema 4.2.5 (Inversione di Möbius) *Sia $f : \mathbb{N}^* \to \mathbb{C}$ una funzione aritmetica. Se $F = f * \mathbf{1}$, allora $f = F * \mu$.*
In altri termini, se per ogni $n \in \mathbb{N}$ definiamo $F(n) = \sum_{m|n} f(m)$, allora vale che

$$f(n) = \sum_{m|n} F(m)\mu(n/m) = \sum_{m|n} \mu(m)F(n/m),$$

per ogni $n \in \mathbb{N}^*$.

DIMOSTRAZIONE.

$$f = f * \delta = f * (\mu^{-1} * \mu) = (f * \mu^{-1}) * \mu = (f * \mathbf{1}) * \mu = F * \mu.$$

■

La funzione ϕ di Eulero

Ricordiamo la definizione di funzione di Eulero data nel Capitolo 2, Sezione 2.1. Assegnato $n \in \mathbb{N}^*$, il valore $\phi(n)$ indica la cardinalità dell'insieme, $U(\mathbb{Z}_n)$, degli elementi invertibili di $\mathbb{Z}_n$, ovvero il numero di interi compresi tra 1 e n che sono coprimi con n:

$$\phi(n) = |\{a \in \mathbb{N}^* \mid a \leq n,\ (a, n) = 1\}|.$$

Lemma 4.2.6 *Valgono le seguenti relazioni*

$$\phi * \mathbf{1} = id \quad e \quad \phi = \mu * id,$$

ovvero, per ogni $n \in \mathbb{N}^*$:

$$\sum_{m|n} \phi(m) = n \quad e \quad \phi(n) = n \sum_{m|n} \frac{\mu(m)}{m}. \tag{27}$$

DIMOSTRAZIONE. Nel Capitolo 2 (Lemma 2.1.4) abbiamo provato che per ogni $n \in \mathbb{N}^*$, vale

$$\sum_{m|n} \phi(m) = n,$$

ovvero la relazione

$$\phi * \mathbf{1} = id.$$

Applicando la formula di inversione di Möbius (Teorema 4.2.5), si completa la dimostrazione del Lemma. ■

Se $n = p$ è un numero primo, il valore di $\phi(p)$ è $p - 1$. Mentre se $n = p^a$, allora un numero r (compreso tra 1 ed n) è comprimo con n se e solo se p non divide r, pertanto se e solo se r non appartiene alla sequenza: $p, 2p, 3p, \ldots, p^{a-1}p$, quindi

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

Ne segue il seguente

Teorema 4.2.7 *Per ogni $n \in \mathbb{N}^*$, se $p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ è la fattorizzazione in potenze di primi distinti di n, allora*

$$\phi(n) = n \cdot \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right). \tag{28}$$

Proposizione 4.2.8 (P. Erdös) *Per ogni $n \in \mathbb{N}^*$ esiste un intero m tale che $n! = \phi(m)$.*

DIMOSTRAZIONE. Notiamo che

$$\prod_{p \leq n} (p - 1) \mid n!.$$

Posto $n! = \prod_{p \leq n} p^{a_p}$, con $a_p := v_p(n!)$ interi positivi, abbiamo che

$$\frac{n!}{\prod_{p \leq n}(p-1)} = \prod_{p \leq n} p^{b_p},$$

dove $b_p \geq 0$. Sia ha allora che l'intero $m := \prod_{p \leq n} p^{b_p + 1}$ è una retroimmagine di $n!$, tramite ϕ, infatti

$$\phi(m) = \prod_{p \leq n} (p-1) \cdot \prod_{p \leq n} p^{b_p} = n!$$

il che completa la dimostrazione. ■

Nella parte restante del Capitolo, introduciamo alcune importanti funzioni aritmetiche (non moltiplicative).

LA FUNZIONE Λ DI MANGOLDT

La funzione Λ *di Mangoldt* è definita ponendo per ogni $n \in \mathbb{N}^*$,

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^k \text{ per qualche primo } p \text{ e } k \geq 1, \\ 0 & \text{altrimenti.} \end{cases}$$

Questa funzione ha una rilevanza storica fondamentale, in quanto è strettamente legata alla successione dei numeri primi (si vedano i Capitoli 6 e 8).

Di seguito ci limitiamo a provare il seguente Lemma, di cui faremo spesso uso.

Lemma 4.3.1 *Valgono:*

$$\log = \Lambda * \mathbf{1} \quad e \quad \Lambda = \mu * \log,$$

ovvero, per ogni $n \in \mathbb{N}^*$,

$$\sum_{m|n} \Lambda(m) = \log n \quad e \quad \Lambda(n) = -\sum_{m|n} \mu(m) \log m.$$

Dimostrazione. Sia $n = \prod_{p|n} p^{v_p(n)}$. allora

$$\log n = \sum_{p|n} v_p(n) \log p = \sum_{p^i|n} \log p = \sum_{m|n} \Lambda(m) = (\Lambda * \mathbf{1})(n).$$

Applicando la formula di inversione di Möbius (Teorema 4.2.5) si ottiene

$$\Lambda = \mu * \log,$$

ovvero:

$$\begin{aligned} \Lambda(n) &= \sum_{m|n} \mu(m) \log\left(\frac{n}{m}\right) \\ &= \sum_{m|n} \mu(m) \left(\log n - \log m\right) \\ &= \log n \sum_{m|n} \mu(m) - \sum_{m|n} \mu(m) \log m \\ &= -\sum_{m|n} \mu(m) \log m, \end{aligned}$$

ricordando che, per $n > 1$, $\sum_{m|n} \mu(m) = 0$. ∎

DA EULERO ALLA ZETA

Nell'Appendice al Capitolo 1 abbiamo accennato alla seguente formula dimostrata da L. Eulero intorno al 1737

$$\sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{29}$$

valida per ogni numero reale $s > 1$.

Vediamone ora in dettaglio la dimostrazione.
Per ogni numero reale u, con $|u| < 1$, abbiamo che

$$\frac{1}{1-u} = 1 + u + u^2 + \ldots + u^n + \ldots = \sum_{h=0}^{\infty} u^h.$$

Pertanto

$$\prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p\in\mathbb{P}} \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} \ldots\right),$$

e se espandiamo il prodotto di destra, notiamo che il generico termine è della forma

$$\frac{1}{p_1^{a_1 s} \ldots p_k^{a_k s}} = \frac{1}{(p_1^{a_1} \ldots p_k^{a_k})^s}.$$

La formula (29) segue allora dal Teorema Fondamentale dell'Aritmetica (Teorema 1.2.3).

Questo ragionamento (e la conseguente formula) si estende facilmente ad ogni s *numero complesso con parte reale* $\Re(s) > 1$.

Definizione 4.4.1 *Ogni espansione di una serie di Dirichlet, ovvero della forma* $\sum_n \frac{a_n}{n^s}$*, tramite un prodotto infinito indicizzato sull'insieme dei numeri primi, viene (informalmente) chiamato* prodotto di Eulero.

L'esempio dell'equazione (29) è il più celebre fra tutti i prodotti di Eulero, e permette di introdurre una fra le più importanti funzioni aritmetiche: la funzione "zeta".

LA FUNZIONE ζ DI RIEMANN

La funzione *Zeta di Riemann* ζ è definita per numeri complessi s tali che $\Re(s) > 1$ da

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}\,.$$

Si noti che la definizione è ben posta, in quanto se $s = a + ib$, con $a = \Re(s)$ e $b = \Im(s)$, essendo $a > 1$:

$$\left|\frac{1}{n^s}\right| = \frac{1}{n^a} < \frac{1}{n}$$

e pertanto la serie è assolutamente convergente.

È possibile estendere in modo analitico la funzione $\zeta(s)$ a tutti i numeri complessi $s \neq 1$, chi fosse interessato può consultare [4], Theorem 12.5.

Lemma 4.5.1 *Se* $1 < s \in \mathbb{R}$*, allora*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\,.$$

DIMOSTRAZIONE. Poichè $s > 1$ la serie $\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$ è assolutamente convergente. Quindi

$$\begin{aligned}\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} &= \left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right)\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) \\ &= \sum_{m,n=1}^{\infty} \frac{\mu(n)}{(mn)^s} = \sum_{t=1}^{\infty} \frac{1}{t^s}\left(\sum_{n|t} \mu(n)\right).\end{aligned}$$

Ricordando il Lemma 4.2.4, possiamo scrivere

$$\zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1$$

che è quello che si voleva. ■

Presentiamo una dimostrazione (tratta da [29]) del seguente importante risultato, congetturato ma non dimostrato da Eulero (si veda anche [3]).

Teorema 4.5.2

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

DIMOSTRAZIONE. Ricordando che $\sin x = 2 \sin \frac{x}{2} \cos \frac{x}{2}$, si ottiene la seguente identità,

$$\begin{aligned}\frac{1}{\sin^2 x} &= \frac{1}{4 \sin^2 \frac{x}{2} \cos^2 \frac{x}{2}} \\ &= \frac{1}{4}\left(\frac{1}{\sin^2 \frac{x}{2}} + \frac{1}{\cos^2 \frac{x}{2}}\right) \\ &= \frac{1}{4}\left(\frac{1}{\sin^2 \frac{x}{2}} + \frac{1}{\sin^2 \frac{\pi+x}{2}}\right).\end{aligned}$$

In particolare,

$$1 = \frac{1}{\sin^2 \frac{\pi}{2}} = \frac{1}{4}\left(\frac{1}{\sin^2 \frac{\pi}{4}} + \frac{1}{\sin^2 \frac{3\pi}{4}}\right).$$

Applicando ripetutamente questa uguaglianza, per induzione su n, si prova che, per ogni $n \geq 2$,

$$\begin{aligned}1 &= \frac{1}{4^n} \sum_{k=0}^{2^n-1} \frac{1}{\sin^2 \frac{(2k+1)\pi}{2^{n+1}}} \\ &= \frac{1}{4^n}\left(\sum_{k=0}^{2^{n-1}-1} \frac{1}{\sin^2 \frac{(2k+1)\pi}{2^{n+1}}} + \sum_{k=2^{n-1}}^{2^n-1} \frac{1}{\sin^2 \frac{(2k+1)\pi}{2^{n+1}}}\right) \\ &= \frac{2}{4^n} \sum_{k=0}^{2^{n-1}-1} \frac{1}{\sin^2 \frac{(2k+1)\pi}{2^{n+1}}}. \qquad (30)\end{aligned}$$

Ora, per $0 < x < \pi/2$, si ha $\sin x < x < \tan x$, e quindi

$$\frac{1}{\sin^2 x} > \frac{1}{x^2} > \frac{1}{\tan^2 x} = \frac{1}{\sin^2 x} - 1.$$

Ponendo $N = 2^n$, e $x_k = (2k+1)\pi/2N$, con $k = 0, 1, \ldots, N/2 - 1$, nelle disuguaglianze di sopra e applicando la (30), si ottiene:

$$1 > \frac{8}{\pi^2} \sum_{k=0}^{N/2-1} \frac{1}{(2k+1)^2} > 1 - \frac{1}{N}.$$

Passando al limite per $n \to \infty$ si ottiene,

$$1 = \frac{8}{\pi^2} \sum_{k=0}^{\infty} \frac{1}{(2k+1)^2}.$$

Da tale identità segue quella per $\zeta(2)$. Infatti

$$\zeta(2) = \sum_{u=1}^{\infty} \frac{1}{u^2} = \sum_{k=0}^{\infty} \frac{1}{(2k+1)^2} + \sum_{k=1}^{\infty} \frac{1}{(2k)^2} = \frac{\pi^2}{8} + \frac{1}{4}\zeta(2),$$

e quindi $\zeta(2) = \pi^2/6$. ■

Lemma 4.5.3

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2}\,.$$

DIMOSTRAZIONE. L'uguaglianza discende immediatamente dal Lemma 4.5.1 e il Teorema 4.5.2. ■

APPENDICE

Amicable Pairs e problema di Catalan-Dickson

Per ogni naturale n, poniamo

$$\sigma^*(n) = \sigma(n) - n = \sum_{\substack{m|n \\ m \neq n}} m$$

e definamo $\sigma^*(0) = 0$.

Una coppia di interi positivi (m, n) si dice *amicable pair* se

$$\sigma^*(m) = n \quad \text{e} \quad \sigma^*(n) = m$$

o, equivalentemente se

$$\sigma(m) = \sigma(n) = m + n.$$

Coppie di questo tipo erano già note ai Pitagorici e una prima formula in grado di generare amicable pairs la si deve a Thābit ibn Qurra (850 d.C.), formula poi riscoperta da P. de Fermat.
La più piccola coppia di numeri di questo tipo è $(220, 284)$ e a giugno 2017 sono note ben 1.220.319.238 amicable pairs.

https://sech.me/ap/index.html fornisce un ampio database e i source codes dei più moderni algoritmi utilizzati.

Rimane un interessante problema matematico aperto dimostrare che queste coppie sono in numero infinito, si sa comunque che la loro densità (in $\mathbb{N}^*$) è zero ([18]).

Per ogni $n \in \mathbb{N}^*$, la successione, $\{S_k(n)\}_k$, delle *aliquote* di n è definita induttivamente da

$$\begin{cases} S_0(n) = n, \\ S_k(n) = \sigma^*(S_{k-1}(n)) \end{cases}$$

Poiché i numeri naturali possono essere perfetti ($n = \sigma^*(n)$), difettivi ($n > \sigma^*(n)$) o abbondanti ($n < \sigma^*(n)$), la successione delle aliquote può oscillare a piacere. Tuttavia, se n è un numero perfetto, allora $S_k(n) = n$ per ogni k, cioè la successione delle aliquote è costante; mentre se (m, n) è una amicable pair allora $S_{2h}(n) = n$ e $S_{2h+1}(n) = m$, cioè $\{S_k(n)\}_k$ oscilla con periodo 2. La seguente congettura è tuttora aperta

Congettura di Catalan-Dickson *Per ogni numero naturale positivo n la successione $\{S_k(n)\}_k$ è definitivamente periodica.*

Il più piccolo numero di cui è ancora ignota la sequenza delle aliquote è 276.

L'ipotesi di Riemann

**** In preparazione. ****

ESERCIZI

Esercizio 4.1 *Si provi che per ogni $n \geq 1$, $d(n) < 2\sqrt{n}$.*

Esercizio 4.2 *Si provi che per ogni $n \geq 1$*

$$\sum_{m|n} (d(m))^3 = \left(\sum_{m|n} d(m) \right)^2$$

Esercizio 4.3 *Si provi che per ogni $n \geq 1$*

$$\prod_{m|n} m = n^{\frac{d(n)}{2}}$$

Esercizio 4.4 *Le celle di una prigione sono numerate da* 1 *a* 100 *e le loro porte sono controllate da un pulsante centrale. Quando viene premuto, il pulsante attiva* alcune *delle porte, aprendole se sono chiuse, chiudendole se aperte. Partendo dallo stato in cui tutte le porte sono chiuse il pulsante viene premuto* 100 *volte, attivando alla k-esima pressione tutte e sole le porte che sono numerate con un multiplo di k. Quali porte saranno aperte alla fine?*

Esercizio 4.5 *Provare che se $\sigma(n)$ è dispari, allora $n = a^2$ oppure $n = 2a^2$, per qualche $a \in \mathbb{N}$.*

Esercizio 4.6 *(Olimpiadi Matematiche 1998) Sia $k \in \mathbb{N}^*$. Provare che esiste $n \in \mathbb{N}$ tale che*

$$\frac{d(n^2)}{d(n)} = k$$

se e solo se k è dispari.

Esercizio 4.7 *Si provi che l'ultima cifra dello sviluppo decimale di un numero perfetto pari è 6 o 8.*

Esercizio 4.8 *Si provi che se n è un numero perfetto dispari, allora n è diviso da almeno 3 primi distinti.*

Esercizio 4.9 *Fissato un intero $k \geq 2$, si dice che n è k-perfetto se $\sigma(n) = kn$. Si determinino tutti i numeri naturali n che sono 3-perfetti, con $1 \leq n \leq 150$.*

Esercizio 4.10 *Sia f una funzione aritmetica e sia F la funzione definita da $F(n) = \sum_{d|n} f(d)$, per ogni $n \in \mathbb{N}^*$. Allora f è moltiplicativa se e solo se lo è F.*

Esercizio 4.11 *Si dimostrino le seguenti proprietà della funzione di Möbius*

1. $\sum_{d^2|n} \mu(d) = |\mu(n)|$.
2. $\sum_{i \leq n} \mu(i)\lfloor n/i \rfloor = 1$ *e quindi* $\left|\sum_{i \leq n}(\mu(i)/i)\right| \leq 1$.

Esercizio 4.12 *(La funzione λ di Liouville). Dato $n \in \mathbb{N}^*$, poniamo $v(1) = 0$, e per $n > 1$, $v(n)$ uguale al numero di fattori primi (non necessariamente distinti) di n, ovvero $v(n) = \sum_{p|n} v_p(n)$. La funzione λ di Liouville è definita da*

$$\lambda(n) = (-1)^{v(n)} .$$

1. *Si provi che λ è moltiplicativa, e che per ogni $n \in \mathbb{N}^*$,*

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se } n \text{ è un quadrato,} \\ 0 & \text{altrimenti.} \end{cases}$$

2. *Si determini l'inversa di λ in $U(\mathbb{C}^{\mathbb{N}^*})$.*

Esercizio 4.13 *Si provi che per ogni $n \in \mathbb{N}^*$,*

$$\sum_{d|n} |\mu(d)| = 2^{v(n)} .$$

Esercizio 4.14 *Si provi che, per ogni $n \geq 2$,*

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

dove p varia nell'insieme dei numeri primi che dividono n.

Esercizio 4.15 *Si provi che, per ogni $n \geq 2$,*

$$\sum_{t \leq n,\, (t,n)=1} t = \frac{1}{2} n \phi(n) .$$

Esercizio 4.16 *Si provi che la disuguaglianza $\phi(x) \geq x - \sqrt{x}$ ha come sole soluzioni intere i numeri p e p^2, con p primo.*

Esercizio 4.17 *Si provi che, per ogni $n \in \mathbb{N}^*$,*

$$\sum_{m=1}^{n} \phi(m) \left\lfloor \frac{n}{m} \right\rfloor = \frac{n(n+1)}{2} .$$

Esercizio 4.18 *Per ogni $n \in \mathbb{N}^*$ sia $F(n) = \sum_{t \leq n}(n,t)$.*

1. *Si provi che $F(n)$ è una funzione moltiplicativa.*
2. *Per $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ si dia una esplicita espressione di $F(n)$.*
3. *Si provi che, per ogni $n \in \mathbb{N}^*$,*

$$\phi(n) = \sum_{m|n} \mu(m) F(n/m) m.$$

4. *Si provi che, per ogni $n \in \mathbb{N}^*$,*

$$n\tau(n) = \sum_{m|n} F(m).$$

Esercizio 4.19 *[L. Eulero] Siano n, m numeri interi con $n > m > 0$ e p, q ed r tre numeri primi tali che*

$$\begin{aligned} p &= 2^m(2^{n-m} + 1) - 1, \\ q &= 2^n(2^{n-m} + 1) - 1, \\ r &= 2^{m+n}(2^{n-m} + 1)^2 - 1 \end{aligned}$$

si provi che $(2^n pq, 2^n r)$ è una amicable pair.

L'animale terrestre più veloce è il ghepardo che per brevi tratti può raggiungere una velocità di 120 *km/h. L'uccello più veloce in picchiata è il falco pellegrino, che è stato cronometrato a velocità di* 324 *km/h. Il mammifero acquatico più veloce è l'orca, che raggiunge velocità di* 55,5 *km/h. L'animale più lento in assoluto è il bradipo, che raggiunge velocità di* 0,05 *km/h. L'uomo più veloce di sempre è il giamaicano Usain Bolt, che il 16 agosto 2009 a Berlino ha corso i* 100 *metri in* 9,58 *secondi* [65].

5 MEDIE

In questo Capitolo analizziamo il comportamento all'infinito di alcune fra le funzioni aritmetiche che sono state introdotte nel Capitolo precedente.

Premettiamo innazitutto che la maggior parte di queste funzioni ha un andamento che sembra sfuggire ad ogni concetto di regolarità; si pensi ad esempio alla funzione $d(n)$, che assume il valore 2 infinite volte (quando n è un numero primo), ed al contempo raggiunge valori arbitrariamente grandi (ogni volta che n possiede tanti divisori).

Assegnata una funzione aritmetica f, risulta quindi spesso più utile studiare la cosiddetta *media (aritmetica)*, definita da

$$F(n) = \frac{1}{n} \sum_{k=1}^{n} f(k),$$

la quale ha sicuramente una regolarità maggiore di f.

Dopo aver introdotto la notazione di base e provato alcuni Lemmi tecnici, calcoleremo alcune (fra cui quelle delle funzioni ϕ e d) e vedremo importanti conseguenze di questi risultati.

Notazioni

Richiamiamo alcune notazioni convenzionalmente usate per lo studio del comportamento asintotico.

Siano f e g due funzioni a valori complessi (non necessariamente aritmetiche). Diremo che

- $f(x) = o(g(x))$ [da leggersi "f è un o-piccolo di g"] se
$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

- $f(x) = O(g(x))$ ["f è un o-grande di g"] se la funzione $f(x)/g(x)$ è definitivamente limitata, cioè se esistono $x_0 > 0$ e $K > 0$ tale che
$$|f(x)| \leq K\,|g(x)| \quad \text{per ogni } x \geq x_0.$$

- $f(x) \sim g(x)$ ["f è asintotica a g"] se
$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Altri simboli spesso usati, quando f, g hanno valori reali positivi, sono

- Se $f(x) \ll g(x)$, se esiste $K > 0$ tale che, definitivamente rispetto ad x:
$$f(x) \leq Kg(x).$$
- $f(x) \gg g(x)$ se $g(x) \ll f(x)$.
- $f(x) \asymp g(x)$ [f e g "hanno ugual ordine di grandezza"] se $f(x) \ll g(x)$ e $f(x) \gg g(x)$, cioè se esistono $K_1, K_2 > 0$ tali che
$$K_1 \cdot g(x) \leq f(x) \leq K_2 \cdot g(x),$$
per ogni x sufficientemente grande.

ABEL SUMMATION FORMULA

Elenchiamo alcune tecniche che utilizzeremo spesso.

Proposizione 5.1.1 *Sia f una funzione aritmetica. Per ogni reale $x \geq 1$, sia*
$$F(x) = \sum_{n \leq x} f(n).$$

1. *(Somme per parti.) Se g è una funzione aritmetica e $a, b \in \mathbb{N}$ con $a < b$, allora*
$$\sum_{n=a+1}^{b} f(n)g(n) = F(b)g(b) - F(a)g(a+1) + - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)).$$
2. *(Abel Summation Formula.) Se g è una funzione continua definita dall'intervallo reale $[1, +\infty)$ in $\mathbb{C}$ e derivabile in $(1, +\infty)$, allora*
$$\sum_{n \leq x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)\,dt. \tag{31}$$

Dimostrazione. 1. La prima uguaglianza è un semplice calcolo, tenendo conto che, per ogni $n \geq 2$, $f(n) = F(n) - F(n-1)$:
$$\begin{aligned}\sum_{n=a+1}^{b} f(n)g(n) &= \sum_{n=a+1}^{b} (F(n) - F(n-1))g(n) \\ &= \sum_{n=a+1}^{b} F(n)g(n) - \sum_{n=a}^{b-1} F(n)g(n+1) \\ &= F(b)g(b) - F(a)g(a+1) + \\ &\qquad - \sum_{n=a+1}^{b-1} F(n)(g(n+1) - g(n)).\end{aligned}$$

2. Poniamo $N = \lfloor x \rfloor$. Allora per quanto appena dimostrato

$$\sum_{n \le N} f(n)g(n) = F(N)g(N) - \sum_{n=1}^{N-1} F(n)\big(g(n+1) - g(n)\big).$$

Osserviamo che $g(n+1) - g(n) = \int_n^{n+1} g'(t)\,dt$, per ogni $n = 1, 2, \ldots, N-1$, e che la funzione $F(t)$ è costante in ogni intervallo reale della forma $[n, n+1)$. Pertanto abbiamo che

$$\begin{aligned}
\sum_{n \le N} f(n)g(n) &= F(N)g(N) - \sum_{n=1}^{N-1} F(n) \int_n^{n+1} g'(t)\,dt \\
&= F(N)g(N) - \sum_{n=1}^{N-1} \int_n^{n+1} F(t)g'(t)\,dt \\
&= F(N)g(N) - \int_1^N F(t)g'(t)\,dt
\end{aligned}$$

e questo prova la formula quando $x = N$ è un intero.
Nel caso generale, basta osservare che il membro di sinistra dell'equanzione (31) non cambia se rimpiazziamo N con x. Vediamo cosa succede al valore di destra. Poiché $F(t)$ è costante su $[N, x)$, otteniamo

$$\begin{aligned}
F(x)g(x) - \int_1^x F(t)g'(t)\,dt &= \\
&= F(x)g(x) - \int_1^N F(t)g'(t)\,dt - \int_N^x F(t)g'(t)\,dt \\
&= F(x)g(x) - \int_1^N F(t)g'(t)\,dt - F(N)\int_N^x g'(t)\,dt \\
&= F(x)g(x) - \int_1^N F(t)g'(t)\,dt - F(N)\big(g(x) - g(N)\big) \\
&= F(N)g(N) - \int_1^N F(t)g'(t)\,dt
\end{aligned}$$

il che completa la dimostrazione. ∎

Riserveremo la parte restante di questo Capitolo per trovare importanti stime di alcune funzioni aritmetiche e loro medie.

Lemma 5.1.2 *Per x reale, $x \ge 1$,*

$$\sum_{n \le x} \log n = x \log x - x + O(\log x).$$

DIMOSTRAZIONE. Applichiamo Abel Summation Formula (Proposizione 5.1.1) con $f = \mathbf{1}$ e $g(t) = \log t$. Abbiamo che

$$F(x) = \sum_{n \le x} 1 = \lfloor x \rfloor,$$

e $g'(t) = 1/t$. Pertanto

$$\begin{aligned}\sum_{n\le x} \log n &= \lfloor x\rfloor \log x - \int_1^x \frac{\lfloor t\rfloor}{t}\,dt\\ &= (x-\{x\})\log x - \int_1^x \frac{t-\{t\}}{t}\,dt\\ &= x\log x + O(\log x) - \int_1^x dt + \int_1^x \frac{\{t\}}{t}\,dt\\ &= x\log x + O(\log x) - (x-1) + O\left(\int_1^x \frac{dt}{t}\right)\\ &= x\log x - x + O(\log x)\end{aligned}$$

ed il Lemma è provato. ■

Il seguente Lemma ci servirà nel Capitolo 8 per dimostrare Teorema di Dirichlet.

Lemma 5.1.3 *Esiste una costante K tale che, per $x \ge 1$,*

$$\sum_{n\le x} n^{-\frac{1}{2}} = 2\sqrt{x} + K + O(x^{-\frac{1}{2}}).$$

Dimostrazione. Per ogni numero reale $t \ge 1$, sia al solito $\{t\} = t - \lfloor t\rfloor$ la sua parte frazionaria. Poiché $0 \le \{t\} < 1$, abbiamo che l'integrale

$$\int_1^\infty \{t\}\, t^{-\frac{3}{2}}\,dt$$

esiste finito. Infatti

$$0 < \int_1^\infty \{t\}\, t^{-\frac{3}{2}}\,dt < \int_1^\infty t^{-\frac{3}{2}}\,dt = 2.$$

Poniamo quindi

$$K = -1 - \frac{1}{2}\int_1^\infty \{t\}\, t^{-\frac{3}{2}}\,dt.$$

Applichiamo la Proposizione 5.1.1, con $f(n) = 1$ e $g(t) = t^{-\frac{1}{2}}$. Allora, per ogni $x \in \mathbb{R}$, $x \ge 1$, $F(x) = \lfloor x\rfloor$ e quindi

$$\begin{aligned}\sum_{n\le x} n^{-\frac{1}{2}} &= \frac{\lfloor x\rfloor}{\sqrt{x}} + \frac{1}{2}\int_1^x \lfloor t\rfloor t^{-\frac{3}{2}}\,dt\\ &= \frac{\lfloor x\rfloor}{\sqrt{x}} + \frac{1}{2}\int_1^x (t-\{t\})t^{-\frac{3}{2}}\,dt\\ &= \frac{\lfloor x\rfloor}{\sqrt{x}} + \frac{1}{2}\int_1^x t^{-\frac{1}{2}}\,dt - \frac{1}{2}\int_1^x \{t\}\, t^{-\frac{3}{2}}\,dt\\ &= \sqrt{x} - \frac{\{x\}}{\sqrt{x}} + \sqrt{x} - 1 - \frac{1}{2}\int_1^x \{t\}\, t^{-\frac{3}{2}}\,dt.\end{aligned}$$

Dunque, con la notazione prima introdotta,

$$\sum_{n\le x} n^{-\frac{1}{2}} = 2\sqrt{x} - \frac{\{x\}}{\sqrt{x}} + K + \frac{1}{2}\int_x^\infty \{t\}\, t^{-\frac{3}{2}}\,dt,$$

e poiché

$$0 < \frac{1}{2}\int_x^\infty \{t\}\, t^{-\frac{3}{2}}\, dt < \frac{1}{2}\int_x^\infty t^{-\frac{3}{2}}\, dt = \frac{1}{\sqrt{x}}$$

si ottiene il risultato dell'enunciato. ■

La costante di Eulero-Mascheroni

Si tratta di una costante estremamente importante nella Teoria dei Numeri e può essere definta in vari modi. Noi daremo la seguente

Definizione 5.1.1 *La* costante di Eulero-Mascheroni *è la quantità*

$$\gamma := 1 - \int_1^{+\infty} \frac{\{t\}}{t^2} dt.$$

Si noti che, poichè $0 \leq \{t\} = t - \lfloor t \rfloor < 1$, γ risulta ben definita e appartiene all'intervallo $(0, 1)$. Un valore approssimato di tale costante è $0,57721$. È un problema classico, tuttora aperto, stabilire se γ sia razionale o irrazionale.

Se $\gamma = a/b \in \mathbb{Q}$, con $(a, b) = 1$, allora $b > 10^{242080}$ (si veda [27]).

Teorema 5.1.4 *Per x reale, $x \to +\infty$,*

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + O\Big(\frac{1}{x}\Big) \tag{32}$$

Dimostrazione. Applichiamo Abel Summation Formula (Proposizione 5.1.1) con $f = \mathbf{1}$ e $g(t) = 1/t$. Abbiamo che

$$F(x) = \sum_{n \leq x} 1 = \lfloor x \rfloor,$$

e $g'(t) = -1/t^2$. Pertanto

$$\begin{aligned}
\sum_{n \leq x} \frac{1}{n} &= \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2}\, dt \\
&= \frac{x - \{x\}}{x} + \int_1^x \frac{t - \{t\}}{t^2}\, dt \\
&= 1 + O\left(\frac{1}{x}\right) + \int_1^x \frac{dt}{t} - \int_1^x \frac{\{t\}}{t^2}\, dt \\
&= 1 + O\left(\frac{1}{x}\right) + \left(\log t\Big|_{t=1}^{t=x}\right) - \left(\int_1^\infty \frac{\{t\}}{t^2}\, dt - \int_x^\infty \frac{\{t\}}{t^2}\, dt\right) \\
&= \log x + \gamma + O\left(\frac{1}{x}\right) + \int_x^\infty \frac{\{t\}}{t^2}\, dt \\
&= \log x + \gamma + O\left(\frac{1}{x}\right) + O\left(\int_x^\infty \frac{dt}{t^2}\right) \\
&= \log x + \gamma + O\left(\frac{1}{x}\right),
\end{aligned}$$

quando x tende a $+\infty$. ■

Nel Capitolo precedente abbiamo definito la funzione $\zeta(s)$ di Riemann per ogni valore complesso s con parte reale $\Re(s) > 1$. Il seguente Teorema fornisce una definizione equivalente a quella data a pagina 75, da cui è esplicita l'estensione naturale di $\zeta(s)$ ad una funzione analitica definita per ogni $s \in \mathbb{C} \setminus \{1\}$ con $\Re(s) > 0$.

Teorema 5.1.5 *Se $s \in \mathbb{C}$ con $\Re(s) > 1$, allora*

$$\zeta(s) = \frac{s}{s-1} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt \tag{33}$$

Dimostrazione. Sia x un numero reale positivo. Applichiamo Abel Summation Formula (Proposizione 5.1.1) con $f = \mathbf{1}$ e $g(t) = \frac{1}{t^s}$. Abbiamo che

$$\sum_{n\le x} \frac{1}{n^s} = \frac{\lfloor x \rfloor}{x^s} + s\int_1^x \frac{\lfloor t \rfloor}{t^{s+1}}\,dt.$$

Mandando $x \longrightarrow \infty$, si ottiene

$$\begin{aligned}
\zeta(s) &= 0 + s\int_1^\infty \frac{\lfloor t \rfloor}{t^{s+1}}\,dt \\
&= s\int_1^\infty \frac{t - \{t\}}{t^{s+1}}\,dt \\
&= s\int_1^\infty \frac{dt}{t^s} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt \\
&= s\left(\frac{t^{1-s}}{1-s}\Big|_1^\infty\right) - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt \\
&= \frac{s}{s-1} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt,
\end{aligned}$$

che completa la dimostrazione. ■

Si osserva che l'integrale improprio $\int_1^\infty \frac{\{t\}}{t^{s+1}}\,dt$ converge assolutamente per ogni $s \neq 1$ con $\Re(s) > 0$, pertanto è possibile adottare la formula (33) come definizione per la funzione ζ su questo dominio. Si noti che ζ è una funzione analitica.

CONVOLUZIONE GENERALIZZATA E "DIVISOR SUM IDENTITY"

In questa sezione estendiamo il concetto di prodotto di convoluzione, introdotto in 4.1. Denotiamo con $\mathcal{B}$ l'insieme delle funzioni a valori complessi, definite sulla semiretta reale $(0, +\infty)$ e che si annullano nell'intervallo $(0, 1)$, ovvero:

$$\mathcal{B} = \left\{k \in \mathbb{C}^{(0,+\infty)} | k(x) = 0 \text{ se } x \in (0,1)\right\}.$$

Sia inoltre $\mathcal{A} = \mathbb{C}^{\mathbb{N}^*}$ l'insieme delle funzioni aritmetiche.
Se $f \in \mathcal{A}$ e $k \in \mathcal{B}$ definiamo, per ogni $x \in (0, +\infty)$:

$$(f \star k)(x) = \sum_{n \leq x} f(n) k\Big(\frac{x}{n}\Big).$$

Notiamo che $f \star k \in \mathcal{B}$ e pertanto è ben definita la seguente operazione:

$$\begin{aligned} \star : \mathcal{A} \times \mathcal{B} &\longrightarrow \mathcal{B} \\ (f, k) &\longmapsto f \star k \end{aligned}$$

Nel caso in cui $k(x) = 0$ per ogni $x \notin \mathbb{N}^*$, la restrizione di k a $\mathbb{N}^*$ (che continueremo a chiamare k) è una funzione aritmetica, ovvero un elemento di $\mathcal{A}$, e si osserva banalmente che

$$(f \star k)(n) = (f * k)(n)$$

per ogni intero $n \geq 1$; pertanto l'operazione $\star$ può essere considerata una generalizzazione del prodotto di convoluzione $*$, definito a pagina 67.

Esiste una relazione di "pseudo-associatività" che lega le operazioni $*$ e $\star$, ed è espressa dalla seguente

Proposizione 5.2.1 *Assegnate arbitrariamente due funzioni aritmetiche f, g ed una funzione $k \in \mathcal{B}$, si ha che:*

$$f \star (g \star k) = (f * g) \star k.$$

DIMOSTRAZIONE. Per ogni x un numero reale positivo, si ha:

$$\begin{aligned} (f \star (g \star k))(x) &= \sum_{n \leq x} f(n)\,(g \star k)\left(\frac{x}{n}\right) \\ &= \sum_{n \leq x} f(n) \sum_{m \leq x/n} g(m) k\Big(\frac{x}{mn}\Big) \\ &= \sum_{mn \leq x} f(n) g(m) k\Big(\frac{x}{mn}\Big) \\ &= \sum_{t \leq x} \Big(\sum_{n \mid t} f(n) g\Big(\frac{t}{n}\Big)\Big) k\Big(\frac{x}{t}\Big) \\ &= \sum_{t \leq x} (f * g)(t) k\Big(\frac{x}{t}\Big) \\ &= ((f * g) \star k)(x). \end{aligned}$$

Questo completa la dimostrazione. ∎

Il seguente principio è spesso molto utile per il calcolo delle sommatorie.

Teorema 5.2.2 *(Divisor Sum Identity) Siano f e g due funzioni aritmetiche e sia $h = f * g$. Dette rispettivamente*

$$F(x) = \sum_{n \le x} f(n), \quad G(x) = \sum_{n \le x} g(n) \quad e \quad H(x) = \sum_{n \le x} h(n),$$

si ha

$$H(x) = \sum_{n \le x} f(n) G\left(\frac{x}{n}\right) = \sum_{n \le x} g(n) F\left(\frac{x}{n}\right).$$

Dimostrazione. Per ogni $x \in (0, +\infty)$ sia

$$U(x) = \begin{cases} 0 & \text{se } 0 < x < 1 \\ 1 & \text{altrimenti.} \end{cases}$$

Allora $U \in \mathcal{B}$ e $F = f \star U$, $G = g \star U$ e $H = h \star U$.
Applicando la Proposizione 5.2.1 e la commutatività di $*$, otteniamo che

$$H = (f * g) \star U = f \star (g \star U) = f \star G$$
$$H = (g * f) \star U = g \star (f \star U) = g \star F,$$

ovvero la tesi. ■

Particolarizzando il Teorema precedente al caso $g = \mathbf{1}$, si ottiene

Corollario 5.2.3 *Se f è una funzione aritmetica e $F(x) = \sum_{n \le x} f(n)$, allora*

$$\sum_{n \le x} \sum_{m | n} f(m) = \sum_{n \le x} f(n) \left\lfloor \frac{x}{n} \right\rfloor = \sum_{n \le x} F\left(\frac{x}{n}\right).$$

Nel seguito applicheremo le tecniche sopra descritte per calcolcare le medie delle funzioni ϕ e d, e vedremo importanti applicazioni di esse. Medie di altre funzioni (quali ad esempio μ e Λ) saranno affrontate nel Capitolo 6.

MEDIA DI ϕ

Teorema 5.3.1 *Per ogni numero reale $x \ge 1$ si ha*

$$\sum_{n \le x} \phi(n) = \frac{3}{\pi^2} x^2 + O(x \log x),$$

pertanto il valore medio di $\phi(n)$ è $3n/\pi^2$.

Dimostrazione. Partiamo dalla formula $\phi = \mu * id$, ovvero

$$\frac{\phi(n)}{n} = \sum_{m | n} \frac{\mu(m)}{m}$$

dimostrata nel Lemma 4.2.6.
Poniamo $T(x) = \sum_{n\le x} \frac{\phi(n)}{n}$; allora, applicando il Corollario 5.2.3 con $f(m) = \frac{\mu(m)}{m}$, abbiamo che

$$\begin{aligned} T(x) &= \sum_{n\le x}\sum_{m\mid n} \frac{\mu(m)}{m} = \sum_{m\le x} \frac{\mu(m)}{m}\left\lfloor \frac{x}{m}\right\rfloor \\ &= \sum_{m\le x} \frac{\mu(m)}{m}\Big(\frac{x}{m} + O(1)\Big) = x\sum_{m\le x}\frac{\mu(m)}{m^2} + O\Big(\sum_{m\le x}\frac{1}{m}\Big) \\ &= x\Big(\sum_{m=1}^{\infty}\frac{\mu(m)}{m^2} - \sum_{m>x}\frac{\mu(m)}{m^2}\Big) + O\Big(\sum_{m\le x}\frac{1}{m}\Big) \\ &= x\Big(\sum_{m=1}^{\infty}\frac{\mu(m)}{m^2}\Big) + O\Big(x\sum_{m>x}\frac{1}{m^2} + \sum_{m\le x}\frac{1}{m}\Big). \end{aligned}$$

Ora per il Teorema 5.1.4

$$\sum_{m\le x}\frac{1}{m} \ll \log x,$$

mentre per il Teorema 4.5.3

$$\sum_{m=1}^{\infty}\frac{\mu(m)}{m^2} = \frac{6}{\pi^2}.$$

Inoltre,

$$\sum_{m>x}\frac{1}{m^2} \le \int_{x-1}^{\infty}\frac{dt}{t^2} = \frac{1}{x-1}.$$

Inserendo queste stime, otteniamo che

$$T(x) = \frac{6}{\pi^2}x + O(\log x). \tag{34}$$

Per terminare la dimostrazione basta ora applicare la Abel summation formula (Proposizione 5.1.1) con $f(n) = \phi(n)/n$ e $g(t) = t$. In virtù di (34) otteniamo

$$\begin{aligned} \sum_{n\le x}\phi(n) &= \Big(\frac{6}{\pi^2}x + O(\log x)\Big)x - \int_1^x \Big(\frac{6}{\pi^2}t + O(\log t)\Big)dt \\ &= \frac{6}{\pi^2}x^2 + O(x\log x) - \frac{6}{\pi^2}\int_1^x t\,dt + O\Big(\int_1^x \log t\,dt\Big) \\ &= \frac{6}{\pi^2}x^2 + O(x\log x) - \frac{3}{\pi^2}t^2\Big|_1^x + O(x\log x) \\ &= \frac{3}{\pi^2}x^2 + O(x\log x), \end{aligned}$$

che è la stima voluta. ■

Vediamo una interessante applicazione del Teorema appena provato.

Corollario 5.3.2 *La probabilità che due interi positivi siano coprimi è* $6/\pi^2$ *(poco meno di* 61%*).*

Dimostrazione. Fissato un $n \in \mathbb{N}^*$, il numero di coppie di interi (r, s) tali che $1 \leq r \leq s \leq n$ è $n(n+1)/2$. Il numero di tali coppie che sono costituite da numeri coprimi, è chiaramente $\sum_{s \leq x} \phi(s)$. Quindi, denotata con $P(n)$ la probabilità che due numeri interi minori di n siano coprimi, si ha

$$P(n) = \frac{2}{n(n+1)} \sum_{i \leq n} \phi(i) \ .$$

La probabilità che due interi positivi qualsiasi siano coprimi è

$$P = \lim_{n \to \infty} P(n) = \lim_{n \to \infty} \frac{2}{n(n+1)} \sum_{i \leq n} \phi(i)$$

per cui, applicando il Teorema precedente, si ha

$$P = \lim_{n \to \infty} \frac{6n^2}{\pi^2 n^2} = \frac{6}{\pi^2},$$

che completa la dimostrazione. ■

Proposizione 5.3.3 *L'insieme* $\{\phi(n)/n\}_{n \geq 1}$ *è denso nell'intervallo* $[0, 1]$.

Dimostrazione. Ci limitiamo a segnalare le linee guida di una possibile dimostrazione.
Scriviamo

$$\frac{n}{\phi(n)} = \prod_{p \mid n} \left(1 + \frac{1}{p-1}\right).$$

Passando ai logaritmi ed usando la continuità, è sufficiente dimostrare che ogni numero reale positivo è limite di una successione di numeri della forma

$$\sum_{p \in P} \log\left(1 + \frac{1}{p-1}\right),$$

dove P è un qualche sottoinsieme finito di $\mathbb{P}$.
Ora, $\log(1 + 1/(p-1)) > 0$ e tende a zero per $p \to \infty$, mentre la serie

$$\sum_{p \in \mathbb{P}} \log\left(1 + \frac{1}{p-1}\right)$$

è divergente. L'Esercizio 5.4 conclude la dimostrazione. ■

MEDIA DI d

Ricordiamo la definizione della funzione d definita a pagina 70:

$$d(n) = \sum_{m|n} 1.$$

Teorema 5.4.1 (P. G. Dirichlet) *Per ogni numero reale $x \geq 1$ si ha*

$$\sum_{n\leq x} d(n) = \sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor = x\log x + (2\gamma - 1)x + O(\sqrt{x}),$$

dove γ è la costante di Eulero-Mascheroni. Pertanto, il valore medio di $d(n)$ è $\log n + 2\gamma - 1$.

DIMOSTRAZIONE. Poichè $d(n) = \sum_{m|n} 1$, per il Teorema 5.2.3 possiamo scrivere

$$\sum_{n\leq x} d(n) = \sum_{n\leq x}\sum_{m|n} 1 = \sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor = \sum_{m\leq x}\sum_{j\leq x/m} 1$$

dunque $\sum_{n\leq x} d(n)$ non è altro che il numero di coppie ordinate (m, j) di interi positivi tali che $mj \leq x$. Denotiamo con D tale insieme

$$D = \left\{(m, j) \in \mathbb{N}^2 | m > 0,\, j > 0,\, mj \leq x\right\}.$$

Poniamo

$$D_1 = \{(m, j) \in D \mid m \leq \sqrt{x}\},\quad D_2 = \{(m, j) \in D \mid j \leq \sqrt{x}\}\,.$$

Allora chiaramente $|D_1| = |D_2|$ e quindi

$$|D| = |D_1| + |D_2| - |D_1 \cap D_2| = 2|D_1| - |D_1 \cap D_2|\,;$$

Poichè $D_1 \cap D_2 = \{(m, j) \in D \mid m \leq \sqrt{x},\ j \leq \sqrt{x}\}$, otteniamo

$$\sum_{n\leq x} d(n) = 2\sum_{m\leq\sqrt{x}}\sum_{j\leq x/m} 1 - \sum_{m\leq\sqrt{x}}\sum_{j\leq\sqrt{x}} 1 = 2\sum_{m\leq\sqrt{x}} \left\lfloor \frac{x}{m} \right\rfloor - \lfloor\sqrt{x}\rfloor^2.$$

Ora abbiamo che

$$\begin{aligned}\left\lfloor \frac{x}{m} \right\rfloor &= \frac{x}{m} - \left\{\frac{x}{m}\right\} = \frac{x}{m} + O(1),\\ \lfloor\sqrt{x}\rfloor^2 &= \left(\sqrt{x} - \left\{\sqrt{x}\right\}\right)^2 = (\sqrt{x} + O(1))^2 = x + O(\sqrt{x}).\end{aligned}$$

Possiamo quindi scrivere

$$\begin{aligned}\sum_{n\leq x} d(n) &= 2\sum_{m\leq\sqrt{x}} \left(\frac{x}{m} + O(1)\right) - x + O(\sqrt{x})\\ &= 2\sum_{m\leq\sqrt{x}} \frac{x}{m} + O\left(2\sum_{m\leq\sqrt{x}} 1\right) - x + O(\sqrt{x})\\ &= 2x\sum_{m\leq\sqrt{x}} \frac{1}{m} - x + O(\sqrt{x}).\end{aligned}$$

Infine applicando il Teorema 5.1.4, si ottiene

$$\begin{aligned}\sum_{n\le x} d(n) &= 2x\left(\log\sqrt{x}+\gamma+O\left(\frac{1}{\sqrt{x}}\right)\right)-x+O(\sqrt{x})\\ &= x\log x+(2\gamma-1)x+O(\sqrt{x})\end{aligned}$$

e la dimostrazione è completata. ■

ESERCIZI

Esercizio 5.1 *Si provi che se f e g sono due arbitrarie funzioni aritmetiche e x un reale positivo, allora*

$$\sum_{n\le x}\left(f(n)\sum_{m\mid n} g(m)\right)=\sum_{m\le x}\left(g(m)\sum_{k\le x/m} f(mk)\right).$$

Esercizio 5.2 *Si provi che $\gamma=\lim_{n\to\infty}\left(\sum_{k=1}^{n}\frac{1}{k}-\log n\right)$.*

Esercizio 5.3 *Si provi che la funzione δ è elemento neutro a sinistra rispetto al prodotto $\star$, ovvero $\delta\star F=F$ per ogni $F\in\mathcal{B}$.*

Esercizio 5.4 *Sia $\{a_n\}_{n\ge1}$ una successione di numeri reali non negativi tale che $a_n\to 0$ per $n\to\infty$. Se la serie $\sum_{n\ge1}a_n$ è divergente, allora per ogni $a\in\mathbb{R}_{>0}$, $N\in\mathbb{N}$ ed $\epsilon>0$, esiste un numero finito di interi $n_1<n_2<\ldots<n_s$, con $n_1>N$ e tali che*

$$\left|a-\sum_{i=1}^{s}a_{n_1}\right|<\epsilon.$$

Esercizio 5.5 *Si descriva il comportamento (asintotico) della funzione*

$$\sum_{i\le n}\frac{\phi(i)}{i}.$$

Esercizio 5.6 *Si provi che*

$$\sum_{i\le x}\frac{\sigma(i)}{i}=\frac{\pi^2}{6}x+O(\log x)\,.$$

Esercizio 5.7 *Si provi che*

$$\left|\sum_{n\le x}\mu(n)\right|\le 1,\ \text{per ogni } x\ge 1,$$

e che vale l'uguaglianza se e solo se $x<2$.

"I'm not quali-
fied to say whe- ther or not God
exists. I kind of doubt He does. Nevertheless, I'm
always saying that the SF has this transfinite Book that
contains the best proofs of all mathematical theorems, proofs
that are elegant and perfect." (Paul Erdös) The strongest
compliment Erdös gave to a colleague's work
was to say, *"It's straight from the*
Book." ([30])

6 NUMERI PRIMI

Uno dei risultati più profondi della Teoria dei Numeri è senza dubbio *il Teorema dei numeri primi* (in breve PNT, per "Prime Number Theorem").

Teorema dei Numeri Primi. *Sia π la funzione che associa ad ogni reale positivo x il numero di primi positivi minori od uguali ad x. Allora per $x \longrightarrow \infty$,*

$$\pi(x) \sim \frac{x}{\log x}.$$

Tale risultato fu congetturato da A. M. Legendre, intorno al 1798, e riprosto da C. F. Gauss che esaminò la lista di tutti i numeri interi $\leq 10^6$. Entrambi però non riuscirono a fornirne una prova, né a confutare l'enunciato. Il problema rimase aperto per quasi 100 anni.

Un primo importante passo in avanti lo fece L. P. Čhebyshev nel 1851, provando che le funzioni $\pi(x)$ e $x/\log x$ hanno lo stesso ordine di grandezza, ovvero $\pi(x) \asymp x/\log x$.

Circa quarant'anni dopo, nel 1896, il Teorema fu dimostrato, e ciò avvenne in modo indipendente da parte di J. Hadamard e C. J. de la Vallée Poussin. Entrambi svilupparono le idee di Riemann, e dimostrarono quindi il Teorema con metodi analitici.

Nel 1949, altri due due matematici, Atle Selberg e Paul Erdös, fornirono una dimostrazione *elementare* del PNT, ovvero una dimostrazione che, sebbene complicata, non utilizza la funzione $\zeta(s)$, né argomenti sofisticati di teoria delle funzioni complesse, ed è quindi, in linea di principio, accessibile anche a chi abbia solo una conoscenza di base di analisi elementare.

In questo Capitolo il lettore non troverà nessuna dimostrazione del PNT (la dimostrazione di Erdös si trova in [46, Chapter 9], mentre ad esempio in [4, Chapter 13] è presente una dettagliata dimostrazione analitica). Vedremo invece il risultato di Čhebyshev del 1851, seguendo una dimostrazione elementare, anch'essa dovuta ad Erdös. Dimostreremo poi il postulato di Bertrand, e faremo alcune considerazioni sulle funzioni θ e ϕ di Čhebyshev, che hanno giocato un ruolo significativo nella dimostrazione del PNT. Di esso vedremo diverse riformulazioni, tutte logicamente equivalenti. Il Capitolo si conclude con il calcolo delle medie della funzione μ di Möbius e della Λ di Mangoldt, risultati che poi in parte riprenderemo nel Capitolo 8.

UNA PRIMA STIMA DI $\pi(x)$

Dal Teorema di Euclide (Teorema 1.2.4) segue agevolmente la seguente stima inferiore della funzione π.

Proposizione 6.1.1 *Per ogni $x \geq 2$, si ha $\pi(x) > \log\log x$.*

DIMOSTRAZIONE. Incominciamo con l'osservare che

$$p_k \leq 2^{2^{k-1}} \quad \text{per ogni intero } k \geq 2, \tag{35}$$

dove, al solito, p_k indica il k-esimo numero primo.
Facciamo induzione su k. Per $k = 2$ è banalmente vero, assumiamo quindi che sia $k > 2$ e che la stima (35) sia vera per ogni $j < k$. Seguendo il ragionamento di Euclide, si ha che

$$p_{k+1} \leq p_1 p_2 \dots p_k + 1 \leq 2^{2^0+2^1+\dots+2^{k-1}} + 1 = 2^{2^k-1} + 1 = \frac{2^{2^k}}{2} + 1 < 2^{2^k}$$

il che completa l'induzione.
Sia ora $x \geq 2$ e sia $s \in \mathbb{N}^*$ tale che

$$2^{2^{s-1}} \leq x < 2^{2^s}.$$

Pertanto $p_s \leq 2^{2^{s-1}}$ e quindi $\pi(x) \geq s$. Passando ai logaritmi nella disuguaglianza $x < 2^{2^s}$ si ottiene che

$$\log_2 x = \frac{\log x}{\log 2} < 2^s$$

e quindi

$$s > \frac{\log(\log x/\log 2)}{\log 2} = \frac{1}{\log 2}(\log\log x - \log\log 2).$$

Essendo $\log 2 < 1$, otteniamo che $-\log\log 2 > 0$ e $1/\log 2 > 1$, pertanto $\pi(x) > \log\log x$, per ogni $x \geq 2$. ∎

IL TEOREMA DI ČHEBYSHEV

Pafnuty Lvovich Čhebyshev per primo provò che la funzione $\pi(x)$ ha lo stesso ordine di grandezza di $x/\log x$. Per la precisione il risultato di Čhebyshev asserisce che, per ogni $x \geq 10$,

$$C_1 \frac{x}{\log x} \leq \pi(x) \leq C_2 \frac{x}{\log x},$$

dove $C_1 = \log\left(\frac{\sqrt[2]{2}\sqrt[3]{3}\sqrt[5]{5}}{\sqrt[30]{30}}\right)$ e $C_2 = \frac{6C_1}{5}$.

Di seguito proponiamo una variante di P. Erdös (leggermente più debole, ma logicamente equivalente) di tale risultato. La dimostrazione è un esempio di eleganza *"straight from the Book"*.

Teorema 6.2.1 *Per ogni $x \geq 2$,*

$$\left(\frac{3\log 2}{8}\right)\frac{x}{\log x} < \pi(x) < (6\log 2)\frac{x}{\log x}.$$

La dimostrazione richiede alcune osservazioni preliminari.

Come già accennato nel Capitolo 1, dal Teorema fondamentale dell'Aritmetica (Teorema 1.2.3) segue che ogni intero positivo n si scrive come il prodotto

$$n = \prod_{p\in\mathbb{P}} p^{v_p(n)}$$

dove i $v_p(n)$ sono numeri naturali univocamente determinati da n, e quasi tutti nulli (ovvero: $v_p(n) \neq 0$ solo per un numero finito di primi p). La funzione v_p viene detta *valore p-adico* ed è una funzione *completamente additiva*, nel senso che, per ogni $n, m \in \mathbb{N}^*$,

$$v_p(mn) = v_p(m) + v_p(n).$$

Meno evidente, ma molto importante è la formula seguente, di cui diamo due diverse dimostrazioni.

Lemma 6.2.2 *Per ogni $n \in \mathbb{N}^*$ e $p \in \mathbb{P}$ vale*

$$v_p(n!) = \sum_{j\geq 1}\left\lfloor \frac{n}{p^j}\right\rfloor = \sum_{j=1}^{\lfloor \log_p n\rfloor}\left\lfloor \frac{n}{p^j}\right\rfloor.$$

Dimostrazione. Facciamo induzione su n. La formula è banalmente vera per $n = 1$, e per tutti i primi p. Assumiamo che valga per n e scriviamo $n+1 = p^a m$, con $p \nmid m$, allora $a = v_p(n+1)$. Allora per ipotesi induttiva abbiamo che

$$\begin{aligned} v_p((n+1)!) &= v_p(n+1) + v_p(n!) \\ &= a + v_p(n!) \\ &\quad a + \sum_{j\geq 0}\left\lfloor \frac{n}{p^j}\right\rfloor \\ &= \sum_{j=1}^{a}\left(\left\lfloor \frac{n}{p^j}\right\rfloor + 1\right) + \sum_{j>a}\left\lfloor \frac{n}{p^j}\right\rfloor. \end{aligned}$$

Da ultimo basta osservare che

$$\left\lfloor \frac{n+1}{p^j}\right\rfloor = \begin{cases} \left\lfloor \frac{n}{p^j}\right\rfloor + 1 & \text{se } 1 \leq j \leq a, \\ \left\lfloor \frac{n}{p^j}\right\rfloor & \text{se } j > a \end{cases}$$

e la dimostrazione è completata. ■

DIMOSTRAZIONE ALTERNATIVA. Siano $I = \{1, 2, \ldots, \lfloor \log_p n \rfloor\}$, l'insieme dei numeri naturali compresi tra 1 e $\lfloor \log_p n \rfloor$, e $T = \{1, 2, \ldots, n\}$, e consideriamo l'insieme delle coppie:

$$S = \{\ (i, m) \in I \times T \mid p^i \text{ divide } m\ \}.$$

Sia $i \in I$; allora il numero di elementi di S che hanno i come prima componente è uguale al numero di interi minori o uguali ad n che sono multipli di p^i, cioè $\lfloor n/p^i \rfloor$. Dunque, il numero di elementi di S (che si può ottenere sommando, per ogni $i \in I$ il numero di coppie di cui essa è la prima componente) è

$$|S| = \sum_{i=1}^{\lfloor \log_p n \rfloor} \left\lfloor \frac{n}{p^i} \right\rfloor$$

Viceversa, fissato un $m \in T$, il numero di elementi di S che hanno m come seconda componente è il numero di potenze di p che dividono m, cioè $v_p(m)$; quindi

$$|S| = \sum_{m=1}^{n} v_p(m)\ .$$

Poiché, per l'osservazione fatta sopra,

$$\sum_{m=1}^{n} v_p(m) = v_p\left(\prod_{m=1}^{n} m\right) = v_p(n!)$$

dal confronto delle due espressioni di $|S|$ si ottiene l'enunciato. ■

Lemma 6.2.3 *Sia n un naturale $n \geq 2$. Allora*

$$2^n < \binom{2n}{n} < 2^{2n}.$$

DIMOSTRAZIONE. Se $n = 2$ l'enunciato del Lemma è banalmente vero. Sia $n \geq 3$. Poichè $2^{2n} = (1+1)^{2n} = \sum_{l=0}^{2n} \binom{2n}{l}$, la stima superiore è banale. Inoltre, essendo, per ogni $l = 0, 1, \ldots, 2n$, $\binom{2n}{n} \geq \binom{2n}{l}$, vale che

$$\frac{2^{2n}}{2n+1} < \binom{2n}{n}.$$

Da ultimo, si prova per induzione su $n \geq 3$, che

$$2^n < \frac{2^{2n}}{2n+1}, \quad \forall n \geq 3,$$

completando così la dimostrazione. ■

Lemma 6.2.4 *La funzione $g(t) = t/\log t$ è crescente nell'intervallo $(e, +\infty)$.*

DIMOSTRAZIONE. Esercizio. ■

DIMOSTRAZIONE DEL TEOREMA 6.2.1 [P. Erdös].
Proviamo prima la stima inferiore.

Mostriamo che se n un intero, $n > 1$, allora

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} \left| \prod_{p<2n} p^{r_p} \right. \tag{36}$$

dove r_p è l'intero positivo tale che $p^{r_p} \leq 2n < p^{r_p+1}$. L'esponente di p che compare nel coefficiente binomiale $\binom{2n}{n}$ è dato da

$$v_p((2n)!) - v_p((n!)^2) = v_p((2n)!) - 2v_p((n!)) = \sum_{k\geq 1} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Pertanto la (36) segue dal fatto che $\lfloor 2y \rfloor - 2\lfloor y \rfloor \in \{0, 1\}$, per ogni reale y, e che quando $k > r_p$ allora $p^k > 2n$ e quindi $\lfloor 2n/p^k \rfloor = 0$.

Per il Lemma 6.2.3, otteniamo allora in particolare che

$$2^n < \binom{2n}{n} \leq \prod_{p<2n} p^{r_p} \leq (2n)^{\pi(2n)},$$

cioè, prendendo i logaritmi,

$$\pi(2n) > \frac{\log(2^n)}{\log(2n)} = \frac{\log 2}{2} \cdot \frac{2n}{\log(2n)}.$$

Assumiamo ora che sia $x \geq 8$. Preso n tale che $2n \leq x < 2n + 2$, si ha $n \geq 3$ e

$$2n > x - 2 \geq 3x/4 \geq 6 > e$$

essendo $x \geq 8$, pertanto per il Lemma 6.2.4,

$$\pi(x) \geq \pi(2n) \geq \frac{\log 2}{2} \cdot \frac{2n}{\log(2n)} \geq \frac{\log 2}{2} \cdot \frac{3x/4}{\log(3x/4)} > \frac{3\log 2}{8} \cdot \frac{x}{\log(x)},$$

una verifica diretta mostra che tale stima vale anche per $x \in [2, 8)$.

Proviamo ora la stima superiore.

Notiamo che

$$\prod_{n<p\leq 2n} p \left| \binom{2n}{n} \right. \tag{37}$$

quindi,

$$\prod_{n<p\leq 2n} p < (1+1)^{2n} = 2^{2n}.$$

Prendendo i logaritmi abbiamo

$$\sum_{n<p\leq 2n} \log p \leq 2n \log 2.$$

Ma

$$\sum_{n<p\leq 2n} \log p > \sum_{n<p\leq 2n} \log n = \big(\pi(2n) - \pi(n)\big) \log n,$$

e pertanto abbiamo

$$\pi(2n)\log n - \pi(n)(\log(n/2) + \log 2) < 2n\log 2.$$

Usando la stima $\pi(n) \leq n$,

$$\pi(2n)\log n - \pi(n)\log(n/2) < 2n\log 2 + \pi(n)\log 2 \leq (3\log 2)n,$$

ovvero

$$f(n) - f(n/2) < (3\log 2)n,$$

dove $f(n) = \pi(2n)\log n$, per ogni $n \geq 2$. In particolare, per ogni $k \geq 2$, abbiamo che

$$f(2^k) - f(2) = \sum_{j=2}^{k} \left(f(2^j) - f(2^{j-1}) \right) < (3\log 2) \sum_{j=2}^{k} 2^j$$

da cui segue che

$$\pi(2^{k+1}) < (6\log 2) \left(\frac{2^k}{\log(2^k)} \right).$$

Sia ora x un numero reale $x \geq 4$, e sia tale che $2^k \leq x < 2^{k+1}$. Allora $2^k > e$, pertanto per il Lemma 6.2.4, $2^k/\log(2^k) \leq x/\log x$; ne segue che

$$\pi(x) \leq \pi(2^{k+1}) < (6\log 2) \left(\frac{2^k}{\log(2^k)} \right) < (6\log 2) \frac{x}{\log x}$$

stima che si verifica essere vera anche se $x \in [2, 4)$. ■

Corollario 6.2.5 *Dato $n \in \mathbb{N}^*$, l'n-esimo numero primo p_n soddisfa a*

$$c_1 n \log n < p_n < c_2 \left(n\log n + n\log(c_2/e) \right),$$

dove $c_1 = \frac{1}{6\log 2} \simeq 0,24$ e $c_2 = \frac{16}{3\log 2} \simeq 7,69$.

Dimostrazione. ■

IL POSTULATO DI BERTRAND

Nel 1845 Joseph Bertrand provò che, per ogni naturale $n \leq 6 \cdot 10^6$, esiste sempre un numero primo nell'intervallo $[n, 2n]$ e congetturò che tale risultato doveva essere sempre vero. La prima dimostrazione di questa congettura (nota come *postulato di Bertrand*) fu data da Čebyshev nel 1850, e fa uso di metodi non elementari. Nel 1919 Srinivasa Ramanujan fornì una dimostrazione elementare, sintetica ed elegante (vedi [52] e [33]). Quella che riportiamo è invece opera di un giovane Paul Erdös (diciotto anni).

Lemma 6.3.1 *Per ogni $n \in \mathbb{N}^*$, vale $\prod_{p \leq n} p < 4^n$.*

DIMOSTRAZIONE. Facciamo induzione su n. Per $n = 1$ o $n = 2$ il risultato è banale. Sia dunque $n \geq 3$. Se n fosse pari, allora da

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p,$$

il risultato segue per l'ipotesi induttiva. Sia pertanto $n = 2m + 1$, con $m \geq 1$. Notiamo che

$$\prod_{m+1 < p \leq 2m+1} p \,\Bigg|\, \binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$

e poiché $\binom{2m+1}{m} = \binom{2m+1}{m+1}$ e appaiono come termini dello sviluppo del binomio $(1+1)^{2m+1}$, otteniamo che

$$\binom{2m+1}{m} \leq \frac{1}{2}(2^{2m+1}) = 4^m.$$

Pertanto

$$\prod_{p \leq 2m+1} p = \left(\prod_{p \leq m+1} p\right)\left(\prod_{m+1 < p \leq 2m+1} p\right) < 4^{m+1}\binom{2m+1}{m} \leq 4^{2m+1},$$

che completa la dimostrazione. ∎

Lemma 6.3.2 *Se $n \geq 3$ e p un primo tale che $2n/3 < p \leq n$, allora p non divide $\binom{2n}{n}$.*

DIMOSTRAZIONE. Dall'ipotesi segue che $p > 2$ e che p e $2p$ sono gli unici multipli (positivi) di p ad essere minori o uguali a $2n$. Pertanto $p^2 \parallel (2n)!$, ovvero $v_p((2n)!) = 2$. Essendo $p \leq n$, segue che $p | n!$ e quindi p non divide $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. ∎

Teorema 6.3.3 (Postulato di Bertrand) *Sia $n \in \mathbb{N}^*$. Allora esiste un numero primo p tale che $n < p \leq 2n$.*

DIMOSTRAZIONE. [P. Erdös, 1932]. Notiamo che il risultato è sicuramente vero per $n = 1, 2$ e 3. Assumiamo per assurdo che sia falso per qualche $n \geq 4$. Allora per l'ipotesi d'assurdo e per il Lemma 6.3.2, ogni primo che divide $\binom{2n}{n}$ è $\leq 2n/3$. Sia p un tale primo e sia $p^\alpha \parallel \binom{2n}{n}$. In particolare, per la relazione (36) (provata nel corso della dimostrazione del Teorema 6.2.1), abbiamo che $\alpha \leq r_p$, dove r_p è tale

che $p^{r_p} \leq 2n < p^{r_p+1}$, quindi $p^\alpha \leq p^{r_p} \leq 2n$. Osserviamo che se $\alpha \geq 2$, allora $p^2 \leq p^\alpha \leq 2n$ e quindi $p \leq \sqrt{2n}$. Pertanto

$$\begin{aligned}\binom{2n}{n} &\leq \prod_{p \leq 2n/3} p^{r_p} \\ &\leq \left(\prod_{p \leq 2n/3} p\right)\left(\prod_{p \leq \sqrt{2n}} p^{r_p-1}\right) \\ &\leq \left(\prod_{p \leq 2n/3} p\right)(2n)^{\pi(\sqrt{2n})} \\ &\leq 4^{2n/3}(2n)^{\sqrt{2n}},\end{aligned}$$

dove abbiamo usato nuovamente il Lemma 6.3.2 e le maggiorazioni $p^{r_p-1} \leq 2n$ e $\pi(\sqrt{2n}) \leq \sqrt{2n}$. Ora, poiché $\binom{2n}{n}$ è il più grande fra i coefficienti binomiali dello sviluppo di $(1+1)^{2n}$, abbiamo che

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n+1}.$$

Ne segue che

$$\frac{4^n}{2n+1} \leq 4^{2n/3}(2n)^{\sqrt{2n}},$$

che implica

$$2^{2n/3} < (2n)^{\sqrt{2n}}(2n+1) < (2n)^{\sqrt{2n}+2}.$$

Prendendo i logaritmi,

$$\frac{2n\log 2}{3} < (\sqrt{2n}+2)\log(2n).$$

Posto $y = \sqrt{2n}$, la disuguaglianza di sopra diventa

$$\frac{y^2\log 2}{3} - 2(y+2)\log y < 0. \tag{38}$$

Detta $f(y) := \frac{y^2\log 2}{3} - 2(y+2)\log y$ proviamo che (38) è impossibile se $y \geq 32$. Infatti abbiamo che

$$f'(y) = \frac{2(\log 2)y}{3} - 2\left(1+\frac{2}{y}\right) - 2\log y > \frac{2(\log 2)y}{3} - 2,2 - 2\log y.$$

Sia $g(y) := \frac{2(\log 2)y}{3} - 2\log y - 2,2$ e notiamo che

$$g'(y) = 2(\log 2)/3 - 2/y > 0$$

se $y \geq 32$, pertanto g è crescente per tali valori di y. Essendo $g(32) = 34(\log 2)/3 - 2,2 > 0$, abbiamo che $f'(y) \geq 0$ se $y \geq 32$. Poiché $f(32) = 4(\log 2)/3 > 0$, la (38) risulta possibile solo se $y < 32$, ovvero se e solo se $n < 512$.

Da ultimo si osserva che i primi: $2, 3, 5, 7, 13, 23, 43, 83, 163, 317, 557$ coprono il caso $n < 512$. ■

Il Teorema 6.3.3 è equivalente all'affermare che $\pi(2n) - \pi(n) \geq 1$, per ogni $n \geq 2$. Ora, il Teorema dei numeri primi afferma che $\pi(x) \sim x/\log x$, o, equivalentemente che

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right)$$

per $x \to \infty$. Pertanto, preso un $\epsilon > 0$ il numero di primi compresi nell'intervallo $(x, (1+\epsilon)x]$ è dato da:

$$\begin{aligned}
\pi((1+\epsilon)x) - \pi(x) &= \frac{(1+\epsilon)x}{\log((1+\epsilon)x)} - \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) \\
&= \frac{(1+\epsilon)x}{\log x\left(1 + \frac{\log(1+\epsilon)}{\log x}\right)} - \frac{x}{\log x} + o\left(\frac{x}{\log x}\right) \\
&= \frac{(1+\epsilon)x}{\log x}\left(1 + O\left(\frac{\log(1+\epsilon)}{\log x}\right)\right) - (1+o(1))\frac{x}{\log x} \\
&= \frac{\epsilon x}{\log x} + O\left(\frac{x}{(\log x)^2}\right) + o\left(\frac{x}{\log x}\right) \\
&= \frac{\epsilon x}{\log x} + o\left(\frac{x}{\log x}\right) \quad (\text{per } x \to \infty) \qquad (39)
\end{aligned}$$

dove si è usata la stima $\frac{1}{1+z} = 1 + O(z)$, valida per ogni $z \in (0, 1/2)$. Ne segue che il numero di primi compresi fra n e $2n$ è approssimativamente $\frac{n}{\log n}$ quando n è grande, ed in particolare, ci sono in questo intervallo molti più numeri primi di quanti ne siano garantiti dal Postulato di Bertrand. In altre parole, questo postulato è quantitativamente più debole rispetto al PNT. Tuttavia, è stato dimostrato da Čhebyshev molto tempo prima del PNT ed inoltre la stima (39), al contrario del Teorema 6.3.3, è valida solo per valori di n sufficientemente grandi.

Paul Erdös dimostrò in [17] che per ogni intero positivo k, esiste un numero N tale che per ogni $n > N$, ci sono almeno k primi compresi fra n e $2n$. Inoltre, provò che esistono sempre due numeri primi p e q con $n < p, q < 2n$ per ogni $n > 6$, di cui uno è congruo ad 1 modulo 4, e l'altro è congruo a -1 modulo 4.

Nel 2006, M. El Bachraoui ha dimostrato che anche $\pi(3n) - \pi(2n) \geq 1$ ([16], mentre nel 2011, Andy Loo ([40]) ha provato che $\pi(4n) - \pi(3n) \geq 1$, inoltre quando n tende all'infinito, il numero di primi compresi tra $3n$ e $4n$ va anch'esso all'infinito, generalizzando in questo modo precedenti risultati di Erdös e Ramanujan.

Una congettura di Legendre, ancora indimostrata, afferma che per ogni $n > 0$, esiste un primo p tale che $n^2 < p < (n+1)^2$, o, in altre parole, che tra due quadrati consecutivi esiste almeno un numero primo.

LE FUNZIONI ψ E θ DI ČHEBYSHEV

Ricordiamo come è stata definita la funzione di Mangoldt nel Capitolo 4.

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^k \text{ per qualche } k \geq 1, \\ 0 & \text{altrimenti.} \end{cases}$$

Nel corso della dimostrazione del Teorema dei numeri Primi, due funzioni, introdotte da Čhebyshev, giocano un ruolo significativo. Sono le cosiddette 'psi' e 'theta', definite per ogni reale positivo x da:

$$\psi(x) = \sum_{1<p^k\leq x} \log p = \sum_{n\leq x} \Lambda(n)$$

$$\theta(x) = \sum_{p\leq x} \log p = \log\left(\prod_{p\leq x} p\right).$$

Notiamo che

$$\psi = \Lambda \star U,$$

dove $\star$ è il prodotto di convoluzione generalizzato definito a pagina 88 e la funzione U è data da:

$$U(x) = \begin{cases} 0 & \text{se } 0 < x < 1 \\ 1 & \text{altrimenti.} \end{cases}$$

Inoltre,

$$\theta(x) \leq \sum_{p\leq x} \log x = \pi(x) \log x.$$

Similmente,

$$\begin{aligned} \psi(x) &= \sum_{p\leq x} \lfloor \log_p x \rfloor \log p = \sum_{p\leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \\ &\leq \sum_{p\leq x} \frac{\log x}{\log p} \log p = \pi(x) \log x. \end{aligned}$$

Pertanto, in virtù del Teorema 6.2.1, abbiamo $\theta(x), \psi(x) \leq O(x)$. Volendo essere più precisi, dal fatto che $p^k \leq x$ è equivalente a $p \leq x^{1/k}$, otteniamo che

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \ldots + \theta(x^{1/t}),$$

dove $t = \lfloor \log_2 x \rfloor = \lfloor \log x / \log 2 \rfloor$, e quindi

$$\begin{aligned} \theta(x) \leq \psi(x) &\leq \theta(x) + \theta(x^{1/2})(\log x / \log 2) \\ &\leq \theta(x) + O(x^{1/2} \log x). \end{aligned} \tag{40}$$

In realtà, per x tendente all'infinito, le due funzioni sono asintotiche; come dimostra la seguente Proposizione.

Proposizione 6.4.1 *$\theta(x) \sim \psi(x)$, quando $x \to \infty$.*

DIMOSTRAZIONE. Per $p \geq x^{1/2}$ si ha che $\log p \geq (\log x)/2 \gg \log x$, pertanto

$$\begin{aligned}\theta(x) &\geq \sum_{x^{1/2} \leq p \leq x} \log p \\ &\gg (\pi(x) - \pi(\sqrt{x})) \log x \\ &= \pi(x) \log x - \pi(\sqrt{x}) \log x \\ &= \pi(x) \log x + O(x^{1/2}) \\ &\gg x,\end{aligned}$$

essendo $\pi(x) \log x \gg x$ per il Teorema 6.2.1. Applicando la (40), ne segue che

$$0 \leq \frac{\psi(x) - \theta(x)}{\theta(x)} = \frac{O(x^{1/2} \log x)}{\theta(x)} \ll \frac{O(x^{1/2} \log x)}{x} \longrightarrow 0,$$

per $x \to \infty$, ovvero $\psi(x) \sim \theta(x)$. ∎

Teorema 6.4.2 *Per $x \to \infty$ si ha*

$$\pi(x) \sim \frac{\theta(x)}{\log x} \sim \frac{\psi(x)}{\log x}.$$

DIMOSTRAZIONE. Per la Proposizione precedente, basta provare la prima uguaglianza asintotica. Dal fatto che $\theta(x) \leq \pi(x) \log x$, si ha

$$\limsup_{x \to \infty} \frac{\theta(x)/\log x}{\pi(x)} \leq 1. \tag{41}$$

Occorre e basta quindi provare che

$$\liminf_{x \to \infty} \frac{\theta(x)/\log x}{\pi(x)} \geq 1. \tag{42}$$

Sia δ un reale positivo arbitrariamente piccolo, diciamo $\delta \in (0, 1/2)$. Allora

$$\begin{aligned}\theta(x) &\geq \sum_{x^{1-\delta} < p \leq x} \log p \\ &\geq \log(x^{1-\delta}) \sum_{x^{1-\delta} < p \leq x} 1 \\ &= (1-\delta)(\log x)(\pi(x) - \pi(x^{1-\delta})) \\ &= (1-\delta)\pi(x) \log x + O(x^{1-\delta}),\end{aligned}$$

dove abbiamo usato la stima di Čhebyshev

$$\pi(x^{1-\delta}) \ll \frac{x^{1-\delta}}{\log(x^{1-\delta})} < \frac{2x^{1-\delta}}{\log x},$$

essendo $1-\delta > 1/2$. Esistono allora due costanti positive c_1 e c_2 tali che

$$\frac{\theta(x)/\log x}{\pi(x)} \geq (1-\delta) - \frac{c_1 x^{1-\delta}}{\pi(x)\log x} \geq (1-\delta) - \frac{c_1}{c_2 x^{\delta}}.$$

Mandando x all'infinito si ottiene

$$\liminf_{x\to\infty} \frac{\theta(x)/\log x}{\pi(x)} \geq 1-\delta$$

e dall'arbitrarietà di $\delta > 0$, si deduce la (42). ■

Dai due risultati precedenti segue immediatamente il seguente Corollario.

Corollario 6.4.3 (Formulazioni equivalenti del PNT, I) *Le seguenti sono tre formulazioni equivalenti del Teorema dei Numeri Primi.*

1. $\pi(x) \sim \frac{x}{\log x}$, *per* $x \to \infty$;
2. $\psi(x) \sim x$, *per* $x \to \infty$;
3. $\theta(x) \sim x$, *per* $x \to \infty$.

Concludiamo questa sezione con un risultato che lega il PNT al valore asintotico dell'n-esimo numero primo.

Proposizione 6.4.4 (Formulazioni equivalenti del PNT, II) *Le seguenti condizioni sono equivalenti:*

1. $\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1$;
2. $\lim_{x\to\infty} \frac{\pi(x)\log \pi(x)}{x} = 1$;
3. $\lim_{n\to\infty} \frac{p_n}{n\log n} = 1$.

Dimostrazione. Proviamo prima l'equivalenza fra 1. e 2.
Assumiamo 1., cioè $\pi(x) \sim x/\log x$, per $x \to \infty$. Allora

$$\log \pi(x) \sim \log x - \log\log x \sim \log x$$

da cui segue 2.
Viceversa, assumendo 2. si ha che $\pi(x) \sim x/\log \pi(x)$, per $x \to \infty$, da cui segue

$$\log x \sim \log \pi(x) + \log\log \pi(x) \sim \log \pi(x),$$

e quindi 1.
Proviamo ora che 2. è equivalente a 3.
Assumiamo 2. Se $x = p_n$ allora $\pi(x) = n$ e

$$\pi(x)\log \pi(x) = n\log n,$$

quindi 2. implica 3.
Infine assumiamo 3.. Dato x reale positivo , sia p_n tale che

$$p_n \leq x < p_{n+1},$$

così che $n = \pi(x)$. Allora

$$\frac{p_n}{n\log n} \leq \frac{x}{n\log n} < \frac{p_{n+1}}{(n+1)\log(n+1)} \frac{(n+1)\log(n+1)}{n\log n}.$$

Mandando $n \to \infty$ si ottiene 2. ■

MEDIA DI Λ E APPLICAZIONI

Il Corollario 6.4.3 afferma in particolare che

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 0 \quad \Longleftrightarrow \quad \lim_{x\to\infty} \frac{1}{x}\sum_{n\leq x} \Lambda(n) = 1.$$

Pertanto essendo vero il PNT, abbiamo che il valore medio della funzione Λ esiste ed è uno.

Di seguito proviamo un interessante risultato che sfrutta proprio il comportamento medio asintotico della funzione Λ. Tra le applicazioni più significative, vi è la dimostrazione del Teorema di Dirichlet (Teorema 8.2.6), che presenteremo nel Capitolo 8.

Lemma 6.5.1 *Per* $1 \leq x \in \mathbb{R}$,

$$\sum_{n\leq x} \frac{\Lambda(n)}{n} = \log x + O(1)\ .$$

DIMOSTRAZIONE. Per il Lemma 4.3.1, $\sum_{m|n} \Lambda(m) = \log n$. Quindi, applicando il Teorema 5.2.3,

$$\sum_{n\leq x} \log n = \sum_{n\leq x} \left\lfloor \frac{x}{n} \right\rfloor \Lambda(n).$$

Si ottiene quindi

$$\begin{aligned}\sum_{n\leq x} \frac{\Lambda(n)}{n} &= \frac{1}{x}\sum_{n\leq x} \frac{\Lambda(n)x}{n} \\ &= \frac{1}{x}\sum_{n\leq x} \Lambda(n)\left\lfloor \frac{x}{n} \right\rfloor + \frac{1}{x}\sum_{n\leq x} \Lambda(n)\cdot\left\{\frac{x}{n}\right\} \\ &= \frac{1}{x}\sum_{n\leq x} \log n + \frac{1}{x}\sum_{n\leq x} \Lambda(n)\cdot\left\{\frac{x}{n}\right\}.\end{aligned}$$

Per il Lemma 4.3.1,

$$0 \leq \frac{1}{x}\sum_{n\leq x} \Lambda(n)\cdot\left\{\frac{x}{n}\right\} \leq \frac{1}{x}\sum_{n\leq x} \Lambda(n) = \frac{\psi(x)}{x} = O(1).$$

Quindi, applicando il Lemma 5.1.2,

$$\sum_{n\leq x}\frac{\Lambda(n)}{n}=\frac{1}{x}(x\log x-x+O(\log x))+O(1)=\log x+O(1),$$

come si voleva. ■

Teorema 6.5.2 *Per x sufficientemente grande, vale*

$$\sum_{p\leq x}\frac{\log p}{p}=\log x+O(1). \tag{43}$$

Dimostrazione. Ovviamente,

$$\begin{aligned}\sum_{p\leq x}\frac{\log p}{p}&=\sum_{n\leq x}\frac{\Lambda(n)}{n}-\sum_{m\geq 2}\sum_{p^m\leq x}\frac{\log p}{p^m}\\&=\log x+O(1)-\sum_{m\geq 2}\sum_{p^m\leq x}\frac{\log p}{p^m},\end{aligned}$$

per il Lemma precedente. Tuttavia,

$$\begin{aligned}\sum_{m\geq 2}\sum_{p^m\leq x}\frac{\log p}{p^m}&\leq\sum_{p\in\mathbb{P}}\left(\frac{1}{p^2}+\frac{1}{p^3}+\dots\right)\log p\\&=\sum_{p\in\mathbb{P}}\frac{\log p}{p(p-1)}.\end{aligned}$$

Infine la serie $\sum_{p\in\mathbb{P}}\frac{\log p}{p(p-1)}$ è a termini positivi ed è maggiorata da una serie convergente, ad esempio da $\sum_{n\geq 2}n^{-3/2}$, pertanto è essa stessa convergente, ovvero è un $O(1)$. Ciò completa la dimostrazione. ■

MEDIA DI μ E ULTERIORE FORMULAZIONE DEL PNT

Un'altra condizione equivalente al PNT, oltre a quelle già citate nel Corollario 6.4.3 e nella Proposizione 6.4.4, è la seguente:

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x}=0\quad\Longleftrightarrow\quad\lim_{x\to\infty}\frac{1}{x}\sum_{n\leq x}\mu(n)=0. \tag{44}$$

In questa sezione ci limiteremo a provare l'implicazione da sinistra a destra, e pertanto proveremo così che il valore medio della funzione di Möbius esiste ed è nullo. La dimostrazione completa dell'equivalenza (44) si può trovare in [4] (Teoremi 4.14 e 4.15).

Per ogni $x\geq 1$, poniamo $M(x):=\sum_{n\leq x}\mu(n)=(\mu\star U)(x)$.

Lemma 6.6.1 *Per ogni $x \geq 1$ reale, sia $H(x) = \sum_{n \leq x} \mu(n) \log n$. Allora*

$$\lim_{x \to \infty} \left(\frac{M(x)}{x} - \frac{H(x)}{x \log x} \right) = 0.$$

DIMOSTRAZIONE. Applicando la Abel Summation Formula (Proposizione 5.1.1) con $f = \mu$ e $g = \log$ si ottiene

$$H(x) = \sum_{n \leq x} \mu(n) \log n = M(x) \log x - \int_1^x \frac{M(t)}{t} dt.$$

Pertanto per $x > 1$ abbiamo che

$$\frac{M(x)}{x} - \frac{H(x)}{x \log x} = \frac{1}{x \log x} \int_1^x \frac{M(t)}{t} dt. \tag{45}$$

Ora $|M(x)| \leq \sum_{n \leq x} |\mu(n)| \leq x$, e quindi $M(x) = O(x)$ e, conseguentemente, $\frac{M(t)}{t} = O(1)$ e $\int_1^x \frac{M(t)}{t} dt = O\left(\int_1^x dt\right) = O(x)$.
Da (45) si ha la tesi per $x \to \infty$. ■

Teorema 6.6.2 *Assumendo il PNT si ha $\lim_{x \to \infty} \frac{M(x)}{x} = 0$.*

DIMOSTRAZIONE. Dimostreremo che

$$\psi(x) \sim x \quad \text{implica} \quad \lim_{x \to \infty} \frac{H(x)}{x \log x} = 0,$$

la tesi seguirà dal Corollario 6.4.3 e dal Lemma 6.6.1.

Incominciamo con il provare che

$$-H(x) = \sum_{n \leq x} \mu(n) \psi\left(\frac{x}{n}\right). \tag{46}$$

Infatti per il Lemma 4.3.1 abbiamo che

$$\Lambda(n) = -\sum_{m|n} \mu(m) \log m$$

e applicando l'inversione di Möbius (Teorema 4.2.5), otteniamo

$$-\mu(n) \log n = \sum_{m|n} \mu(m) \Lambda\left(\frac{n}{m}\right).$$

Sommando membro a membro su tutti gli $n \leq x$, abbiamo

$$-H(x) = \sum_{n \leq x} \mu(n) \log n = \sum_{n \leq x} \sum_{m|n} \mu(m) \Lambda\left(\frac{n}{m}\right),$$

cioè

$$-H(x) = ((\mu * \Lambda) \star U)(x).$$

Applicando la Divisor Summation Identity (Teorema 5.2.2) e tenendo conto della definizione della funzione ψ, si ottiene

$$-H(x) = ((\mu * \Lambda) \star U)(x) = (\mu \star (\Lambda \star U))(x) = \sum_{n \leq x} \mu(n)\psi\left(\frac{x}{n}\right).$$

Sia ora assegnato un $\epsilon > 0$ piccolo a piacere. Poiché $\psi(x) \sim x$ scegliamo x_0 reale positivo per cui

$$|\psi(x) - x| \leq \frac{\epsilon}{2}x, \quad \text{per ogni } x \geq x_0.$$

Preso allora $x \geq x_0$ e detto $y = \lfloor x/x_0 \rfloor$, abbiamo che

$$-H(x) = \sum_{n \leq y} \mu(n)\psi\left(\frac{x}{n}\right) + \sum_{y < n \leq x} \mu(n)\psi\left(\frac{x}{n}\right)$$

stimeremo separatamente le due sommatorie.

Se $n \leq y$, allora $x/n \geq x_0$ e pertanto $\left|\psi(\frac{x}{n}) - \frac{x}{n}\right| \leq \frac{\epsilon}{2}\frac{x}{n}$. Quindi

$$\begin{aligned}\sum_{n \leq y} \mu(n)\psi\left(\frac{x}{n}\right) &= \sum_{n \leq y} \mu(n)\left(\frac{x}{n} + \psi\left(\frac{x}{n}\right) - \frac{x}{n}\right) \\ &= x\sum_{n \leq y} \frac{\mu(n)}{n} + \sum_{n \leq y} \mu(n)\left(\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right),\end{aligned}$$

da cui segue

$$\begin{aligned}\left|\sum_{n \leq y} \mu(n)\psi\left(\frac{x}{n}\right)\right| &\leq x\left|\sum_{n \leq y} \frac{\mu(n)}{n}\right| + \sum_{n \leq y}\left|\psi\left(\frac{x}{n}\right) - \frac{x}{n}\right| \\ &\leq x + \frac{\epsilon}{2}\sum_{n \leq y}\frac{x}{n} \\ &\leq x + \frac{\epsilon}{2}x(1 + \log y) \\ &x + \frac{\epsilon}{2}x + \frac{\epsilon}{2}x\log x,\end{aligned}$$

dove si sono usati l'Esercizio 5.7 e la maggiorazione $\sum_{n \leq y} 1/n \leq 1 + \log y$.

Se invece $y < n \leq x$, allora $n \geq y + 1$ e $x/n < x_0$, quindi $\psi(x/n) \leq \psi(x_0)$ e

$$\sum_{y < n \leq x} \mu(n)\psi\left(\frac{x}{n}\right) \leq x\psi(x_0).$$

Si conclude quindi che per ogni $0 < \epsilon < 1$, vale

$$|H(x)| \leq (1 + \frac{\epsilon}{2})x + \frac{\epsilon}{2}x\log x + x\psi(x_0),$$

per ogni $x \geq x_0$. Infine, scegliendo x_1 tale che $\frac{2+\psi(x_0)}{\log x} \leq \frac{\epsilon}{2}$ se $x \geq x_1$, abbiamo che per ogni $x \geq \max\{x_0, x_1\}$

$$0 \leq \frac{H(x)}{x\log x} \leq \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon,$$

ovvero la tesi. ■

Per molti anni rimase aperta la seguente

Congettura di Mertens *Se* $x > 1$, *allora* $|M(x)| < \sqrt{x}$.

Solo nel 1985 fu confutata da A.M Odlyzko e H.J.J. te Riele ([50]). L'esatto ordine di grandezza, in termini di O, per la funzione M è tuttora ignoto, anche perché vale il seguente importante risultato

Teorema 6.6.3 *L'ipotesi di Riemann è equivalente alla congettura* $M(x) = O(x^{1/2+\epsilon})$, *per ogni* $\epsilon > 0$.

APPENDICE

Ancora sulla serie $\sum_{p\in\mathbb{P}} \frac{1}{p}$

Nell'Appendice al Capitolo 1 a pagina 15 abbiamo proposto una dimostrazione della divergenza della serie $\sum_{p\in\mathbb{P}} \frac{1}{p}$. Vediamo ora una stima più accurata dovuta a F. Mertens ([42]).

Teorema 6.7.1 (F. Mertens) *Esiste una costante* β_1 *tale che:*

$$\sum_{p\le x} \frac{1}{p} = \log\log x + \beta_1 + O\Big(\frac{1}{\log x}\Big), \quad \textit{per } x \to +\infty.$$

Dimostrazione. Definiamo

$$f(n) = \begin{cases} \frac{\log p}{p} & \text{se } n = p, \\ 0 & \text{altrimenti.} \end{cases}$$

e sia $g(t) = (\log t)^{-1}$, per $t \in [2, +\infty)$. Allora $g'(t) = -(t(\log t)^2)^{-1}$ e

$$F(x) = \sum_{n\le x} f(n) = \sum_{p\le x} \frac{\log p}{p} = \log x + h(x),$$

dove $h(x) = O(1)$ per il Teorema 6.5.2. Applicando la Proposizione 5.1.1, otteniamo

$$\begin{aligned}
\sum_{p\le x}\frac{1}{p} = \sum_{n\le x} f(n)g(n) &= \frac{F(x)}{\log x} + \int_2^x \frac{F(t)}{t(\log t)^2}\,dt \\
&= 1 + \frac{h(x)}{\log x} + \int_2^x \frac{\log t + h(t)}{t(\log t)^2}\,dt \\
&= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t\log t} + \int_2^x \frac{h(t)}{t(\log t)^2}\,dt \\
&= 1 + O\left(\frac{1}{\log x}\right) + (\log\log t)\Big|_2^x + \int_2^\infty \frac{h(t)}{t(\log t)^2}\,dt + \\
&\qquad - \int_x^\infty \frac{h(t)}{t(\log t)^2}\,dt \\
&= \log\log x + 1 - \log\log 2 + \int_2^\infty \frac{h(t)}{t(\log t)^2}\,dt + \\
&\qquad + O\left(\frac{1}{\log x}\right) + O\left(\int_x^\infty \frac{dt}{t(\log t)^2}\right) \\
&= \log\log x + \beta_1 + O\left(\frac{1}{\log x} + \left(-\frac{1}{\log t}\right)\Big|_x^\infty\right) \\
&= \log\log x + \beta_1 + O\left(\frac{1}{\log x}\right),
\end{aligned}$$

dove $\beta_1 = 1 - \log\log 2 + \int_2^\infty \frac{h(t)}{t(\log t)^2}\,dt$. ■

Sul prodotto di Eulero $\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1}$

Nel Capitolo 4, Sezione 4.4, abbiamo provato che per ogni reale $s > 1$

$$\zeta(s) = \sum_{n\ge 1}\frac{1}{n^s} = \prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)^{-1}$$

Vediamo ora una stima, sempre dovuta a F. Mertens, per $s = 1$ di questo prodotto.

Teorema 6.7.2 (F. Mertens) *Per $x \ge 2$*

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} = e^{\gamma}\log x + O(1),$$

dove γ è la costante di Eulero-Mascheroni.

Dimostrazione. Limitiamoci a provare che esiste una costante β tale che

$$\prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} = e^{\beta}\log x + O(1).$$

La dimostrazione che $\beta = \gamma$ si può trovare in [45, Theorem 6.9].

Incominciamo con due osservazioni. Innanzitutto la serie

$$\sum_p \sum_{k=2}^{\infty} \frac{1}{kp^k}$$

è convergente. Infatti

$$\begin{aligned}\sum_p \sum_{k=2}^{\infty} \frac{1}{kp^k} &\leq \sum_p \sum_{k=2}^{\infty} \frac{1}{p^k} = \sum_p \frac{1}{p(p-1)} \\ &< \sum_{n=2}^{\infty} \frac{1}{n(n-1)} < \infty.\end{aligned}$$

Sia $\beta_2 = \sum_p \sum_{k=2}^{\infty} \frac{1}{kp^k}$.

Ora, per $x \geq 2$ abbiamo che

$$\begin{aligned}0 < \sum_{p>x} \sum_{k=2}^{\infty} \frac{1}{kp^k} &< \sum_{p>x} \frac{1}{p(p-1)} < \sum_{n>x} \frac{1}{n(n-1)} \\ &= \sum_{n=\lfloor x \rfloor + 1}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) \\ &= \frac{1}{\lfloor x \rfloor} \leq \frac{2}{x},\end{aligned}$$

poiché $\lfloor x \rfloor \leq x < 2\lfloor x \rfloor$.
Dallo sviluppo $-\log(1-t) = \sum_{k=1}^{\infty} \frac{t^k}{k}$, per $|t| < 1$, e dal Teorema 6.7.1, otteniamo

$$\begin{aligned}\log \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} &= \sum_{p \leq x} \log \left(1 - \frac{1}{p}\right)^{-1} \\ &= \sum_{p \leq x} \sum_{k=1}^{\infty} \frac{1}{kp^k} \\ &= \sum_{p \leq x} \frac{1}{p} + \sum_{p \leq x} \sum_{k=2}^{\infty} \frac{1}{kp^k} \\ &= \log\log x + \beta_1 + O\left(\frac{1}{\log x}\right) + \beta_2 + \\ &\qquad - \sum_{p>x} \sum_{k=2}^{\infty} \frac{1}{kp^k} \\ &= \log\log x + \beta_1 + \beta_2 + O\left(\frac{1}{\log x}\right) + O\left(\frac{1}{x}\right) \\ &= \log\log x + \beta_1 + \beta_2 + O\left(\frac{1}{\log x}\right).\end{aligned}$$

Ora sia $\beta = \beta_1 + \beta_2$, allora

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = e^{\beta} \log x \cdot e^{O\left(\frac{1}{\log x}\right)}.$$

Poiché $e^t = 1 + O(t)$ in ogni intervallo limitato $[0, t_0]$, e poiché $O(1/\log x)$ è limitato per $x \geq 2$, abbiamo

$$e^{O\left(\frac{1}{\log x}\right)} = 1 + O\left(\frac{1}{\log x}\right).$$

Ne segue che

$$\begin{aligned}\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} &= e^{\beta} \log x \cdot \left(1 + O\left(\frac{1}{\log x}\right)\right) \\ &= e^{\beta} \log x + O(1)\end{aligned}$$

che è la formula di Mertens. ■

PNT su altri pianeti

*** In preparazione. ***

ESERCIZI

Esercizio 6.1 *Siano $n, b \in \mathbb{N}^*$, con $b \geq 2$. Se*

$$n = n_0 + n_1 b + \ldots + n_t b^t$$

è la rappresentazione b-adica di n, si provi che per ogni $j = 0, 1, \ldots, t$ vale:

$$n_j = \left\lfloor \frac{n}{b^j} \right\rfloor - \left(\left\lfloor \frac{n}{b^{j+1}} \right\rfloor b + \left\lfloor \frac{n}{b^{j+2}} \right\rfloor b^2 + \ldots + \left\lfloor \frac{n}{b^t} \right\rfloor b^{t-j} \right).$$

Esercizio 6.2 *Siano $n \in \mathbb{N}^*$ e $p \in \mathbb{P}$. Se $n = p^a m$, con $(p, m) = 1$, si provi che:*

$$\left\lfloor \frac{n+1}{p^j} \right\rfloor = \begin{cases} \left\lfloor \frac{n}{p^j} \right\rfloor + 1 & \text{se } 1 \leq j \leq a, \\ \left\lfloor \frac{n}{p^j} \right\rfloor & \text{se } j > a \end{cases}$$

Esercizio 6.3 *Si provi che per ogni $y \in \mathbb{R}$, vale $\lfloor 2y \rfloor - 2\lfloor y \rfloor \in \{0, 1\}$.*

Esercizio 6.4 *Provare che $\psi(x) = log(m(x))$, dove $m(x)$ è il Minimo Comune Multiplo di tutti gli interi minori od uguali a x.*

Esercizio 6.5 *Assumendo il Teorema dei Numeri Primi, provare che l'insieme $\{p/q | p, q \in \mathbb{P}\}$ è denso in $[0, +\infty)$. (Suggerimento. Dati a, b interi positivi, determinare il limite di p_{an}/p_{bn}. Si usi 6.4.4.)*

Esercizio 6.6 *Provare che esiste una costante C tale che*

$$\int_2^x \frac{\log t \, dt}{t^2} = C + O\left(\frac{1}{x^{1/2}}\right).$$

Esercizio 6.7 *Provare che*

$$\int_2^x \frac{dt}{\log t} = \frac{x}{\log x} + O\left(\frac{1}{(\log x)^2}\right).$$

Co-
me mi dis-
se il mio
maestro
Her-

mite: "In
matematica sia-
mo più servito-
ri che padro-
ni". Per
quanto la
verità ci
sia ancora
sconosciu-
ta, essa ci
preesiste
imponen-
doci inelut-
tabilmente il
sentiero da segui-
re, se non voglia-
mo perderci.
([23])

7 CARATTERI DI GRUPPI ABELIANI

La Teoria dei Caratteri fornisce uno strumento molto potente (spesso essenziale) per dimostrare teoremi circa i gruppi finiti. Quando lavoriamo con gruppi abeliani, gli ingredienti di base di questa teoria sono piuttosto semplici, in quanto un carattere (ordinario) di un gruppo abeliano G altro non è che un omomorfismo da G nel gruppo moltiplicativo del campo complesso. Nonostante ciò le applicazioni possono essere notevoli, un esempio su tutti: la dimostrazione del Teorema 8.2.6 di Dirichlet che affronteremo nel Capitolo successivo.

In breve richiameremo gli aspetti essenziali dei caratteri per i gruppi abeliani. L'intero Capitolo è propedeutico al successivo, pertanto chi già ha una buona familiarità con questi concetti, può decidere di passare oltre. A chi invece ha interesse nell'approfondire la Teoria dei Caratteri in generale, consigliamo le letture di [31] e [32].

COSTRUZIONE DI CARATTERI

Sia G un gruppo abeliano finito. Un *carattere (ordinario)* di G è un omomorfismo di gruppi (moltiplicativi) da G nel gruppo $\mathbb{C}^*$ dei numeri complessi non nulli. Di seguito indicheremo con $\widehat{G}$ l'insieme dei caratteri del gruppo (abeliano) G.

Ricordo che se G è un gruppo abeliano finito, e $g \in G$, allora esiste un intero $k \geq 1$ tale che $g^k = 1_G$, ed il minimo $k \geq 1$ per cui ciò avviene si dice *ordine* dell'elemento g. Inoltre, dal noto Teorema di Lagrange ([8]), discende che l'ordine di ciascun elemento di G divide la cardinalità di G.

Sia χ un carattere di G, e sia $g \in G$ un elemento di ordine k; allora, poiché χ è un omomorfismo

$$\chi(g)^k = \chi(g^k) = \chi(1_G) = 1$$

e quindi $\chi(g)$ deve essere una radice k-esima dell'unità. Pertanto, per ogni carattere χ di un gruppo abeliano finito, l'immagine $\mathrm{Im}\,(\chi)$ è un sottogruppo nel gruppo moltiplicativo $U = U(\mathbb{C}^*)$ di tutte le radici dell'unità del campo complesso.

Esempio 7.1.1 Sia $G = \langle x \rangle$ un gruppo ciclico di ordine $n \geq 1$, e sia g un suo generatore. Allora

$$G = \{\, 1,\, g,\, g^2,\, \ldots,\, g^{n-2},\, g^{n-1} \,\}.$$

Indichiamo con U_n l'insieme delle radici n-esime dell'unità in $\mathbb{C}$, ovvero:

$$U_n = \{ \zeta_{n,k} = e^{\frac{2\pi i}{n}k} \mid 0 \leq k \leq n-1 \}.$$

Ricordo che U_n è un gruppo moltiplicativo ciclico di ordine n, e che un suo generatore è una radice *primitiva* n-esima, ovvero un numero complesso della forma $\zeta_{n,m}$ per qualche m coprimo con n. Inoltre se $\zeta_{n,k} \in U_n$, e $m \in \mathbb{Z}$, $(\zeta_{n,k})^m = \zeta_{n,r}$, dove r è il resto della divisione di km per n.

Fissata una radice n-esima $\zeta_{n,k}$, definiamo, $\chi_k(g) = \zeta_{n,k}$, e per ogni $g^m \in G$,

$$\chi_k(g^m) = (\zeta_{n,k})^m.$$

Si riconosce subito che tale applicazione χ_k così definita è un omomorfismo G in $\mathbb{C}^*$, ovvero è un carattere di G.

Viceversa, sia χ un carattere di $G = \langle g \rangle$. Per quanto osservato sopra, $\chi(g)$ deve essere un elemento di U_n; dunque $\chi(g) = \zeta_{n,k}$, per qualche $0 \leq k \leq n-1$. Ma allora, poiché χ è un omomorfismo, per ogni $g^m \in G$, si ha

$$\chi(g^m) = \chi(g)^m = (\zeta_{n,k})^m = \chi_k(g^m),$$

quindi χ coincide con χ_k. In conclusione, l'insieme dei caratteri di G coincide con l'insieme dei χ_k con $0 \leq k \leq n-1$ (e questi sono tutti distinti).

La discussione dell'esempio contiene in particolare la dimostrazione del seguente

Lemma 7.1.1 *Sia G un gruppo ciclico di ordine n. Allora il numero di caratteri distinti di G è n.*

Osserviamo che, come emerge dall'esempio di sopra, non tutti i caratteri sono omomorfismi iniettivi.

Esempio 7.1.2 Sia $G = A \times B$, il prodotto diretto di due gruppi entrambi ciclici di ordine primo p. Allora G ha ordine p^2, e non è ciclico (ogni suo elemento non identico ha ordine p). Siano a e b rispettivamente generatori di A e di B. Quindi

$$G = \{ (a^r, b^s) \mid 0 \leq r, s \leq p-1 \}.$$

Siano ζ e ξ due fissate radici p-esime dell'unità. Allora, definendo per ogni $(a^r, b^s) \in G$,

$$\chi_{\zeta,\xi}((a^r, b^s)) = \zeta^r \xi^s$$

si ottiene un carattere di G. Viceversa, ogni carattere di G è di questo tipo (e dunque il numero di caratteri distinti di G è uguale a $p^2 = |G|$).

Lasciamo come esercizio dimostrare la seguente

Proposizione 7.1.2 *Sia $G = G_1 \times G_2 \times \cdots \times G_l$ un gruppo prodotto diretto di gruppi abeliani finiti. Siano $\chi_1, \chi_2, \ldots, \chi_l$ caratteri rispettivamente di $G_1, G_2, \ldots, G_l$ rispettivamente. Allora l'applicazione*

$$\chi(g_1, g_2, \ldots, g_l) = \chi_1(g_1)\chi_2(g_2)\cdots\chi_l(g_l)$$

definita per ogni $(g_1, g_2, \ldots, g_l) \in G$, è un carattere di G. Viceversa ogni carattere di G si ottiene in tal modo, per un'unica scelta dei caratteri $\chi_1, \chi_2, \ldots, \chi_l$.

Enunciamo ora, senza dimostrare, il Teorema di struttura per gruppi abeliani finiti (una dimostrazione di questo fatto si trova nell'Appendice al Capitolo).

Teorema 7.1.3 *Ogni gruppo abeliano finito è isomorfo ad un prodotto diretto di gruppi ciclici.*

Da questo Teorema, insieme con la Proposizione 7.1.2 ed il Lemma 7.1.1, si deduce immediatamente la seguente osservazione.

Proposizione 7.1.4 *Sia G un gruppo abeliano finito. Allora il numero di caratteri distinti di G è uguale all'ordine di G.*

PRODOTTO DI CARATTERI

Fissiamo G un gruppo (abeliano) finito e, al solito, denotiamo con $\widehat{G}$ l'insieme dei suoi caratteri. L'applicazione $\chi_0 : G \longrightarrow \mathbb{C}^*$ definita ponendo, per ogni $g \in G$, $\chi_0(g) = 1$, è un carattere di G, ed è chiamato il *carattere principale* di G. Verrà sempre da noi indicato con χ_0.

Siano ora χ e ψ due caratteri del gruppo G. Definiamo il loro *prodotto* ponendo, per ogni $g \in G$,

$$\chi\psi(g) = \chi(g)\psi(g).$$

Si verifica immediatamente che l'applicazione $\chi\psi$ così definita è un carattere di G, e che l'operazione di prodotto è un'operazione associativa e commutativa sull'insieme $\widehat{G}$ dei caratteri di G. Inoltre, chiaramente, il carattere principale χ_0 è l'elemento neutro per il prodotto. Vediamo ora che in $\widehat{G}$ esistono anche gli elementi inversi.

Sia χ un carattere di G. Definiamo il carattere *coniugato* $\overline{\chi}$ di χ, ponendo, per ogni $g \in G$,

$$\overline{\chi}(g) = \overline{\chi(g)},$$

dove $\overline{\chi(g)}$ è il coniugato in $\mathbb{C}$ del numero complesso $\chi(g)$. Si vede subito che anche $\overline{\chi}$ è un carattere di G. Inoltre, per ogni $g \in G$,

tenendo conto che $\chi(g)$ è una radice dell'unità (e quindi ha modulo uguale ad 1),

$$\chi\overline{\chi}(g) = \chi(g)\overline{\chi(g)} = |\chi(g)|^2 = 1 = \chi_0(g),$$

dunque, in $\widehat{G}$, $\chi\overline{\chi} = \chi_0$; pertanto $\overline{\chi}$ è l'inverso di χ rispetto al prodotto di caratteri. Abbiamo dunque provato il seguente risultato.

Teorema 7.2.1 *Sia G un gruppo abeliano finito. Allora, con l'operazione di prodotto, $\widehat{G}$ è un gruppo abeliano dello stesso ordine di G.*

Il gruppo $\widehat{G}$ è chiamato il *duale* del gruppo G.
Osserviamo che, per ogni $g \in G$, ed ogni $\chi \in \widehat{G}$,

$$\overline{\chi}(g) = \chi(g)^{-1} = \chi(g^{-1}).$$

Di fatto, utilizzando l'esercizio 7.3 ed i Teoremi 7.1.2 e 7.1.3, non è difficile provare che se G è un gruppo abeliano finito, allora il gruppo duale $\widehat{G}$ è isomorfo a G.

Osserviamo che sia la definizione di carattere, che l'operazione di prodotto tra caratteri definita sopra, hanno senso anche se G è un gruppo abeliano infinito, ed anche in tal caso si ottiene che $\widehat{G}$ è un gruppo abeliano. Tuttavia, se G non è finito, non è in generale vero che $\widehat{G}$ è isomorfo a G (chi è interessato può provare per proprio conto ad analizzare il caso in cui G è il gruppo additivo $(\mathbb{Z}, +)$ dei numeri interi).

Ora, un'altra osservazione che ci sarà utile

Lemma 7.2.2 *Sia G un gruppo abeliano finito, e sia $1_G \neq x \in G$. Allora esiste un carattere χ di G tale che $\chi(x) \neq 1$.*

Dimostrazione. Se G è un gruppo ciclico, allora la proprietà segue immediatamente dalla costruzione data nell'esempio 7.1.1. Infatti, fissato un generatore g di G, ogni carattere χ che associa ad g una radice primitiva $|G|$-esima dell'unità è iniettivo, e quindi $\chi(x) \neq 1$ per ogni $1_G \neq x \in G$.

Altrimenti, G è (isomorfo ad) un prodotto diretto di gruppi ciclici, per il Teorema 7.1.3. La proprietà segue ora facilmente (i dettagli per esercizio) dal Teorema 7.1.2 e dal caso ciclico. ∎

Un carattere χ di G si dice *reale* se, per ogni $g \in G$, $\chi(g) \in \mathbb{R}$. Dalla definizione segue subito che χ è un carattere reale se e solo se $\chi = \overline{\chi}$. Inoltre, se χ è un carattere reale, allora, per ogni $g \in G$, $\chi(g) = \pm 1$ (dato che 1 e -1 sono le sole radici dell'unità che appartengono a $\mathbb{R}$).

RELAZIONI DI ORTOGONALITÀ

Le relazioni di ortogonalità sono importanti proprietà dei caratteri, che hanno svariate applicazioni.

Teorema 7.3.1 *Siano G un gruppo abeliano finito e $\widehat{G}$ il gruppo dei caratteri di G.*

Per ogni $g \in G$, vale

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & \text{se } g = 1_G \\ 0 & \text{se } g \neq 1_G. \end{cases}$$

Inoltre, per ogni $\chi \in \widehat{G}$, vale

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & \text{se } \chi = \chi_0 \\ 0 & \text{se } \chi \neq \chi_0. \end{cases}$$

Dimostrazione. Poiché $\chi(1_G) = 1$ per ogni $\chi \in \widehat{G}$, e, per la Proposizione 7.1.4, $|\widehat{G}| = |G|$, si ha

$$\sum_{\chi \in \widehat{G}} \chi(1_G) = |G|.$$

Sia quindi $1_G \neq g \in G$. Allora, per il Lemma 7.2.2 esiste un carattere ψ tale che $\psi(g) \neq 1$. Dunque, tenendo conto che, essendo $\widehat{G}$ un gruppo: $\{\psi\chi \mid \chi \in \widehat{G}\} = \widehat{G}$,

$$\psi(g) \cdot \sum_{\chi \in \widehat{G}} \chi(g) = \sum_{\chi \in \widehat{G}} \psi(g)\chi(g) = \sum_{\chi \in \widehat{G}} \psi\chi(g) = \sum_{\chi \in \widehat{G}} \chi(g)$$

e poiché $\psi(g) \neq 1$, deve essere

$$\sum_{\chi \in \widehat{G}} \chi(g) = 0.$$

La seconda parte è analoga. Per il carattere principale si ha

$$\sum_{g \in G} \chi_0(g) = \sum_{g \in G} 1 = |G|.$$

Se $\chi \neq \chi_0$, allora esiste un elemento $a \in G$ tale che $\chi(a) \neq 1$. Ora

$$\chi(a) \cdot \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(a)\chi(g) = \sum_{g \in G} \chi(ag) = \sum_{g \in G} \chi(g)$$

e di conseguenza $\sum_{g \in G} \chi(g) = 0$. ∎

Teorema 7.3.2 *[Relazioni di ortogonalità] Con le stesse notazioni del Teorema precedente, per ogni $a, b \in G$, vale*

$$\sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi}(b) = \begin{cases} |G| & \text{se } a = b \\ 0 & \text{se } a \neq b. \end{cases}$$

Inoltre, per ogni $\chi_1, \chi_2 \in \widehat{G}$, vale

$$\sum_{g \in G} \chi_1(g)\overline{\chi_2}(g) = \begin{cases} |G| & \text{se } \chi_1 = \chi_2 \\ 0 & \text{se } \chi_1 \neq \chi_2. \end{cases}$$

Dimostrazione. Le identità seguono immediatamente da quelle del Teorema precedente. Infatti, se $a, b \in G$,

$$\sum_{\chi \in \widehat{G}} \chi(a)\overline{\chi}(b) = \sum_{\chi \in \widehat{G}} \chi(ab^{-1}).$$

Mentre, se $\chi_1, \chi_2 \in \widehat{G}$,

$$\sum_{g \in G} \chi_1(g)\overline{\chi_2}(g) = \sum_{g \in G} \chi_1\chi_2^{-1}(g),$$

da cui la tesi. ■

APPENDICE

La struttura dei gruppi abeliani finiti

Presentiamo una dimostrazione del Teorema 7.1.3.
Innanzitutto, ricordiamo il seguente criterio per prodotti diretti.

Proposizione 7.4.1 *Siano N ed M due sottogruppi normali di un arbitrario gruppo G. Se avviene che $NM = G$ e $N \cap M = \{1_G\}$, allora*

$$G \simeq N \times M.$$

Dimostrazione. Si veda ad esempio [8], Teorema 3.15. ■

In particolare, se G è un gruppo abeliano ogni sottogruppo è normale, quindi la Proposizione di sopra si applica a qualunque coppia di sottogruppi che soddisfa le ipotesi. Osserviamo anche che, se H e K sono sottogruppi di un gruppo abeliano G, allora il prodotto

$$HK = \{xy \mid x \in H, y \in K\}$$

è sempre un sottogruppo di G.

D'ora in avanti con G intenderemo sempre un gruppo *abeliano* finito.

Lemma 7.4.2 *Siano H e K sottogruppi di G, con K massimale tale che $H \cap K = \{1_G\}$. Sia $x \in G$, e supponiamo che esista un numero primo p tale che $x^p \in K$. Allora $x \in HK = H \times K$.*

Dimostrazione. Osserviamo, innanzi tutto che, siccome $H \cap K = \{1_G\}$, dalla Proposizione 7.4.1 segue che $HK = H \times K$.

Sia $x \in G$ come nelle ipotesi. Se $x \in K$, non c'è nulla da provare. Supponiamo quindi che $x \notin K$. Allora K è un sottogruppo proprio di $\langle K, x\rangle = K\langle x\rangle$, e quindi, per l'assunzione su K, $K\langle x\rangle \cap H \neq \{1_G\}$. Dunque, esistono $y \in K$, $h \in H$, e un intero $t \neq 0$ tali che

$$yx^t = h \neq 1_G.$$

Allora, $x^t = y^{-1}h \in KH$. Se fosse $p|t$, si avrebbe $y^{-1}h = (x^p)^{t/p} \in K$, e pertanto $h \in K$, che, siccome $H \cap K = \{1_G\}$, conduce alla contraddizione $h = 1_G$. Dunque p non divide t, quindi $(p, t) = 1$ ed esistono interi a, b tali che $1 = pa + tb$. Ma allora

$$x = x^{pa+tb} = (x^p)^a(x^t)^b = (x^p)^a(y^{-1}h)^b = (x^{pa}y^{-b})h^b \in KH,$$

come si voleva. ■

Per ogni elemento $g \in G$ denotiamo con $o(g)$ l'ordine di g (cioè il minimo intero positivo non nullo tale che $g^{o(g)} = 1_G$). Allora, $o(g)$ è la cardinalità del sottogruppo ciclico $\langle g\rangle$ generato da g; quindi, per il Teorema di Lagrange,

$$o(g) \text{ divide } |G|.$$

Inoltre, se $n \geq 1$, allora

$$g^n = 1_G \text{ se e solo se } o(g)|n.$$

Infatti, se $d = (n, o(g))$, ed a e b sono interi tali che $na + o(g)b = d$, si ha

$$g^d = g^{na+o(g)b} = g^{na}g^{o(g)b} = (g^n)^a(g^{o(g)})^b = 1_G^a 1_G^b = 1_G$$

e quindi, $o(g) \leq d$, che comporta $o(g) = d$, cioè $o(g)|n$. Viceversa, se n è un multiplo di $o(g)$, è chiaro che $g^n = 1_G$.

Infine ricordiamo che, se $o(g) = n$ e $t \in \mathbb{Z}$, allora si ha

$$o(g^t) = \frac{n}{(n, t)},$$

(la dimostrazione di ciò è lasciata per esercizio); in particolare, se $t|n$ allora $o(g^t) = n/t$.

Lemma 7.4.3 *Siano g e h due elementi di G, i cui ordini sono coprimi. Allora*

$$o(gh) = o(g)o(h).$$

DIMOSTRAZIONE. Esercizio (si cerchi anche di provare che la tesi non vale se gli ordini di g e di h non sono coprimi). ■

Lemma 7.4.4 *Sia g un elemento di G il cui ordine è il massimo possibile. Allora, per ogni $x \in G$, $o(x)|o(g)$.*

DIMOSTRAZIONE. Sia $n = o(g)$. Sia $x \in G$ e sia $r = o(x)$. Poniamo $d = (n, r)$, allora $(n/d, r/d) = 1$. Sia t il massimo fattore di n che è coprimo con n/d, ed u il massimo fattore di r coprimo con r/d. Allora n/t ed r/u sono coprimi, e inoltre $(n/t)(r/u) = [n, r]$.

Ora, per quanto ricordato sopra, $o(g^t) = n/t$, e $o(x^u) = r/u$; quindi, per il Lemma 7.4.3

$$o(g^t x^u) = \frac{n}{t} \cdot \frac{r}{u} = [n, r].$$

Ma allora, per la scelta di g deve essere $n = o(g) \geq o(g^t x^u) = [n, r]$. Quindi $n = [n, r]$ che significa che r divide n. ■

Lemma 7.4.5 *Sia g un elemento di G avente massimo ordine possibile. Allora esiste un sottogruppo K di G tale che $G \simeq \langle g \rangle \times K$.*

DIMOSTRAZIONE. Siano $n = o(g)$ e $K \leq G$ un sottogruppo di G, massimale tra quelli per cui $\langle g \rangle \cap K = \{1_G\}$. Proviamo che

$$G = \langle g \rangle K = \langle g \rangle \times K.$$

Sia $x \in G$, allora esiste un $m \geq 1$ tale che $x^m \in \langle g \rangle K$. Per induzione su m proviamo che $x \in \langle g \rangle K$. Se $m = 1$ la cosa è data. Sia quindi $m \geq 1$ e sia p un divisore primo di n. Allora $(x^{m/p})^p = x^m \in \langle g \rangle K$, e quindi, se $p < m$ si conclude per ipotesi induttiva che $x \in \langle g \rangle K$. Dunque, possiamo supporre che $m = p$ sia un numero primo.

Ora, esiste un elemento $k \in K$ ed un numero intero t tali che $x^p = g^t k$. Osserviamo anche che, per il Lemma 7.4.4, $x^n = 1_G$.

Supponiamo che p non divida n. In tal caso $(p, n) = 1$ ed esistono interi a, b tali che $1 = pa + nb$. Si ha allora

$$x = x^{pa+nb} = (x^p)^a (x^n)^b = (x^p)^a = g^{ta} k^a \in \langle g \rangle K.$$

Possiamo quindi assumere che $p|n$. Allora

$$1_G = x^n = (x^p)^{n/p} = g^{tn/p} k^{n/p}$$

e quindi $g^{tn/p} = (k^{n/p})^{-1} \in \langle g \rangle \cap K = \{1_G\}$. Dunque $g^{tn/p} = 1_G$, e pertanto $n = o(g)$ divide tn/p, da cui segue che p divide t. Allora, posto $y = x^{-1} g^{t/p}$, si ha

$$y^p = (x^p)^{-1} g^t = k^{-1} \in K$$

e quindi, per il Lemma 7.4.2, $x^{-1}g^{t/p} = y \in \langle g \rangle K$. Da ciò segue subito che x appartiene a $\langle g \rangle K$, completando così la dimostrazione. ■

Teorema 7.4.6 *Sia G un gruppo abeliano finito. Allora esistono elementi $g_1, \ldots, g_n$ di G, tali che*

$$G \simeq \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_n \rangle.$$

DIMOSTRAZIONE. Procediamo per induzione sull'ordine di G. Se $G = \{1_G\}$ non c'è nulla da dimostrare. Sia quindi $|G| > 1$, e sia g_1 un elemento di G del massimo ordine possibile. Per il Lemma 7.4.5, esiste un sottogruppo K di G tale che

$$G \simeq \langle g_1 \rangle \times K.$$

Ora $|K| = |G|/|\langle g \rangle| = |G|/o(g) < |G|$, e quindi, per ipotesi induttiva, esistono elementi $g_2, \ldots, g_n$ di K tali che

$$K \simeq \langle g_2 \rangle \times \cdots \times \langle g_n \rangle.$$

Quindi si ha

$$G \simeq \langle g_1 \rangle \times K \simeq \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_n \rangle$$

e la dimostrazione è completa. ■

ESERCIZI

Esercizio 7.1 *Siano G un gruppo ciclico di ordine 12 e g un suo generatore. Sia inoltre $\zeta = \zeta_{12,2} = e^{\frac{2\pi i}{6}}$ una radice 12-esima dell'unità come definita nell'esempio 1. Si determini il nucleo $\ker(\chi_2)$ del carattere χ_2, associato a ζ rispetto al generatore g.*

Esercizio 7.2 *Si provi che nessun carattere del gruppo G dell'esempio 2 è iniettivo.*

Esercizio 7.3 *Sia G un gruppo ciclico di ordine n. Si provi che $\widehat{G}$ è un gruppo ciclico di ordine n (si dimostri che G è isomorfo a $\widehat{G}$).*

Esercizio 7.4 *Sia H un sottogruppo del gruppo abeliano finito G. Si provi che ogni carattere χ di G/H si può "sollevare" ad un carattere χ^G di G, ovvero esiste un carattere χ^G di G tale che, per ogni $g \in G$, si ha*

$$\chi^G(g) = \chi(H + g).$$

Esercizio 7.5 *Si provi che un gruppo abeliano finito G ammette un carattere reale diverso dal carattere principale se e solo se 2 divide l'ordine di G.*

"I even know of a mathematician who slept with his wife only on prime numbered days," Graham said. "It was pretty good early in the month-two, three, five, seven-but got tough toward the end, when the primes are thinner, nineteen, twenty three, then a big gap till twenty-nine. But this guy was seriously nuts. He's now serving twenty years in the Oregon State Penitentiary for kidnapping and attempted murder." [30]

8 PRIMI IN PROGRESSIONI

In questo Capitolo proveremo, con tecniche elementari, un celebre Teorema di Dirichlet: *assegnati due numeri naturali coprimi a e c, esistono infiniti numeri primi congrui ad a modulo c, ovvero la progressione aritmetica $\{a + cn | n \in \mathbb{Z}\}$ contiene infiniti numeri primi.*

CARATTERI DI DIRICHLET

Definizione 8.1.1 Sia $c \in \mathbb{N}^*$. Una applicazione $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$, si dice *carattere di Dirichlet modulo c* se soddisfa alle seguenti condizioni, per ogni $a, b \in \mathbb{Z}$:

1. $\chi(a) = \chi(b)$ se $a \equiv b \, (mod\, c)$;
2. $\chi(a) \neq 0$ se e solo se $(a, c) = 1$;
3. $\chi(ab) = \chi(a)\chi(b)$.

Ad esempio, se p è un numero primo dispari, allora il simbolo di Legendre, definito nel Capitolo 3,

$$\left(\frac{\cdot}{p}\right) : \mathbb{Z} \longrightarrow \mathbb{C}$$
$$a \mapsto \left(\frac{a}{p}\right)$$

è un carattere di Dirichlet modulo p.

Dalla condizione 3. segue subito che ogni carattere di Dirichlet χ è una funzione moltiplicativa, ed in particolare, anche in virtù della condizione 2., $\chi(1) = 1$.

Nel seguito, dato $c \geq 1$, denotiamo con $\mathfrak{D}_c$ l'insieme dei caratteri di Dirichlet modulo c. Al solito, sia $\mathbb{Z}_c$ l'anello $\mathbb{Z}/c\mathbb{Z}$ delle classi di resto modulo c, e indichiamo semplicemente con $\mathbb{Z}_c^*$ il gruppo moltiplicativo degli elementi invertibili di $\mathbb{Z}_c$. Come nel capitolo precedente, il simbolo $\widehat{\mathbb{Z}_c^*}$ rappresenta il gruppo dei caratteri del gruppo abeliano $\mathbb{Z}_c^*$.

Si verifica facilmente che se χ è un carattere di Dirichlet modulo c, allora l'applicazione χ', definita da, per ogni $a + c\mathbb{Z} \in \mathbb{Z}_c^*$,

$$\chi'(a + c\mathbb{Z}) = \chi(a)$$

è un carattere (ordinario) di $\mathbb{Z}_c^*$ [la condizione 1) per i caratteri di Dirichlet assicura che è ben definita, la 2) che la sua immagine è contenuta in $\mathbb{C}^*$, e la 3) che è un omomorfismo di gruppi moltiplicativi].

Viceversa, ad ogni carattere ψ di $\mathbb{Z}_c^*$, si associa χ_ψ, carattere di Dirichlet modulo c, ponendo, per ogni $a \in \mathbb{Z}$:

$$\chi_\psi(a) = \begin{cases} 0 & \text{se } (a,c) \neq 1, \\ \psi(a + c\mathbb{Z}) & \text{se } (a,c) = 1. \end{cases}$$

È immediato verificare che queste corrispondenze sono l'una l'inversa dell'altra, e quindi stabiliscono una biezione tra l'insieme dei caratteri di Dirichlet modulo c ed il gruppo dei caratteri di $\mathbb{Z}_c^*$. In particolare, per il Teorema 7.2.1, il numero di caratteri di Dirichlet modulo c è uguale all'ordine di $\mathbb{Z}_c^*$, che, come sappiamo è uguale a $\phi(c)$. Inoltre, se χ è un carattere di Dirichlet modulo c, allora per ogni a coprimo con c, $\chi(a)$ è una radice $\phi(c)$-esima dell'unità.

Dato un carattere di Dirichlet χ, si definisce in modo naturale il carattere coniugato $\overline{\chi}$ (e si ha $\overline{\chi}' = \overline{\chi'}$), e si dice che un carattere di Dirichlet è *reale* se coincide con il suo coniugato (ovvero se la sua immagine è contenuta in $\mathbb{R}$). Continueremo poi a denotare con χ_0 il carattere di Dirichlet *principale*, ovvero quello definito da

$$\chi_0(a) = \begin{cases} 1 & \text{se } (a,c) = 1, \\ 0 & \text{se } (a,c) \neq 1. \end{cases}$$

Infine, l'operazione di prodotto per caratteri si estende in modo naturale ai caratteri di Dirichlet. A questo punto le relazioni di ortogonalità si ottengono immediatamente da quelle per i caratteri (Teoremi 7.3.1 e 7.3.2).

Teorema 8.1.1 *Siano $c \in \mathbb{N}^*$ e $\mathfrak{D}_c$ l'insieme dei caratteri di Dirichlet modulo c. Per ogni $a \in \mathbb{Z}$,*

$$\sum_{\chi \in \mathfrak{D}_c} \chi(a) = \begin{cases} \phi(c) & \text{se } a \equiv 1 \,(mod\, c), \\ 0 & \text{se } a \not\equiv 1 \,(mod\, c). \end{cases}$$

Sia U un insieme di rappresentati delle classi di congruenza modulo c. Per ogni $\chi \in \mathfrak{D}_c$,

$$\sum_{a \in U} \chi(a) = \begin{cases} \phi(c) & \text{se } \chi = \chi_0, \\ 0 & \text{se } \chi \neq \chi_0. \end{cases}$$

Teorema 8.1.2 *Per ogni $a, b \in \mathbb{Z}$,*

$$\sum_{\chi \in \mathfrak{D}_c} \chi(a)\overline{\chi}(b) = \begin{cases} \phi(c) & \text{se } (a,c) = 1 \text{ e } a \equiv b \,(mod\, c), \\ 0 & \text{altrimenti.} \end{cases}$$

Per ogni $\chi_1, \chi_2 \in \mathfrak{D}_c$,

$$\sum_{a \in U} \chi_1(a)\overline{\chi_2}(a) = \begin{cases} \phi(c) & \text{se } \chi_1 = \chi_2, \\ 0 & \text{se } \chi_1 \neq \chi_2. \end{cases}$$

Lemma 8.1.3 *Sia $2 \leq c \in \mathbb{N}^*$, e sia χ un carattere di Dirichlet modulo c, con $\chi \neq \chi_0$. Sia $\{a_n\}_{n\in\mathbb{N}^*}$ una successione decrescente di numeri reali positivi.*

1. *Se $m, n \in \mathbb{N}^*$, con $n < m$, allora*

$$\left|\sum_{k=n}^{m} \chi(k)a_k\right| < 2\phi(c)a_n.$$

2. *Se inoltre $\lim_{n\to\infty} a_n = 0$, allora è convergente la serie*

$$\sum_{k=1}^{\infty} \chi(k)a_k$$

e per ogni t naturale sufficientemente grande, vale

$$\sum_{k=t+1}^{\infty} \chi(k)a_k = O(a_t).$$

DIMOSTRAZIONE. 1. Siano $n, m \in \mathbb{Z}$, con $n < m$. Per la divisione euclidea, scriviamo $m - n = qc + r$, con $0 \leq r < c$. Allora, l'intervallo (di numeri interi) $n \leq i \leq n + qc - 1$ è l'unione di q sistemi di rappresentanti di classi di congruenza modulo c. Pertanto per il Teorema 8.1.1,

$$\sum_{i=n}^{n+qc-1} \chi(i) = 0$$

e quindi

$$\begin{aligned}\left|\sum_{i=n}^{m} \chi(i)\right| &= \left|\sum_{j=0}^{r} \chi(j+n+qc)\right| \\ &= \left|\sum_{j=0}^{r} \chi(j+n)\right| \\ &\leq \sum_{j=0}^{r} |\chi(j+n)| \leq \phi(c),\end{aligned}$$

poiché tra n ed $n + c - 1$ esistono al più $\phi(c)$ numeri y per cui $\chi(y) \neq 0$ e quindi $|\chi(y)| = 1$.
Per ogni reale $x \geq 0$, definiamo $F(x) = \sum_{n\leq x} \chi(n)$. Sia $\{a_n\}_{n\in\mathbb{N}^*}$ una successione decrescente di numeri reali positivi. Allora, per la prima parte della Proposizione 5.1.1 (somme per parti),

$$\sum_{k=n}^{m} \chi(k)a_k = F(m)a_m - F(n-1)a_n - \sum_{k=n}^{m-1} F(k)(a_{k+1} - a_k).$$

Ma, per quanto osservato sopra, $|F(x)| \leq \phi(c)$; pertanto

$$\left|\sum_{k=n}^{m} \chi(k)a_k\right| < \phi(c)a_n + \phi(c)a_m + \phi(c)\sum_{k=n}^{m-1}(a_k - a_{k+1}) = 2\phi(c)a_n,$$

provando così la prima parte.

2. Supponiamo ora che $\lim_{n\to\infty} a_n = 0$. Allora, per ogni reale $\epsilon > 0$, esiste un intero $n = n(\epsilon)$ tale che

$$a_n < \frac{\epsilon}{2\phi(c)}.$$

Allora, per ogni $m \geq n$, e $s \geq 1$, per la parte precedente, si ha

$$\left|\sum_{k=m}^{m+s} \chi(k)a_k\right| < 2\phi(c)a_m \leq 2\phi(c)a_n < \epsilon.$$

Dunque la serie $\sum_{k=1}^{\infty} \chi(k)a_k$ soddisfa il criterio di Cauchy ed è quindi convergente.
Infine, a patto di scegliere s sufficientemente grande,

$$\begin{aligned}\left|\sum_{k=t+1}^{\infty} \chi(k)a_k\right| &\leq \left|\sum_{k=t+1}^{s} \chi(k)a_k\right| + \left|\sum_{k=s+1}^{\infty} \chi(k)a_k\right| \\ &\leq 2\phi(c)a_{t+1} + \epsilon \\ &\leq Ca_t = O(a_t),\end{aligned}$$

ed il Lemma è così provato. ■

IL TEOREMA DI DIRICHLET

Sia $c \in \mathbb{N}$, $c \geq 2$. Se χ è un carattere non-principale modulo c, poniamo

$$L(\chi) := L(1,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}.$$

Per il Lemma 8.1.3, $L(\chi)$ è un numero complesso.

Esempio 8.2.1 *Ci sono solo due caratteri di Dirichlet modulo 3: il carattere principale ed il simbolo di Legendre (chiamiamolo, per questa volta, λ). Per ogni $a \in \mathbb{Z}$ si ha*

$$\lambda(a) = \begin{cases} 0 & se\ \ a \equiv 0\,(mod\,3) \\ 1 & se\ \ a \equiv 1\,(mod\,3) \\ -1 & se\ \ a \equiv 2\,(mod\,3). \end{cases}$$

Quindi

$$L(\lambda) = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{5} + \ldots = \sum_{h=0}^{\infty} \frac{1}{(3h+1)(3h+2)}.$$

Uno dei passi principali della dimostrazione di Dirichlet è provare che, per ogni carattere non-principale χ, vale $L(\chi) \neq 0$. Vediamo subito il caso dei caratteri reali.

Lemma 8.2.1 *Sia χ un carattere di Dirichlet modulo c, reale (cioè $\chi = \overline{\chi}$) e tale che $\chi \neq \chi_0$. Allora $L(\chi) \neq 0$.*

DIMOSTRAZIONE. Poniamo $f = \chi * \mathbf{1}$, ovvero per ogni $n \in \mathbb{N}^*$,

$$f(n) = \sum_{m|n} \chi(m).$$

Per il Teorema 4.2.1, f è una funzione moltiplicativa. Sia p un primo e $r \geq 1$; poiché χ è un carattere reale, $\chi(p) \in \{0, 1, -1\}$.

- se $\chi(p) = 1$, allora $f(p^r) = r + 1 \geq 1$;
- se $\chi(p) = 0$, allora $f(p^r) = \chi(1) = 1$;
- se $\chi(p) = -1$, allora $f(p^r) = 1, 0$ a seconda se r è pari o dispari.

Poiché f è moltiplicativa si conclude che, per ogni $n \in \mathbb{N}^*$, $f(n) \geq 0$, e che $f(n) \geq 1$ se n è un quadrato.

Per x reale, $x \geq 1$, sia

$$F(x) := \sum_{n \leq x} \frac{f(n)}{\sqrt{n}} = \sum_{n \leq x} \left(\frac{1}{\sqrt{n}} \sum_{m|n} \chi(m) \right).$$

Per quanto osservato sopra, i termini della somma in $F(x)$ sono tutti non negativi, e inoltre

$$F(x) \geq \sum_{k^2 \leq x} \frac{1}{k}$$

e dunque

$$\lim_{x \to \infty} F(x) = \infty.$$

D'altra parte, abbiamo che

$$F(x) = \sum_{n \leq x} \left(\frac{1}{\sqrt{n}} \sum_{m|n} \chi(m) \right) = \sum_{(m,j) \in D} \frac{\chi(m)}{\sqrt{mj}},$$

dove $D = \{(m, j) \in \mathbb{N}^* \times \mathbb{N}^* | mj \leq x\}$. Poniamo

$$D_1 = \{(m, j) \in D | m \leq \sqrt{x}\} \quad \text{e} \quad D_2 = \{(m, j) \in D | m > \sqrt{x}\}.$$

Allora, usando il Lemma 5.1.3,

$$\begin{aligned} F_1(x) &= \sum_{(m,j) \in D_1} \frac{\chi(m)}{\sqrt{mj}} \\ &= \sum_{m \leq \sqrt{x}} \left(\frac{\chi(m)}{\sqrt{m}} \sum_{j \leq x/m} \frac{1}{\sqrt{j}} \right) \\ &= \sum_{m \leq \sqrt{x}} \frac{\chi(m)}{\sqrt{m}} \left(2\sqrt{\frac{x}{m}} + K + O(x^{-1/2}) \right), \end{aligned}$$

con K costante positiva. Da ciò segue

$$F_1(x) = 2\sqrt{x} \sum_{m \le \sqrt{x}} \frac{\chi(m)}{m} + K_2 \cdot O(1) + \frac{1}{\sqrt{x}} \cdot O(1),$$

e dunque, per il Lemma 8.1.3,

$$\begin{aligned} F_1(x) &= 2\sqrt{x} \left(L(\chi) - \sum_{m > \sqrt{x}} \frac{\chi(m)}{m} \right) + O(1) \\ &= 2L(\chi)\sqrt{x} + \sqrt{x}\, O(1/\sqrt{x}) \\ &= 2L(\chi)\sqrt{x} + O(1). \end{aligned}$$

Per quanto riguarda le rimanenti coppie $(m, j) \in D_2$,

$$F_2(x) = \sum_{(m,j) \in D_2} \frac{\chi(m)}{\sqrt{mj}} = \sum_{j \le \sqrt{x}} \frac{1}{\sqrt{j}} \sum_{\sqrt{x} < m \le x/j} \frac{\chi(m)}{\sqrt{m}} ;$$

quindi, applicando il Lemma 8.1.3,

$$|F_2(x)| \le 2\phi(c) \frac{1}{x^{1/4}} \sum_{j \le \sqrt{x}} \frac{1}{\sqrt{j}} \le 2\phi(c) \frac{1}{x^{1/4}} \cdot O(x^{1/4}) = O(1),$$

essendo

$$\sum_{j \le \sqrt{x}} \frac{1}{\sqrt{j}} \le 2x^{1/4} + C + O(x^{-1/4}) = O(x^{1/4}).$$

Pertanto si ottiene

$$F(x) = F_1(x) + F_2(x) = 2L(\chi)\sqrt{x} + O(1) ,$$

che è compatibile con $\lim_{x \to \infty} F(x) = \infty$ soltanto se $L(\chi) \neq 0$. ∎

Siamo ora in grado di definire una funzione associata ad ogni carattere di Dirichlet χ (modulo c). Per ogni $x \in \mathbb{R}_{\ge 1}$, sia

$$T_\chi(x) := \sum_{n \le x} \frac{\chi(n)\Lambda(n)}{n},$$

dove Λ è la funzione di Mangoldt definita in 4.3.

Lemma 8.2.2 *Sia χ_0 il carattere principale modulo c. Allora*

$$T_{\chi_0}(x) = \log x + O(1).$$

Dimostrazione. Osserviamo che l'insieme Δ dei primi che dividono c è finito, e che $\Lambda(n)\chi_0(n) \neq 0$ se e solo se n è potenza di un primo che non appartiene a Δ, ed in tal caso $\chi_0(n) = 1$. Dunque

$$\begin{aligned} T_{\chi_0}(x) &= \sum_{p^i \le x} \frac{\Lambda(p^i)}{p^i} - \sum_{\substack{p^i \le x \\ p \in \Delta}} \frac{\Lambda(p^i)}{p^i} \\ &= \sum_{n \le x} \frac{\Lambda(n)}{n} - \sum_{p \in \Delta} \left(\log p \sum_{p^i \le x} \frac{1}{p^i} \right). \end{aligned}$$

Ora

$$\sum_{p\in\Delta}\log p\sum_{p^i\le x}\frac{1}{p^i}<\sum_{p\in\Delta}\log p\sum_{i=1}^{\infty}\frac{1}{p^i}=\sum_{p\in\Delta}\frac{\log p}{p-1}=O(1),$$

essendo Δ finito. In conclusione, applicando il Lemma 6.5.1,

$$T_{\chi_0}(x)=\sum_{n\le x}\frac{\Lambda(n)}{n}+O(1)=\log x+O(1),$$

come si voleva. ■

Lemma 8.2.3 *Sia χ un carattere di Dirichlet, tale che $\chi\neq\chi_0$. Allora*

1. $L(\chi)T_\chi(x)=O(1)$;
2. $T_\chi(x)=-\log x+L(\chi)R(x)+O(1)$, *dove* $R(x)=\sum_{n\le x}\frac{\chi(n)\mu(n)}{n}\log\frac{x}{n}$.

DIMOSTRAZIONE. 1. Consideriamo la funzione

$$A(x)=\sum_{n\le x}\frac{\chi(n)\log n}{n}.$$

Dato che χ è moltiplicativa e $\log=\Lambda*\mathbf{1}$, si ha che

$$\begin{aligned}A(x)&=\sum_{n\le x}\frac{\chi(n)}{n}\sum_{l|n}\Lambda(l)\\&=\sum_{ml\le x}\frac{\chi(ml)}{ml}\Lambda(l)\\&=\sum_{l\le x}\frac{\chi(l)\Lambda(l)}{l}\sum_{m\le x/l}\frac{\chi(m)}{m}\\&=T_\chi(x)\sum_{m\le x/l}\frac{\chi(m)}{m}\\&=L(\chi)T_\chi(x)-R_1(x),\end{aligned}$$

dove

$$R_1(x)=\sum_{l\le x}\frac{\chi(l)\Lambda(l)}{l}\sum_{m>x/l}\frac{\chi(m)}{m}.$$

Ora, poiché $|\chi(l)|\le 1$, applicando il lemma 8.1.3, si ha che esiste una costante positiva K per cui

$$|R_1(x)|\le\sum_{l\le x}\frac{\Lambda(l)}{l}\left|\sum_{m>x/l}\frac{\chi(m)}{m}\right|<\sum_{l\le x}\left(\frac{\Lambda(l)}{l}K\frac{l}{x}\right)$$

ed, essendo $\sum_{l\le x}\Lambda(l)=\psi(x)\sim x$:

$$|R_1(x)|<\frac{K}{x}\sum_{l\le x}\Lambda(l)\le\frac{K}{x}K_1x=O(1).$$

D'altra parte, per il lemma 8.1.3, $A(x)$ è limitata, cioè $A(x) = O(1)$, e quindi

$$L(\chi)T_\chi(x) = A(x) + R_1(x) = O(1).$$

2. Consideriamo la funzione

$$B(x) = \sum_{n\le x} \frac{\chi(n)}{n} \sum_{m|n} \mu(m) \log \frac{x}{m}.$$

Per il Lemma 4.2.4, abbiamo

$$\begin{aligned} B(x) &= \sum_{n\le x} \frac{\chi(n)}{n} \left(\log x \sum_{m|n} \mu(m) - \sum_{m|n} \mu(m) \log m \right) \\ &= \log x - \sum_{n\le x} \frac{\chi(n)}{n} \sum_{m|n} \mu(m) \log m. \end{aligned}$$

e quindi per il Lemma 4.3.1,

$$B(x) = \log x + \sum_{n\le x} \frac{\chi(n)}{n} \Lambda(n) = \log x + T_\chi(x).$$

D'altra parte, riscrivendo la somma in $B(x)$ usando l'Esercizio 5.1 e tenendo conto che χ è moltiplicativa,

$$\begin{aligned} B(x) &= \sum_{m\le x} \left(\mu(m) \log \frac{x}{m} \sum_{k\le x/m} \frac{\chi(mk)}{mk} \right) \\ &= \sum_{m\le x} \left(\frac{\chi(m)\mu(m)}{m} \log \frac{x}{m} \sum_{k\le x/m} \frac{\chi(k)}{k} \right) \\ &= L(\chi) \sum_{m\le x} \frac{\chi(m)\mu(m)}{m} \log \frac{x}{m} - R_2(x) \\ &= L(\chi)R(x) - R_2(x), \end{aligned}$$

dove abbiamo posto

$$R_2(x) = \sum_{m\le x} \left(\frac{\chi(m)\mu(m)}{m} \log \frac{x}{m} \sum_{k>x/m} \frac{\chi(k)}{k} \right).$$

Valutiamo ora tale termine residuo. Siccome per ogni naturale m, $|\chi(m)\mu(m)| \le 1$,

$$|R_2(x)| \le \sum_{m\le x} \left(\frac{1}{m} \log \frac{x}{m} \left| \sum_{k>x/m} \frac{\chi(k)}{k} \right| \right)$$

e dunque, per il Lemma 8.1.3, esiste un $S > 0$ tale che

$$|R_2(x)| \le \sum_{m\le x} \frac{1}{m} \log \frac{x}{m} \left(S \frac{m}{x} \right) = \frac{S}{x} \sum_{m\le x} \log \frac{x}{m}$$

e, infine, per il Lemma 5.1.2,

$$\begin{aligned}|R_2(x)| &\leq \frac{S}{x}\sum_{m\leq x}(\log x - \log m)\\ &\leq \frac{S}{x}(\lfloor x\rfloor \log x - x\log x + x + O(\log x)) = O(1).\end{aligned}$$

In conclusione, ricordando quanto osservato all'inizio su $B(x)$, e con le notazione per $R(x)$ data nell'enunciato, si ricava

$$\log x + T_\chi(x) = B(x) = L(\chi)R(x) - R_2(x),$$

concludendo la dimostrazione del punto 2. ■

Proposizione 8.2.4 *Sia χ un carattere di Dirichlet, tale che $\chi \neq \chi_0$. Allora*

1. $L(\chi) \neq 0$;
2. $T_\chi(x) = O(1)$.

DIMOSTRAZIONE. 1. Per ogni carattere χ poniamo

$$t(\chi) = \begin{cases} -1 & \text{se } L(\chi) = 0,\\ 0 & \text{se } L(\chi) \neq 0.\end{cases}$$

Per il Lemma precedente, se $\chi \neq \chi_0$, si ha che vale sempre $L(\chi)T_\chi(x) = O(1)$ e quindi

$$T_\chi(x) = t(\chi)\log x + O(1).$$

Tenendo conto del Lemma 8.2.2, si ottiene la seguente diseguaglianza

$$\begin{aligned}\log x + \sum_{\chi\neq\chi_0} t(\chi)\log x + O(1) &= \sum_\chi T_\chi(x)\\ &= \sum_{n\leq x}\frac{\Lambda(n)}{n}\sum_\chi \chi(n) \geq 0.\end{aligned}$$

Ciò implica in particolare (basta considerare un x sufficientemente grande),

$$\sum_{\chi\neq\chi_0} t(\chi) \geq -1.$$

Dunque, esiste al più un solo carattere non principale χ tale che $t(\chi) = -1$, cioè $L(\chi) = 0$. Supponiamo che esista un tale carattere e che sia χ_1; allora, χ_1 non è reale per il Lemma 8.2.1, e chiaramente, $L(\overline{\chi}_1) = 0$. Poiché $\chi_1 \neq \overline{\chi_1}$, questo darebbe una contraddizione. Quindi $L(\chi) \neq 0$ per ogni carattere non principale χ.

2. Segue immediatamente dal punto (i) e dal Lemma 8.2.3. ■

Teorema 8.2.5 *Siano a e c due numeri naturali, con $c \geq 2$, e $(a, c) = 1$. Allora*

$$\sum_{\substack{p \leq x \\ p \equiv a \, (mod \, c)}} \frac{\log p}{p} \geq \frac{\log x}{\phi(c)} + O(1).$$

Dimostrazione. Fissati a e c come nell'ipotesi, denotiamo con $\overline{a}$ l'insieme di tutti i numeri naturali congrui ad a modulo c; consideriamo quindi la funzione, definita per $1 \leq x \in \mathbb{R}$,

$$F(x) = \sum_{\substack{n \leq x \\ n \in \overline{a}}} \frac{\Lambda(n)}{n}.$$

Per definizione di Λ,

$$\begin{aligned} F(x) &\leq \sum_{\substack{1 < p^i \leq x \\ p \in \overline{a}}} \frac{\log p}{p^i} \\ &= \sum_{\substack{p \leq x \\ p \in \overline{a}}} \frac{\log p}{p} + \sum_{\substack{p^2 \leq p^i \leq x \\ p \in \overline{a}}} \frac{\log p}{p^i} \\ &= \sum_{\substack{p \leq x \\ p \in \overline{a}}} \frac{\log p}{p} + \sum_{\substack{p \leq x \\ p \in \overline{a}}} \frac{\log p}{p^2} \left(\sum_{i=0}^{\lfloor \log_p x \rfloor} \frac{1}{p^i} \right) \\ &\leq \sum_{\substack{p \leq x \\ p \in \overline{a}}} \frac{\log p}{p} + \sum_{\substack{p \leq x \\ p \in \overline{a}}} \frac{\log p}{p(p-1)}. \end{aligned}$$

Poiché la serie

$$\sum_{n \leq 1}^{\infty} \frac{\log n}{n(n-1)}$$

è convergente, si ottiene

$$F(x) \leq \sum_{\substack{p \leq x \\ p \in \overline{a}}} \frac{\log p}{p} + O(1).$$

Ora, essendo $(a, c) = 1$, esiste $b \in \mathbb{N}$, tale che

$$ab \equiv 1 \, (mod \, c).$$

Per la Proposizione 8.2.4, ed il Lemma 8.2.2,

$$\sum_{\chi} \chi(b) T_{\chi}(x) = T_{\chi_0}(x) + O(1) = \log x + O(1).$$

Ma, per ogni χ carattere di Dirichlet modulo c, vale che $\chi(b) = \overline{\chi}(a)$; quindi, per la legge di ortogonalità per caratteri di Dirichlet,

$$\begin{aligned}\sum_{\chi} \chi(b) T_{\chi}(x) &= \sum_{\chi} \chi(b) \sum_{n \leq x} \frac{\chi(n)\Lambda(n)}{n} \\ &= \sum_{n \leq x} \frac{\Lambda(n)}{n} \sum_{\chi} \chi(b)\chi(n) \\ &= \sum_{n \leq x} \frac{\Lambda(n)}{n} \sum_{\chi} \overline{\chi}(a)\chi(n) \\ &= \phi(c) \sum_{\substack{n \leq x \\ n \in \overline{a}}} \frac{\Lambda(n)}{n} \\ &= \phi(c) F(x).\end{aligned}$$

Dunque, per quanto provato sopra,

$$\log x + O(1) = \phi(c) F(x) \leq \phi(c) \sum_{\substack{p \leq x \\ p \in \overline{a}}} \frac{\log p}{p} + O(1),$$

da cui segue l'enunciato. ■

Il teorema di Dirichlet ora segue immediatamente

Teorema 8.2.6 (P. G. L. Dirichlet) *Siano a e c due numeri interi tali che $c \geq 1$ e $(a, c) = 1$. Allora esistono infiniti numeri primi della forma $a + cn$ con $n \in \mathbb{Z}$.*

Assegnati due numeri naturali coprimi a e c, ed x numero reale positivo, indichiamo con $\pi(x; a, c)$ il numero di primi positivi $\leq x$ della progressione $a + cn$, $n \in Z$. Il Teorema di Dirichlet appena dimostrato mostra che

$$\lim_{x \to +\infty} \pi(x; a, c) = +\infty.$$

Esiste anche un Teorema dei numeri primi per le progressioni aritmetiche che afferma che

$$\pi(x; a, c) \sim \frac{1}{\phi(c)} \frac{x}{\log x},$$

per $x \to \infty$.

APPENDICE

Patterns e gaps tra primi

*** In preparazione. ***

ESERCIZI

Esercizio 8.1 *Si provi che se p è un numero primo dispari allora il carattere principale χ_0 ed il simbolo di Legendre sono i soli caratteri di Dirichlet reali modulo p.*

*** In preparazione ***

Parte III.

Teoria additiva

"Ra- manujan could remember the
idiosyn- crasies of numbers in an almo-
st uncanny way. It was Littlewood who said
that eve- ry po-
sitive in-
teger was
one of Rama-
nujan's per-
sonal friends.
I re- member
going to see
him once in
Putney. I had rid-
den in taxi-cab
No. 1729,

and remarked
that to me the number seemed
a rather dull one, and that I hoped
it was not an unfavourable omen.
<No,> he reflected, <it is a
very interesting num-
ber; it
is the
small- est
num- ber
ex- pres-
sible as the sum of two cubes in
two different ways.> " ([24])

9 PROBLEMA DI WARING

Il termine Teoria Additiva riassume in modo generico tutte quelle questioni che riguardano la possibilità di rappresentare ogni numero naturale (o ogni numnero naturale sufficientemente grande, oppure appartenente ad un certo sottoinsieme notevole) come somma (finita) di elementi di un prefissato sottoinsieme dei numeri interi (quest'ultimo detto in tal caso *base additiva*).

Concordiamo con Nathanson nel ritenere come archetipo di questa Teoria un noto Teorema dovuto a Lagrange: *ogni numero intero non negativo è somma di quattro quadrati*; detto in altri termini: l'insieme dei quadrati naturali costituisce una base additiva d'ordine quattro.

La Teoria Additiva è in gran parte lo studio delle basi di ordine finito. Basi classiche sono i quadrati, i cubi e più in generale le potenze k-esime; i numeri poligonali e i numeri primi. Due problemi classici associati alle basi additive sono il problema di Waring e la congettura di Goldbach. Tratteremo del primo problema in questo Capitolo ed in parte anche nel successivo, dove verrà esposto un metodo classico di attacco a congetture di questo tipo.

TEOREMA DI LAGRANGE

Teorema 9.1.1 (J.-L. Lagrange) *Ogni numero naturale è somma di* 4 *quadrati.*

Dimostrazione. Useremo la seguente identità (dovuta ad L. Eulero)

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2 \quad (47)$$

dove

$$\begin{aligned} z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_3y_1 - x_2y_4 + x_4y_2 \\ z_4 &= x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2 \ . \end{aligned}$$

Il risultato è banalmente vero per $n = 0, 1, 2$. L'identità (47) assicura quindi che è sufficiente dimostrare il Teorema per ogni primo $p \geq 3$. Sia dunque p un primo dispari.

Sappiamo che ogni intero è congruo modulo p ad una somma di due quadrati (vedi Lemma 3.1.1). Dunque, esistono due interi x ed y tali che $x^2 + y^2 \equiv -1 \pmod{p}$. Tali interi x, y possono essere presi in modo che $0 \leq x, y \leq \frac{p-1}{2}$. Dunque esistono interi non negativi x, y ed m tali che

$$1 + x^2 + y^2 = mp \quad (48)$$

ed inoltre $0 < 1 + x^2 + y^2 < 1 + 2(\frac{p}{2})^2 < p^2$; e quindi

$$0 < m < p \ . \tag{49}$$

Sia ora m_0 il più piccolo intero positivo tale che $m_0 p$ è somma di quattro quadrati. Vogliamo provare che $m_0 = 1$. Per la (48) e la (49), si ha $0 < m_0 < p$.

Siano x_1, x_2, x_3, x_4 interi tali che

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \ . \tag{50}$$

Supponiamo per assurdo, $m_0 \geq 2$, ed analizziamo separatamente i due casi:

1. m_0 è pari;
2. m_0 è dispari.

1. Se m_0 è pari, allora $x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p$ è pari. Dunque si verifica una delle seguenti posssibilità:

- x_1, x_2, x_3, x_4 sono tutti pari;
- x_1, x_2, x_3, x_4 sono tutti dispari;
- x_1, x_2, x_3, x_4 sono due pari e due dispari (in questo caso possiamo assumere che x_1, x_2 siano pari, e x_3, x_4 siano dispari).

In tutti e tre i casi si ha che

$$x_1 + x_2, \ x_1 - x_2, \ x_3 + x_4, \ x_3 - x_4$$

sono interi pari. Ma allora

$$\frac{m_0}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

il che, poichè $\frac{m_0}{2}$ è un intero, contraddice la scelta di m_0.

2. Sia m_0 dispari; e quindi $m_0 \geq 3$. Allora, dividendo ogni x_i per m_0, è possibile trovare interi b_i e y_i, per $i = 1, 2, 3, 4$, tali che

$$y_i = x_i - b_i m_0 \qquad \text{con } |y_i| < \frac{m_0}{2} \ .$$

Osserviamo che, poichè m_0 non divide p, almeno uno degli x_i non è divisibile per m_0, e quindi almeno uno degli y_i è diverso da 0. Dunque

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{m_0}{2}\right)^2 = m_0^2$$

ed inoltre

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \ (\text{mod } m_0)$$

ovvero, mettendo insieme queste due proprietà,

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_1 m_0 \tag{51}$$

per qualche $0 < m_1 < m_0$. Moltiplicando membro a membro le uguaglianze (50) e (51), otteniamo

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = m_0^2 m_1 p,$$

dove gli z_i sono dati dall'identità di Eulero (47). Ora, si osserva che

$$z_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i(x_i - b_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{m_0}.$$

Analogamente si prova che, per $i = 1, 2, 3, 4$, si ha $z_i \equiv 0 \pmod{m_0}$. Esistono quindi interi positivi t_1, t_2, t_3, t_4 tali che

$$z_i = m_0 t_i \qquad \text{per } i = 1, 2, 3, 4.$$

ma allora

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 p$$

che, ancora una volta essendo $0 < m_1 < m_0$, è in contraddizione con la scelta minimale di m_0.

Pertanto, deve essere $m_0 = 1$, e dunque p è somma di quattro quadrati, completando così la dimostrazione del Teorema. ■

Dati $k \geq 1$ sottoinsiemi $A_1, A_2, \ldots, A_k$ di $\mathbb{N}^*$ si definisce la loro *somma* come

$$A_1 + A_2 + \cdots + A_k = \{a_1 + \ldots + a_k | a_i \in A_i, \text{ per } i = 1, \ldots, k\}.$$

In particolare, se $A_1 = A_2 = \cdots = A_k = A$, si pone $A_1 + A_2 + \cdots + A_k = kA$.

Definizione 9.1.1 *Un sottoinsieme A di interi naturali si dice* base (additiva) di ordine finito *se esiste un intero $h \geq 1$ tale che ogni numero naturale è rappresentabile come una somma di al più h elementi di A, ovvero se:* $\mathbb{N} = hA$.

Il Teorema di Lagrange si può quindi enunciare in questo modo

Teorema 9.1.2 (J.-L. Lagrange) *L'insieme dei quadrati naturali è una base di ordine quattro.*

Poiché il numero 7 non è somma di tre quadrati, l'enunciato di sopra è il migliore possibile.

SOMME DI 3 QUADRATI

In questa sezione completiamo lo studio riguardante le somme di quadrati, dimostrando un Teorema di Gauss che caratterizza tutti i numeri (naturali) che sono somme di tre quadrati (Teorema 9.2.6).

La dimostrazione di questo risultato richiede la conoscenza di alcune proprietà delle matrici a coefficienti interi, che richiameremo tra poco, ed il Teorema di Dirichlet (Teorema 8.2.6) dimostrato nel Capitolo 8.

Iniziamo con richiamare alcune proprietà delle forme quadratiche (a coefficienti interi), limitandoci al caso di matrici quadrate di ordine 3 (anche se ciò che diremo vale per matrici quadrate di qualunque ordine). Per le dimostrazioni si rinvia il lettore ad un testo di algebra lineare (ad esempio [34]).

Sia data una matrice *simmetrica*, 3×3, a coefficienti in $\mathbb{Z}$:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{1,2} & a_{2,2} & a_{2,3} \\ a_{1,3} & a_{2,3} & a_{3,3} \end{pmatrix} \in M_3(\mathbb{Z})$$

e sia $x \in \mathbb{Z}^3$ il vettore colonna

$$x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{Z}^3.$$

Si chiama *forma quadratica associata alla matrice* A la funzione nelle tre variabili intere x_1, x_2, x_3 data da

$$\begin{aligned} f_A : \mathbb{Z}^3 &\longrightarrow \mathbb{Z} \\ x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &\longmapsto x^T A x = \sum_{i,j=1}^{3} a_{i,j} x_i x_j. \end{aligned}$$

La forma quadratica f_A si dice *definita positiva* se, per ogni $0 \neq x \in \mathbb{Z}^3$, si ha

$$x^T A x \geq 1 \ .$$

Allo stesso modo in cui si trattano le più familiari forme quadratiche sui reali, non è difficile provare che la forma associata ad A è definita positiva se e solo se i minori principali di A, ovvero: $a_{1,1}$, $\det \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix}$ e $\det(A)$, sono positivi.

Dato un intero n, si dice che la matrice A *rappresenta* n se esiste un $x \in \mathbb{Z}^3$ tale che $x^T A x = n$ (ovvero se n appartiene all'immagine della forma quadratica associata ad A su $\mathbb{Z}^3$).

Due matrici simmetriche (d'ordine 3) a coefficienti in $\mathbb{Z}$ dello stesso ordine si dicono *equivalenti* se esiste una matrice a coefficienti interi U con determinante uguale ad 1, ovvero un $U \in \mathrm{SL}(3, \mathbb{Z})$, tale che

$$B = U^T A U \ .$$

Si verifica facilmente che se una matrice simmetrica intera rappresenta n, allora ogni altra matrice ad essa equivalente rappresenta n. Inoltre, vale il seguente risultato (che è l'analogo del teorema spettrale nel caso di matrici a coefficienti interi).

Proposizione 9.2.1 *Sia A una matrice simmetrica 3×3 a coefficienti interi tale che la forma quadratica ad essa associata sia definita positiva. Allora A è equivalente alla matrice identica I_3. In particolare, gli interi rappresentati da A sono tutti e soli quelli rappresentati da I_3, ovvero quelli del tipo $x_1^2 + x_2^2 + x_3^2$.*

DIMOSTRAZIONE. Si veda ad esempio [46]. ■

Lemma 9.2.2 *Sia n un numero naturale, $n \geq 2$. Se esiste un numero naturale $d \geq 1$ tale che $-d$ è un residuo quadratico modulo $dn - 1$, allora n è somma di tre quadrati interi.*

DIMOSTRAZIONE. Se $-d$ è un residuo quadratico modulo $dn - 1$ (con $d \geq 1$), allora esistono $a_{1,1}, a_{1,2} \in \mathbb{Z}$ tali che

$$a_{1,2}^2 + d = a_{1,1}(dn - 1) = a_{1,1}a_{2,2}$$

dove

$$a_{2,2} := dn - 1 \geq 2d - 1 \geq 1,$$

e quindi anche $a_{1,1} \geq 1$.
Ora, la matrice simmetrica

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & 1 \\ a_{1,2} & a_{2,2} & 0 \\ 1 & 0 & n \end{pmatrix}$$

ha determinante

$$\det(A) = (a_{1,1}a_{2,2} - a_{1,2}^2)n - a_{2,2} = dn - a_{2,2} = 1 \ .$$

Inoltre gli altri due minori principali di A sono $a_{1,1}$ e d, quindi sono positivi, ne segue che la forma quadratica associata ad A è definita positiva. Per la proposizione 9.2.1, A è equivalente alla matrice identica I_3. Si osserva anche che A rappresenta n, infatti

$$(0\ 0\ 1)A(0\ 0\ 1)^T = n \ .$$

Per la Proposizione 9.2.1, anche I_3 rappresenta n, ovvero che n può essere scritto come la somma di tre quadrati interi. ■

Lemma 9.2.3 *Se n è un numero naturale tale che*

$$n \equiv 2 \,(mod\ 4)$$

allora n è somma di tre quadrati interi.

Dimostrazione. Sia n un numero naturale tale che $n \equiv 2 \pmod 4$. Allora

$$(4n, n-1) = 1\ .$$

Per il Teorema 8.2.6 di Dirichlet, la progressione aritmetica

$$\{4nj + (n-1) \mid j \in \mathbb{N}^*\}$$

contiene infiniti numeri primi. È dunque possibile scegliere $j \in \mathbb{N}^*$ tale che il numero

$$p = 4nj + n - 1 = (4j+1)n - 1$$

sia primo. Poniamo $d = 4j+1$, ed osserviamo che

$$p = dn - 1 \equiv 1 \pmod 4.$$

Per il Lemma 9.2.2 è ora sufficiente mostrare che $-d$ è un residuo quadratico modulo p. Sia

$$d = \prod_{i=1}^{k} q_i^{s_i},$$

dove i q_i sono i primi distinti che dividono d. Ora

$$p = dn - 1 \equiv -1 \pmod{q_i}$$

per ogni q_i. Inoltre

$$d \equiv \prod_{q_i \equiv 3 \pmod 4} (-1)^{s_i} \pmod 4,$$

e quindi, poiché $d \equiv 1 \pmod 4$,

$$\prod_{q_i \equiv 3 \pmod 4} (-1)^{s_i} = 1.$$

Ora, essendo $p \equiv 1 \pmod 4$, si ha che -1 è un residuo quadratico modulo p (per il Lemma 3.1.3), ovvero

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

e dunque, applicando la Legge di Reciprocità Quadratica (Teorema 3.2.1),

$$\begin{aligned}\left(\frac{-d}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right) \\ &= \prod_{i=1}^{k}\left(\frac{q_i}{p}\right)^{s_i} = \prod_{i=1}^{k}\left(\frac{p}{q_i}\right)^{s_i} \\ &= \prod_{i=1}^{k}\left(\frac{-1}{q_i}\right)^{s_i} = \prod_{q_i \equiv 3 \pmod 4} (-1)^{s_i} = 1.\end{aligned}$$

Dunque $-d$ è un residuo quadratico modulo p, e la dimostrazione è completa. ■

Lemma 9.2.4 *Ogni numero naturale n tale che*

$$n \equiv 1,\ 3,\ 5\ (mod\ 8)$$

è somma di tre quadrati interi.

DIMOSTRAZIONE. Possiamo chiaramente supporre $n \geq 2$. Poniamo

$$c = \begin{cases} 1 & \text{se } n \equiv 3\ (\mathrm{mod}\ 8) \\ \\ 3 & \text{se } n \equiv 1,\ 5\ (\mathrm{mod}\ 8) \end{cases}$$

Con questa scelta di c abbiamo sempre che

$$\frac{cn-1}{2} \equiv \begin{cases} 1\ (\mathrm{mod}\ 4) & \text{se } n \equiv 1, 3\ (\mathrm{mod}\ 8) \\ 3\ (\mathrm{mod}\ 4) & \text{se } n \equiv 5\ (\mathrm{mod}\ 8). \end{cases}$$

Quindi in particolare,

$$\left(4n,\ \frac{cn-1}{2}\right) = 1.$$

Per il teorema di Dirichlet, esiste allora un primo p della forma

$$p = 4nj + \frac{cn-1}{2}$$

per qualche intero positivo j. Sia $d = 8j + c$; allora

$$2p = (8j + c)n - 1 = dn - 1.$$

Per il Lemma 9.2.2, è ora sufficiente provare che $-d$ è un residuo quadratico modulo $2p$. Per questo è sufficiente provare che $-d$ è un residuo quadratico modulo p. Infatti, se questo è il caso, allora esiste un intero a tale che

$$0 \equiv a^2 + d \equiv (a + p)^2 + d\ (\mathrm{mod}\ p).$$

Ora se a è dispari, si pone $u = a$; se invece a è pari, si pone $u = a + p$. Allora u è dispari, e $u^2 + d$ è pari, e pertanto

$$u^2 + d \equiv 0\ (\mathrm{mod}\ 2p),$$

cioè $-d$ è un residuo quadratico modulo $2p$.

Proviamo dunque che $-d$ è un residuo quadratico modulo p. Siano $q_1, \ldots, q_k$ i primi distinti che dividono d, e sia

$$d = \prod_{i=1}^{k} q_i^{s_i}.$$

Poiché $2p \equiv -1 \pmod{d}$, si ha che, per ogni $i = 1, \ldots, k$,

$$2p \equiv -1 \pmod{q_i} \quad \text{e} \quad (p, q_i) = 1.$$

1. Sia $n \equiv 1, 3 \pmod{8}$. Allora $p \equiv \frac{cn-1}{2} \equiv 1 \pmod{4}$, e

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right) = \prod_{i=1}^{k}\left(\frac{q_i}{p}\right)^{s_i} = \prod_{q_i|d}\left(\frac{p}{q_i}\right)^{s_i}.$$

2. Sia $n \equiv 5 \pmod{8}$; allora $p \equiv \frac{cn-1}{2} \equiv 3 \pmod{4}$, e $d \equiv 3 \pmod{8}$. Denotiamo con U l'insieme dei divisori primi di d che sono congrui a 3 modulo 4; e con T quelli che sono congrui a 1 modulo 4. Allora

$$-1 \equiv d \equiv \prod_{q_i \in U} q_i^{s_i} \equiv \prod_{q_i \in U} (-1)^{s_i} \pmod{4}$$

e quindi

$$\prod_{q_i \in U} (-1)^{s_i} = -1. \tag{52}$$

Applicando opportunamente la Legge di Reciprocità Quadratica, abbiamo che

$$\begin{aligned}
\left(\frac{-d}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = -\left(\frac{d}{p}\right) \\
&= -\prod_{q_i \in T}\left(\frac{q_i}{p}\right)^{s_i} \prod_{q_i \in U}\left(\frac{q_i}{p}\right)^{s_i} \\
&= -\prod_{q_i \in T}\left(\frac{p}{q_i}\right)^{s_i} \prod_{q_i \in U}\left(\frac{p}{q_i}\right)^{s_i} \prod_{q_i \in U}(-1)^{s_i} \\
&= \prod_{q_i \in T}\left(\frac{p}{q_i}\right)^{s_i} \prod_{q_i \in U}\left(\frac{p}{q_i}\right)^{s_i} = \prod_{q_i|d}\left(\frac{p}{q_i}\right)^{s_i}.
\end{aligned}$$

In entrambi i casi, e denotando nei prodotti i primi in congruenza modulo 8,

$$\begin{aligned}
\left(\frac{-d}{p}\right) &= \prod_{q_i|d}\left(\frac{p}{q_i}\right)^{s_i} = \prod_{q_i|d}\left(\frac{2}{q_i}\right)^{s_i}\left(\frac{2p}{q_i}\right)^{s_i} \\
&= \prod_{q_i|d}\left(\frac{2}{q_i}\right)^{s_i} \prod_{q_i|d}\left(\frac{-1}{q_i}\right)^{s_i} \\
&= \prod_{q_i \equiv 3,5 \pmod{8}} (-1)^{s_i} \prod_{q_i \equiv 3,7 \pmod{8}} (-1)^{s_i} \\
&= \prod_{q_i \equiv 5,7 \pmod{8}} (-1)^{s_i}.
\end{aligned}$$

Per concludere, è dunque sufficiente provare che

$$\sum_{q_i \equiv 5,7 \pmod{8}} s_i \equiv 0 \pmod{2}.$$

Osserviamo che, modulo 8,

$$\begin{aligned} d &= \prod_{q_i \equiv 1} q_i^{s_i} \prod_{q_i \equiv 3} q_i^{s_i} \prod_{q_i \equiv 5} q_i^{s_i} \prod_{q_i \equiv 7} q_i^{s_i} \\ &\equiv \prod_{q_i \equiv 3} 3^{s_i} \prod_{q_i \equiv 5} (-3)^{s_i} \prod_{q_i \equiv 7} (-1)^{s_i} \\ &\equiv \prod_{q_i \equiv 3,5} 3^{s_i} \prod_{q_i \equiv 5,7} (-1)^{s_i} \pmod 8. \end{aligned}$$

Se $n \equiv 1,\ 5 \pmod 8$; allora $c = 3$, e

$$d = 8j + 3 \equiv 3 \pmod 8.$$

Questo, per la congruenza di sopra, implica in particolare,

$$\sum_{q_i \equiv 5,7 \pmod 8} s_i \equiv 0 \pmod 2.$$

Se invece $n \equiv 3 \pmod 8$; allora $c = 1$, e

$$d = 8j + 1 \equiv 1 \pmod 8.$$

Anche questo, dal confronto con la congruenza di sopra, implica

$$\sum_{q_i \equiv 3,5 \pmod 8} s_i \equiv 0 \pmod 2,$$

e quindi

$$\sum_{q_i \equiv 5,7 \pmod 8} s_i \equiv 0 \pmod 2.$$

La dimostrazione è così completata. ■

Proposizione 9.2.5 *Ogni numero naturale congruo a 7 modulo 8 non può essere scritto come somma di tre quadrati.*

DIMOSTRAZIONE. Sia x un numero naturale positivo.
Se $x = 2m$ è pari, allora: $x^2 = 4m^2 \equiv 0 \pmod 4$.
Se $x = 2m + 1$ è dispari: $x^2 = (2m + 1)^2 = 4m(m + 1) + 1 \equiv 1 \pmod 8$.
Pertanto, per ogni $x \in \mathbb{N}$,

$$x^2 \equiv 0,\ 1,\ 4 \pmod 8.$$

Da ciò segue subito che se $x, y, z \in \mathbb{N}$,

$$x^2 + y^2 + z^2 \not\equiv 7 \pmod 8$$

che è quello che si voleva. ■

Siamo ora in grado di dimostrare il teorema di Gauss.

Teorema 9.2.6 (Gauss) *Un intero $n \geq 0$* non *può essere scritto come somma di 3 quadrati se e solo se esso è del tipo*

$$n = 4^s(8t + 7),$$

con $s, t \in \mathbb{N}$.

Dimostrazione. Sia Ω l'insieme dei numeri naturali che si possono scrivere come somma di tre quadrati. Incominciamo con l'osservare che se $m \in \mathbb{N}$ vale $m \in \Omega$ se e solo se $4m \in \Omega$. Un'implicazione è ovvia. Per provare l'altra, sia $4m \in \Omega$ e sia

$$4m = x^2 + y^2 + z^2.$$

Allora x, y e z sono necessariamente tutti numeri pari, e quindi

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

Ora, per la Proposizione 9.2.5, per ogni $t \in \mathbb{N}$, $8t + 7 \notin \Omega$. Da ciò scende immediatamente che nessun numero della forma

$$4^s(8t + 7)$$

con $s, t \in \mathbb{N}$, appartiene ad Ω.

Viceversa, sia $n \in \mathbb{N}$. Possiamo scrivere $n = 4^s m$, con $s, m \in \mathbb{N}$ univocamente determinati. Per i Lemmi 9.2.3 e 9.2.4 se

$$m \equiv 2 \pmod 4 \qquad \text{oppure} \qquad m \equiv 1,\ 3,\ 5 \pmod 8$$

allora m, e quindi n, appartiene ad Ω. Dunque, se $n \notin \Omega$, allora m deve essere $\equiv 7 \pmod 8$ e ciò completa la dimostrazione. ∎

IL PROBLEMA DI WARING E LE FUNZIONI g E G

Il Teorema 9.1.1, enunciato da Fermat, fu dimostrato da Lagrange nel 1770 (più o meno con la stessa procedura che abbiamo utilizzato noi). In quello stesso anno, Edward Waring, nel suo libro *Meditationes Algebricae*, affermò, senza provarlo, che ogni numero intero può essere espresso come somma di al più 9 cubi, e di al più 19 quarte potenze. Più tardi, nell'edizione del 1782, egli aggiunse le seguenti parole

> *"Omnis integer numerus est quadratus; vel e duobus, tribus vel quatuor quadratis compositus. Omnis integer numerus vel est cubus; vel e duobus, tribus, 4, 5, 6, 7, 8, vel novem cubis compositus: est etiam quadrato-quadratus; vel e duobus, tribus, &c. usque ad novemdecim compositus, & sic deinceps: consimilia etiam affirmari possunt (exceptis excipiendis) de eodem numero quantitatum earundem dimensionum."* (E. Waring [63]).

Ovvero, congettura che *per ogni $k \geq 2$ esista un intero $s = s(k)$ tale che ogni numero naturale possa scriversi come somma di al più s potenze k-esime*. Tale congettura, nota come *problema di Waring*, fu risolta solo nel 1909 dal matematico tedesco D. Hilbert. In seguito G. H. Hardy e J. E. Littlewood hanno fornito una dimostrazione semplificata di tale risultato, dimostrazione che è stata poi ulteriormente migliorata dal matematico russo I. M. Vinogradov. Solo nel 1943, Yu. V. Linnik fornì una dimostrazione di teoria elementare dei numeri ([38]), che utilizza il metodo di Schnirel'man che vedremo in dettaglio nel prossimo Capitolo.

Terminiamo questa sezione con qualche considerazione circa il più piccolo numero di potenze k-esime che compare nel problema di Waring. Nella letteratura moderna, fissato un $k \in \mathbb{N}^*$ si è soliti indicare con $g(k)$ il minimo valore possibile per cui *ogni* intero n si scrive come

$$n = x_1^k + x_2^k + \ldots + x_{g(k)}^k,$$

per qualche $x_i \in \mathbb{N}$. Il Teorema di Lagrange (e il fatto che 7 non è somma di tre quadrati) risolve completamente il caso $k = 2$.

Corollario 9.3.1 $g(2) = 4$.

Il caso $n = 3$ fu risolto indipendentemente da Wieferich e da Kempner intorno al 1910 ([64] e [35]); essi provarono quanto già congetturato da Waring, cioè che $g(3) = 9$ (ovvero che ogni numero naturale può essere espresso come somma di 9 cubi interi, e che esistono numeri naturali che non sono somma di otto cubi). Successivamente altri matematici provarono che $g(4) = 19$ (nel 1986, [5]) e $g(5) = 37$ (1964, [9]).
Una stima inferiore generale per la funzione g fu trovata da Johann Eulero (figlio del grande Leonhard).

Proposizione 9.3.2 (J. A. Eulero) *Siano $k \geq 2$ e $\alpha = (\frac{3}{2})^k$. Allora*

$$g(k) \geq 2^k + \lfloor \alpha \rfloor - 2.$$

Dimostrazione. Con le notazioni dell'enunciato, sia $n = 2^k \lfloor \alpha \rfloor - 1$. Allora

$$n \leq 2^k (3/2)^k - 1 = 3^k - 1 < 3^k.$$

Dunque, in una espressione di n come somma di potenze k-esime i soli addendi non nulli che compaiono sono 1^k e 2^k. Chiaramente, il numero minimo necessario di addendi del tipo 2^k si ottiene come quoziente della divisione di n per 2^k:

$$n = (\lfloor \alpha \rfloor - 1)2^k + (2^k - 1)1^k.$$

Ne segue che per ottenere n come somma di potenze k-esime sono necessari almeno $\lfloor \alpha \rfloor - 1$ addendi uguali a 2^k e $2^k - 1$ addendi uguali a $1 = 1^k$. Pertanto

$$g(k) \geq \lfloor \alpha \rfloor - 1 + 2^k - 1 = 2^k + \lfloor \alpha \rfloor - 2,$$

il che completa la dimostrazione. ■

Per $n = 2, 3$ e 4 la disuguaglianza della Proposizione precedente fornisce rispettivamente

$$g(3) \geq 9, \quad g(4) \geq 19, \quad g(5) \geq 37$$

che sono, di fatto, i valori corretti. Lavori seguenti di diversi matematici (citiamo solamente Niven [48]) hanno portato al seguente

Teorema 9.3.3 *Siano $k \geq 2$, $\alpha = (3/2)^k$ e $\beta = (4/3)^k$, allora*

$$g(k) = \begin{cases} 2^k + \lfloor \alpha \rfloor - 2 & \text{se } 2^k \{\alpha\} + \lfloor \alpha \rfloor \leq 2, \\ 2^k + \lfloor \alpha \rfloor + \lfloor \beta \rfloor - 2 & \text{se } 2^k \{\alpha\} + \lfloor \alpha \rfloor > 2 \quad e \\ & \qquad \lfloor \beta \rfloor \lfloor \alpha \rfloor + \lfloor \beta \rfloor + \lfloor \alpha \rfloor = 2^k, \\ 2^k + \lfloor \alpha \rfloor + \lfloor \beta \rfloor - 3 & \text{se } 2^k \{\alpha\} + \lfloor \alpha \rfloor > 2 \quad e \\ & \qquad \lfloor \beta \rfloor \lfloor \alpha \rfloor + \lfloor \beta \rfloor + \lfloor \alpha \rfloor > 2^k. \end{cases}$$

Nel 1957, K. Mahler ([41]) ha provato (in modo non costruttivo) che esiste al più un numero finito di valori k per cui $2^k \{\alpha\} + \lfloor \alpha \rfloor > 2$; nel 1990 Kubina and Wunderlich ([36]) hanno mostrato che questi eventuali valori di k devono soddisfare $k > 471.600.000$.

Non è noto nessun valore di k per cui valga $2^k \{\alpha\} + \lfloor \alpha \rfloor > 2$. Si congettura che il valore effettivo di $g(k)$ sia quello espresso dalla Proposizione 9.3.2, ovvero $2^k + \lfloor (3/2)^k \rfloor - 2$, per ogni k.

Abbiamo accennato che $g(3) = 9$, ovvero che ogni naturale positivo è somma di nove cubi (ed esistono numeri che non sono somma di otto cubi). Nel 1939 L. E. Dickson ([14]) provò che 23 e 239 sono *i soli* numeri naturali che richiedono almeno nove cubi. Più tardi, nel 1943, Yu. V. Linnik dimostrò, in [39], che ogni numero naturale *sufficientemente grande* può essere rappresentato come somma di 7 cubi. Questo porta a definire in modo naturale una nuova funzione, chiamata $G(k)$, come il minimo valore s, tale che ogni numero intero *sufficientemente grande* può essere espresso come somma di s potenze k-esime. Dal teorema di Lagrange e dalla Proposizione 9.2.5, discende che $G(2) = 4$. Il citato risultato di Linnik dice inoltre che $G(3) \leq 7$. La determinazione dei valori di $G(k)$ è un problema in larga parte ancora aperto; i soli valori esatti conosciuti (a Luglio 2017) sono $G(2) = 4$ e $G(4) = 16$ (Davenport 1939, [12]).

Vediamo ora una semplice stima inferiore per la funzione G.

Lemma 9.3.4 *Sia $1 \leq h \in \mathbb{N}$ fissato. Allora, per ogni $1 \leq n \in \mathbb{N}$ vale*

$$\sum_{j=0}^{n} \frac{(j+1)\dots(j+h)}{h!} = \frac{(n+1)\dots(n+h+1)}{(h+1)!}.$$

Dimostrazione. Esercizio (induzione su n). ■

Teorema 9.3.5 *Per ogni numero naturale $k \geq 2$,*

$$G(k) \geq k+1.$$

DIMOSTRAZIONE. Fissato $k \geq 2$, per ogni naturale N denotiamo con $A(N)$ il numero di numeri naturali $n \leq N$ che sono rappresentabili nella forma

$$n = x_1^k + x_2^k + \cdots + x_k^k, \tag{53}$$

dove $x_i \in \mathbb{N}$, per $i = 1, 2, \ldots, k$. Osserviamo $A(N) \leq B_k(N)$, dove $B_k(N)$ è il numero di k-uple $(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$ tali che

$$0 \leq x_1 \leq x_2 \leq \cdots \leq x_k \leq N^{\frac{1}{k}}.$$

Proviamo, per induzione su k, che

$$B_k(N) = \frac{1}{k!} \prod_{r=1}^{k} \left(\left\lfloor N^{\frac{1}{k}} \right\rfloor + r \right).$$

Per $k = 1$ si trova subito che $B_1(N) = \lfloor N^{\frac{1}{k}} \rfloor + 1$ (stiamo contando anche lo zero), che è ciò che fornisce anche la formula da provare.
Sia $k \geq 2$, e poniamo $t = \lfloor N^{\frac{1}{k}} \rfloor$. Allora, applicando l'ipotesi induttiva (e chiamando $j = x_k$),

$$\begin{aligned} B_k(N) &= \sum_{j=0}^{t} B_{k-1}(j^k) = \sum_{j=0}^{t} \frac{1}{(k-1)!} \prod_{r=1}^{k-1} (j+r) \\ &= \sum_{j=0}^{t} \frac{(j+1)(j+2)\ldots(j+k-1)}{(k-1)!}. \end{aligned}$$

Pertanto, per il Lemma 9.3.4,

$$B_k(N) = \frac{(t+1)(t+2)\ldots(t+k)}{k!}$$

come si voleva. Osserviamo a questo punto che

$$\lim_{N\to\infty} \frac{B_k(N)}{N/k!} = 1. \tag{54}$$

Supponiamo, per assurdo, che si abbia $G(k) \leq k$, cioè che tutti i numeri naturali n, tranne un numero finito siano rappresentabili nella forma (53). In tal caso, esiste un $C \geq 0$, indipendente da N, tale che

$$B_k(N) \geq A(N) > N - C.$$

Ma ciò implica in particolare

$$\lim_{N\to\infty} \frac{N}{B_k(N)} \leq 1,$$

in contraddizione con il limite (54). Dunque $G(k) \geq k+1$. ∎

Oggigiorno la migliore stima superiore trovata per $G(k)$ è data dal seguente risultato di Wooley ([67])

Teorema 9.3.6 *Per k sufficientemente grande*

$$G(k) < (1+c)k\log k,$$

per ogni costante positiva c.

Il lettore interessato può consultare la survey [61].

APPENDICE

Taxi-cab numbers

ESERCIZI

Esercizio 9.1 *Si provi che ogni numero naturale n con $n \equiv 3 \pmod 8$, è somma di tre quadrati dispari.*

Esercizio 9.2 *Sfruttando la seguente identità*

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

si provi che $g(4) \leq 50$.

Esercizio 9.3 *Si provi che $G(4) \geq 16$.*

"ϵ"
was Erdös's word for a
small child. His
langua-
ge
had a spe-
cial voca-
bulary -
not just
"the SF"
and "epsilon" but also "bos-
ses" (women), "slaves" (men),
"captured"
(married),
"liberated"
(divorced),
"recaptured"
(remarried), "noi-
se" (music), "poi- son"
(alcohol), "preaching" (giving
a mathematics lecture).
([30])

10 IL METODO DI SCHNIREL'MAN

In questo Capitolo esporremo uno strumento semplice quanto molto efficace della teoria additiva: il cosiddetto *metodo di Schnirel'man*.

Questo fu sviluppato intorno al 1930 dal matematico russo Lev Genrikhovich Schnirel'man, e sostanzialmente consiste in un criterio molto utile per stabilire quando un prefissato sottoinsieme A di $\mathbb{N}$ è una base additiva d'ordine finito, ovvero qunado ogni numero naturale è somma di un numero *limitato* di elementi di A.

Nel corso del Capitolo, forniremo due esempi significativi del metodo. Il primo è legato alla congettura di Goldbach, ed è la dimostrazione di Schnirel'man che ogni intero > 1 è somma di un numero limitato di primi. Il secondo esempio invece è la dimostrazione data da Yu. V. Linnik del problema di Waring per i polinomi, di cui si è accennato nel Capitolo precedente. In entrambi, i casi non daremo dimostrazioni complete dei due risultati, in quanto presteremo degli atti di fede su due stime asintotiche una dovuta ad A. Selberg e l'altra a Linnik. Entrambe le formule sono dimostrate sui libri di Nathanson, rispettivamente [45] e [46].

IL TEOREMA DI SCHNIREL'MAN

Se A è un sottoinsieme di $\mathbb{N}$ ed $n \in \mathbb{N}$, poniamo

$$A(n) = |\{a \in A \mid 0 < a \leq n\}| = \sum_{\substack{1 \leq a \leq n \\ a \in A}} 1.$$

Più in generale, dato x un numero reale positivo, poniamo

$$A(x) = \sum_{\substack{1 \leq a \leq x \\ a \in A}} 1.$$

È ovvio che per ogni $x \in \mathbb{R}_{>0}$, $0 \leq A(x) \leq \lfloor x \rfloor$.

Definizione 10.1.1 *Dato un sottonsieme A dei numeri naturali si dice* densità di Schnirel'man *di A il valore*

$$d^S(A) = \inf_{n \geq 1} \frac{A(n)}{n}.$$

Le seguenti proprietà sono ovvie:

1. $0 \leq d^S(A) \leq 1$;

2. se $1 \notin A$, allora $d^S(A) = A(1) = 0$;

3. se $d^S(A) = \alpha$, allora $A(x) \geq \alpha x$ per ogni $x \in \mathbb{R}_{\geq 1}$;

4. $d^S(A) = 1$ se e solo se $A = \mathbb{N}$.

Definiamo inoltre la *densità asintotica di Schnirel'man* dell'insieme A come

$$d_L^S(A) = \liminf_{n\to\infty} \frac{A(n)}{n}.$$

Abbiamo che

Proposizione 10.1.1 *Sia A un sottoinsieme di $\mathbb{N}$ contenente il numero 1. Se $d_L^S(A) > 0$ allora $d^S(A) > 0$.*

Dimostrazione. Sia $d_L^S(A) = \alpha > 0$, allora esiste un $x_0 \in \mathbb{R}$ positivo tale che per ogni $x > x_0$ vale $A(x) \geq \frac{\alpha}{2}x$. Poiché $1 \in A$, esiste una costante positiva c_1 tale che $A(x) \geq c_1 x$, per ogni $1 \leq x \leq x_0$. Detto $c = \min\left\{\frac{\alpha}{2}, c_1\right\}$, allora $c > 0$ e $A(x) \geq cx$ per ogni x reale positivo, quindi $d^S(A) = \inf_{n\in\mathbb{N}^*} \frac{A(n)}{n} > 0$. ∎

Richiamiamo le definizioni date nel Capitolo precedente (pagina 164).

Definizione 10.1.2 *Dati due sottoinsiemi A e B dei numeri naturali si definisce la* somma *$A + B$ come l'insieme*

$$A + B = \{a + b | a \in A,\ b \in B\}.$$

Analogamente, dati k insiemi $A_1, A_2, \ldots, A_k$ si definisce la loro somma

$$A_1 + A_2 + \cdots + A_k = \{a_1 + \ldots + a_k | a_i \in A_i,\ \text{per } i = 1, \ldots, k\}.$$

In particolare, se $A_1 = A_2 = \cdots = A_k = A$, si pone $A_1 + A_2 + \cdots + A_k = kA$.

Definizione 10.1.3 *Un sottoinsieme A di interi naturali si dice* base (additiva) di ordine finito *se esiste un intero $h \geq 1$ tale che ogni numero naturale è somma di h elementi di A, ovvero se: $\mathbb{N} = hA$.*

Proveremo il seguente importante risultato di Schnirel'man

Teorema 10.1.2 (L. Schnirel'man) *Se A è un sottoinsieme di $\mathbb{N}$ che contiene lo zero e tale che $d^S(A) > 0$, allora A è una base additiva d'ordine finito per $\mathbb{N}$.*

Lemma 10.1.3 *Siano $A, B \subseteq \mathbb{N}$, con $0 \in A \cap B$. Preso un naturale n, se $A(n) + B(n) \geq n$ allora $n \in A + B$.*

DIMOSTRAZIONE. Se $n \in A$, o $n \in B$ la dimostrazione è banale. Sia dunque $n \notin A \cup B$. Poniamo

$$A' = \{n - a | a \in A,\ 1 \leq a \leq n-1\}$$
$$B' = \{b \in B | 1 \leq b \leq n-1\}$$

Allora $|A'| = A(n)$ e $|B'| = B(n)$, poiché $n \notin A \cup B$. Inoltre $A' \cup B' \subseteq \{1, 2, \dots, n-1\}$, dunque

$$|A'| + |B'| = A(n) + B(n) \geq n$$

e pertanto $A' \cap B' \neq \varnothing$. Ne segue che esistono $a \in A$ e $b \in B$ tali che $n - a = b$, ovvero $n = a + b$. ∎

Lemma 10.1.4 *Siano $A, B \subseteq \mathbb{N}$, con $0 \in A \cap B$. Se $d^S(A) + d^S(B) \geq 1$ allora $n \in A + B$, per ogni $n \in N$.*

DIMOSTRAZIONE. Sia $\alpha = d^S(A)$ e $\beta = d^S(B)$. Preso $n \geq 0$ abbiamo che

$$A(n) + B(n) \geq \alpha n + \beta n = (\alpha + \beta)n \geq n.$$

Il Lemma 10.1.3 completa la dimostrazione. ∎

Lemma 10.1.5 *Sia $0 \in A \subseteq \mathbb{N}$. Se $d^S(A) \geq \frac{1}{2}$, allora A è una base finita d'ordine due.*

DIMOSTRAZIONE. Basta prendere $B = A$ nel Lemma precedente. ∎

Il seguente risultato è cruciale per il proseguo.

Teorema 10.1.6 *Per ogni coppia di sottoinsiemi A e B di $\mathbb{N}$, contenenti entrambi lo zero, si ha*

$$d^S(A + B) \geq d^S(A) + d^S(B) - d^S(A)d^S(B).$$

DIMOSTRAZIONE. Sia $A := \{0 = a_0, a_1, a_2, \dots\}$, e supponiamo che i suoi elementi siano ordinati, ovvero che

$$a_0 < a_1 < a_2 < \dots$$

Per ogni numero naturale i, poniamo

$$l_i := a_{i+1} - a_i - 1.$$

Osserviamo che, se $l_i \geq 1$, allora

$$a_i + 1,\ a_i + 2, \dots, a_i + l_i \notin A.$$

D'altra parte, nell'insieme $\{1, 2, \dots, l_i\}$ ci sono $B(l_i)$ elementi di B; e quindi nell'insieme $\{a_i + 1,\ a_i + 2, \dots, a_i + l_i\}$ ci sono almeno

$B(l_i)$ elementi di $A+B$. Da ciò non è difficile dimostrare (lo si faccia per esercizio!) che, per ogni numero naturale $n \geq 1$,

$$(A+B)(n) \geq A(n) + \sum_{i=0}^{A(n)-1} B(l_i) + B(n - a_{A(n)}).$$

Per la definizione di densità di Schnirel'man, si ha quindi

$$\begin{aligned}(A+B)(n) &\geq A(n) + d^S(B)\left\{\sum_{i=0}^{A(n)-1} l_i + n - a_{A(n)}\right\} \\ &= A(n) + d^S(B)(n - A(n)) \\ &= A(n)(1 - d^S(B)) + nd^S(B) \\ &\geq nd^S(A)(1 - d^S(B)) + nd^S(B).\end{aligned}$$

Ma allora, per ogni numero naturale $n \geq 1$

$$\frac{(A+B)(n)}{n} \geq d^S(A) + d^S(B) - d^S(A)d^S(B),$$

e quindi

$$d^S(A+B) \geq d^S(A) + d^S(B) - d^S(A)d^S(B),$$

come si voleva. ■

Corollario 10.1.7 *Dati $h \geq 1$ sottoinsiemi A_j di $\mathbb{N}$ tali che $0 \in \bigcap_{i=1}^{h} A_i$, si ha*

$$1 - d^S(A_1 + A_2 + \ldots + A_h) \leq \prod_{i=1}^{h}(1 - d^S(A_i)).$$

Dimostrazione. Fare induzione su h. ■

Siamo ora in grado di provare il Teorema di Schnirel'man.

Dimostrazione del Teorema 10.1.2.
Sia $d^S(A) = \alpha > 0$. Allora $0 < \alpha \leq 1$ e quindi $0 \leq 1 - \alpha < 1$. Esiste pertanto un intero $l \geq 1$ per cui

$$0 \leq (1-\alpha)^l \leq \frac{1}{2}.$$

Per il Corollario 10.1.7 abbiamo che

$$1 - d^S(lA) \leq (1 - d(A))^l = (1-\alpha)^l \leq \frac{1}{2}$$

e quindi $d^S(lA) \geq 1/2$. Il Lemma 10.1.5 implica allora che lA è una base additiva d'ordine 2 per $\mathbb{N}$. Ma allora A è base additiva d'ordine $2l$ per $\mathbb{N}$. ■

Osserviamo che il Teorema appena dimostrato non si inverte. Ad esempio se indichiamo con

$$A = \left\{ m^2 | m \in \mathbb{N} \right\},$$

allora è evidente che $0 \in A$. Inoltre, per ogni $n \in \mathbb{N}$:

$$A(n) = \sum_{\substack{1 \leq a \leq n \\ a \in A}} 1 = \sum_{1 \leq m^2 \leq n} 1 = \lfloor \sqrt{n} \rfloor$$

e pertanto $d^S(A) = 0$; mentre per il Teorema 9.1.1 di Lagrange A è una base additiva d'ordine quattro.

IL TEOREMA DI GOLDBACH-SCHNIREL'MAN

Come prima applicazione del metodo di Schnirel'man (esposto nella sezione precedente), proviamo il seguente

Teorema 10.2.1 (Goldbach-Schnirel'man) *Ogni numero intero maggiore di uno è somma di un numero limitato di primi.*

Come già osservato nell'introduzione di questo Capitolo, lo spazio di queste note, ed il tempo a nostra disposizione, non ci consentono di fornire una dimostrazione completa di questo Teorema. I lettori sono quindi invitati a prestare un atto di fede su una stima asintotica profonda, dovuta ad A. Selberg (Teorema 10.2.3). Invitiamo i più scettici (e coraggiosi) di voi a consultare [45, Capitolo 7] per una dimostrazione di questa stima.

Incominciamo con l'osservare che se indichiamo con $A = \{0, 1\} \cup \mathbb{P}$, applicando il Teorema 6.2.1 di Čhebyshev,

$$A(x) = \sum_{\substack{1 \leq a \leq x \\ a \in A}} 1 = \pi(x) + 1 \ll \frac{x}{\log x},$$

per ogni x sufficientemente grande. Pertanto $d^S(A) = 0$ e il Teorema 10.1.2 non si può applicare direttamente.

L'idea semplice, quanto geniale, di Schnirel'man è quella di lavorare sull'insieme

$$A = \{0, 1\} \cup 2\mathbb{P} = \{0, 1\} \cup \{ p + q | p, q \in \mathbb{P} \}.$$

Dato un numero naturale $N \in \mathbb{N}$, indichiamo con $r(N)$ il numero di rappresentazioni (ordinate) di N come somma di due primi. Ad esempio $r(10) = 3$, poiché

$$\begin{aligned} 10 &= 3 + 7 \\ &= 5 + 5 \\ &= 7 + 3 \end{aligned}$$

È immediato accorgersi che se N è un numero dispari, allora

$$r(N) = \begin{cases} 0 & \text{se } N-2 \notin \mathbb{P} \\ 2 & \text{se } N-2 \in \mathbb{P} \end{cases}$$

Lemma 10.2.2 $\sum_{N \leq x} r(N) \gg \frac{x^2}{(\log x)^2}$.

Dimostrazione. Se $p, q \in \mathbb{P}$ e $p, q \leq x/2$, allora $p+q \leq x$, quindi

$$\sum_{N \leq x} r(N) \geq (\pi(x/2))^2 \gg \left(\frac{x/2}{\log(x/2)}\right)^2 \gg \frac{x^2}{(\log x)^2},$$

per il risultato di Čhebyshev (Teorema 6.2.1). ∎

Il risultato che segue è tutt'altro che immediato, ed è frutto di un metodo elementare molto elegante elaborato da Atle Selberg.

Teorema 10.2.3 (A. Selberg) *Se N è un numero pari sufficientemente grande*

$$r(N) \leq \frac{N}{(\log N)^2} \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

Dimostrazione. Si veda [45, Theorem 7.2]. ∎

Lemma 10.2.4 $\sum_{N \leq x} (r(N))^2 \ll \frac{x^3}{(\log x)^4}$.

Dimostrazione. Se n è pari, per il risultato di Selberg, abbiamo che

$$r(N) \ll \frac{N}{(\log N)^2} \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \ll \frac{N}{(\log N)^2} \sum_{d \mid N} \frac{1}{d}.$$

La qual cosa vale anche per N dispari (essendo $r(N) \leq 2$).
Abbiamo allora che

$$\begin{aligned}
\sum_{N\leq x}(r(N))^2 &\ll \sum_{N\leq x}\frac{N^2}{(\log N)^4}\left(\sum_{d|N}\frac{1}{d}\right)^2\\
&\ll \frac{x^2}{(\log x)^4}\sum_{N\leq x}\left(\sum_{d|N}\frac{1}{d}\right)^2\\
&\leq \frac{x^2}{(\log x)^4}\sum_{N\leq x}\sum_{d_1|N}\sum_{d_2|N}\left(\frac{1}{d_1 d_2}\right)\\
&\leq \frac{x^2}{(\log x)^4}\sum_{d_1,d_2\leq x}\frac{1}{d_1 d_2}\sum_{\substack{N\leq x\\ d_1|N\\ d_2|N}}1\\
&= \frac{x^2}{(\log x)^4}\sum_{d_1,d_2\leq x}\frac{1}{d_1 d_2}\sum_{\substack{N\leq x\\ mcm(d_1,d_2)|N}}1\\
&\leq \frac{x^2}{(\log x)^4}\sum_{d_1,d_2\leq x}\frac{1}{d_1 d_2}\frac{x}{mcm(d_1,d_2)}\\
&\leq \frac{x^3}{(\log x)^4}\sum_{d_1,d_2\leq x}\frac{1}{(d_1 d_2)^{3/2}}\\
&\leq \frac{x^3}{(\log x)^4}\left(\sum_{d\leq x}\frac{1}{d^{3/2}}\right)^2\\
&\ll \frac{x^3}{(\log x)^4},
\end{aligned}$$

dove si è usata la maggiorazione $mcm(d_1,d_2)=\frac{d_1 d_2}{(d_1,d_2)}\geq (d_1 d_2)^{1/2}$, e la convergenza della serie $\sum_{d=1}^{\infty}\frac{1}{d^{3/2}}$. ■

Teorema 10.2.5 *L'insieme $A=\{0,1\}\cup\{p+q|p,q\in\mathbb{P}\}$ ha densità di Schnirel'man positiva.*

Dimostrazione. Sia $N\in\mathbb{N}$. Applicando la disuguaglianza di Cauchy-Schwarz otteniamo

$$\left(\sum_{N\leq x}r(N)\right)^2\leq\left(\sum_{\substack{N\leq x\\ r(N)\geq 1}}1\right)\left(\sum_{N\leq x}(r(N))^2\right)\leq A(x)\sum_{N\leq x}(r(N))^2.$$

Quindi, per i Lemmi 10.1.3 e 10.1.4,

$$\frac{A(x)}{x}\geq\frac{1}{x}\frac{\left(\sum_{N\leq x}r(N)\right)^2}{\sum_{N\leq x}(r(N))^2}\gg\frac{1}{x}\frac{x^4/(\log x)^4}{x^3/(\log x)^4}\gg 1.$$

Ovvero $d_L^S(A)>0$. Poiché A contiene 1, per la Proposizione 10.1.1, abbiamo che $d^S(A)>0$. ■

Dimostrazione del Teorema 10.2.1. Prendiamo

$$A := \{0, 1\} \cup \{p + q | p, q \in \mathbb{P}\}.$$

Per il Teorema precedente A ha densità di Schnirel'man positiva e pertanto è una base d'ordine finito per $\mathbb{N}$. Sia $h > 0$ tale che $\mathbb{N} = hA$, cioè ogni numero intero n è somma di esattamente h elementi di A. Ora se $n \geq 2$, esistono $k, l \in \mathbb{N}$ tali che $k + l \leq h$ e

$$n - 2 = \underbrace{1 + \ldots 1}_{k} + (p_1 + q_1) + (p_2 + q_2) + \ldots + (p_l + q_l).$$

Se k è pari allora

$$n = \underbrace{2 + \ldots 2}_{m+1} + (p_1 + q_1) + (p_2 + q_2) + \ldots + (p_l + q_l),$$

mentre se k è dispari

$$n = \underbrace{2 + \ldots 2}_{m} + 3 + (p_1 + q_1) + (p_2 + q_2) + \ldots + (p_l + q_l).$$

In entrambi i casi n si scrive some somma di al più $3h$ primi. ∎

La costante C del Teorema di 10.2.1 viene chiamata *costante di Schnirel'man*. Utilizzando un risultato di V. Brun, Schnirel'man stesso nel 1830 provò che $C \leq 800.000$. Nel 1995 O. Ramaré ([53]) ha mostrato che $C \leq 7$. È utile ricordare a tale proposito la famosa

Congettura di Goldbach *Ogni intero pari > 2 è somma di due numeri primi.*

È ben noto che tale congettura è ancora aperta. Se fosse vera, avremmo che $C = 3$.
Recentemente (2014, [28]) H. A. Helfgott ha ultimato la prova di questo sorprendente risultato

Ternary Goldbach Conjecture *Ogni intero dispari > 5 è somma di tre numeri primi.*

Ovviamente questo risultato implica quella che è la stima attuale migliore possibile per C, ovvero $C \leq 4$.

IL TEOREMA DI WARING PER I POLINOMI

Come già accennato, in questa sezione presenteremo, modulo un profondo risultato di Yu. Linnik (Teorema 10.3.6), una dimostrazione elementare del famoso Problema di Waring

Teorema 10.3.1 (Waring-Hilbert) *Assegnato un intero $k \geq 2$, esiste un intero $s = s(k)$ tale che ogni numero naturale si può scrivere come somma di al più s potenze k-esime.*

In realtà proveremo molto di più. Il Teorema 10.3.1 sarà infatti una immediata conseguenza di un risultato più generale che riguarda "quasi tutti" i polinomi e non solo quelli del tipo x^k. Il risultato che proveremo prende il nome di *Problema di Waring per i polinomi*.

Per chiarire bene ciò di cui stiamo parlando, conviene introdurre subito alcuni concetti fondamentali.

Un polinomio $f(x)$ a coefficienti reali (o complessi) si dice *integer-valued* se $f(\mathbb{Z}) \subseteq \mathbb{Z}$, ovvero se $f(z)$ è un intero per ogni intero z. È ovvio che se f ha coefficienti interi, allora f è integer-valued. Un esempio meno banale è il polinomio binomiale di grado $k \geq 0$

$$b_k(x) = \binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

Gli esercizi 10.1-10.4 provano la cossiddetta rappresentazione standard di un polinomio integer-valued, ovvero

Proposizione 10.3.2 *Se $f(x)$ è un polinomio a coefficienti complessi di grado k che sia integer-valued, allora esistono, e sono unici: $u_0, u_1, \dots, u_k$ numeri* interi, *con $u_k \neq 0$, tali che*

$$f(x) = \sum_{i=0}^{k} u_i b_i(x) = \sum_{i=0}^{k} u_i \binom{x}{i}.$$

Sia ora $f(x)$ un polinomio integer-valued di grado k con coefficiente direttivo positivo. Esiste allora un intero $n \geq 0$ per cui $f(n) \geq 0$ e $f(x)$ è strettamente crescente per $x \geq n$. Posto

$$f_n(x) := f(x+n)$$

si ha che f_n è ancora un polinomio integer-valued dello stesso grado di f e con lo stesso coefficiente direttivo. Inoltre, la successione di interi non negativi

$$A(f_n) := \{f_n(j)\}_{j \geq 0}$$

è strettamente crescente. Pertanto, a meno di rimpiazzare $f(x)$ con $f_n(x)$, possiamo assumere che $f(x)$ sia un polinomio integer-valued tale che

$$A(f) = \{f(j)\}_{j \geq 0}$$

sia una successione crescente di numeri non negativi.

Il *Problema di Waring per i polinomi* si enuncia allora in questo modo

Teorema 10.3.3 *Sia $f(x)$ un polinomio integer-valued e assumiamo che $A(f) = \{f(j)\}_{j \geq 0}$ sia una successione di numeri naturali strettamente crescente. Se $0, 1 \in A(f)$, allora esiste una costante $h > 0$ per cui ogni intero non negativo è somma di esattamente h elementi di $A(f)$.*

Appare ora ovvio che il Teorema 10.3.1 altro non è che il caso speciale in cui $f(x) = x^k$.
Accingiamoci a provare il Teorema 10.3.3.

D'ora in poi ,sia $f(x) = \sum_{i=0}^{k} a_i x^i$ un polinomio integer-valued che soddisfi alle ipotesi del Teorema. In particolare, f ha grado k e coefficiente direttivo $a_k > 0$.
Dati $n, s \in \mathbb{N}$, con $s \neq 0$, definiamo:

$$S_{f,s}(n) := \left\{ (x_1, x_2, \ldots, x_s) \in \mathbb{N}^s \,\middle|\, \sum_{i=1}^{s} f(x_i) = n \right\}$$

e

$$r_{f,s}(n) = \left| S_{f,s}(n) \right|.$$

Sia inoltre per ogni $N \in \mathbb{N}$

$$R_{f,s}(N) = \sum_{0 \leq n \leq N} r_{f,s}(n) = \left| \bigcup_{n=0}^{N} S_{f,s}(n) \right|.$$

Lemma 10.3.4 *Sia $f(x) = \sum_{i=0}^{k} a_i x^i$ come sopra e sia*

$$x^*(f) := \frac{2}{a_k}(|a_{k-1}| + \ldots + |a_0|).$$

Allora se x è un intero maggiore di $x^*(f)$, vale:

$$\frac{a_k}{2} x^k < f(x) < \frac{3a_k}{2} x^k.$$

Se inoltre N è un intero sufficientemente grande, si ha:

$$R_{f,s}(N) > \frac{1}{2} \left(\frac{2N}{3a_k s} \right)^{s/k}.$$

Dimostrazione. Abbiamo che

$$f(x) = a_k x^k \left(1 + \frac{a_{k-1}}{a_k x} + \ldots + \frac{a_0}{a_k x^k} \right),$$

quindi per $x > x^*(f)$ si ha:

$$\begin{aligned} \left| \frac{f(x)}{a_k x^k} - 1 \right| &= \left| \frac{a_{k-1}}{a_k x} + \ldots + \frac{a_0}{a_k x^k} \right| \\ &\leq \frac{|a_{k-1}|}{a_k x} + \ldots + \frac{|a_0|}{a_k x^k} \\ &\leq \frac{|a_{k-1}| + \ldots + |a_0|}{a_k x} \\ &= \frac{x^*(f)}{2x} < \frac{1}{2}, \end{aligned}$$

ovvero:

$$\frac{a_k}{2}x^k < f(x) < \frac{3a_k}{2}x^k.$$

Siano ora assegnati $x_1, \dots, x_s \in \mathbb{N}$ tali che

$$x^*(f) < x_j \leq \left(\frac{2N}{3a_k s}\right)^{1/k}, \text{ per ogni } j = 1, \dots, s.$$

Allora

$$0 < \frac{a_k x_j^k}{2} < f(x_j) < \frac{3a_k x_j^k}{2} \leq \frac{N}{s}$$

e quindi

$$0 < \sum_{j=1}^{s} f(x_j) < N$$

cioè $(x_1, \dots, x_s) \in \bigcup_{n=1}^{N} S_{f,s}(n)$.
Ora, il numero di interi nell'intervallo $\left(x^*(f), \left(\frac{2N}{3a_k s}\right)^{1/k}\right]$ è almeno

$$\left(\frac{2N}{3a_k s}\right)^{1/k} - x^*(f) - 1.$$

Ne segue che

$$R_{f,s}(N) > \left(\left(\frac{2N}{3a_k s}\right)^{1/k} - x^*(f) - 1\right)^s \geq \frac{1}{2}\left(\frac{2N}{3a_k s}\right)^{s/k}$$

per N sufficientemente grande. ■

Lemma 10.3.5 *Siano al solito $f(x) = \sum_{i=0}^{k} a_i x^i$ come sopra e $x^*(f)$ come nel Lemma 10.3.4. Sia inoltre*

$$N(f) := \frac{(x^*(f))^k}{2k!}.$$

Per $N > N(f)$, se $x_1, x_2, \dots x_s \in \mathbb{N}$ sono tali che $\sum_{i=1}^{s} f(x_i) \leq N$, allora

$$0 \leq x_j \leq (2k!N)^{1/k}, \quad \text{per ogni } j = 1, 2, \dots s.$$

Dimostrazione. Per l'Esercizio 10.5, $k!a_k \geq 1$. Pertanto se $N \geq N(f)$ e $x_j > (2k!N)^{1/k} \geq x^*(f)$. Per il Lemma precedente abbiamo che

$$f(x_j) > \frac{a_k x_j^k}{2} \geq k!a_k N \geq N$$

e quindi $\sum_{j=1}^{s} f(x_j) \geq f(x_j) > N$. ■

Teorema 10.3.6 (Yu. Linnik) *Siano c e P due interi positivi ed s la successione così definita:*

$$\begin{cases} s(1) = 1 \\ s(j) = 8j2^{\lfloor \log_2 s(j-1) \rfloor} & \text{se } j \geq 2. \end{cases}$$

Assumiamo che $f(x) = \sum_{i=0}^{k} a_i x^i$ sia un polinomio integer-valued di grado k tale che $|a_i| \leq cP^{k-i}$, $\forall i = 0, \dots, k$. Allora per ogni $n \in \mathbb{N}$

$$\left| \left\{ (x_1, \dots x_{s(k)}) \in \mathbb{Z}^{s(k)} \middle| \sum_{i=1}^{s(k)} f(x_i) = n, \, |x_j| \leq cP \, \forall j \right\} \right| \ll_{k,c} P^{s(k)-k},$$

dove la costante moltiplicativa (relativa a $\ll_{k,c}$) dipende solo da k e da c.

Dimostrazione. Si veda [46, Theorem 12.3]. ∎

L'idea geniale di Linnik consiste nell'aver determinato la successione $s(j)$ di sopra. Infatti, ora non è difficile provare il seguente risultato.

Teorema 10.3.7 *Definita la successione $s(j)$ come nel Teorema 10.3.6, si ha che*

$$d_L^S \Big(s(k) A(f) \Big) > 0.$$

Dimostrazione. Siano $N(f) := \frac{(x^*(f))^k}{2k!}$ e $s := s(k)$ e poniamo $W := sA(f)$, l'insieme i cui elementi sono somme di s elementi della forma $f(m)$ con $m \in \mathbb{N}$.
Siano inoltre $c \geq (2k!)^{1/k}$ e $N \geq N(f)$ sufficientemente grande affinché detto $P = N^{1/k}$ si abbia $|a_i| \leq cP^{k-i}$, per ogni $i = 0, \dots, k$. Allora $0 < a_k \leq c$ e per il Lemma 10.3.5 se $x_1, \dots, x_s$ ono interi non negativi tali che $\sum_{j=1}^{s} f(x_j) \leq N$, si ha $0 \leq x_j \leq (2k!N)^{1/k} \leq cP$, per ogni $j = 1, \dots, s$.
Preso ora $0 \leq n \leq N$ si ha

$$\begin{aligned} r_{f,s}(n) &= \left| \left\{ (x_1, \dots, x_s) \in \mathbb{N}^s \middle| \sum f(x_j) = n \right\} \right| \\ &\leq \left| \left\{ (x_1, \dots, x_s) \in \mathbb{Z}^s \middle| \sum f(x_j) = n, \, |x_j| \leq cP \, \forall j \right\} \right| \\ &\ll_{k,c} P^{s-k} \end{aligned}$$

per il Teorema 10.3.6.
Ne segue che

$$\begin{aligned} R_{f,s}(N) &= \sum_{0 \leq n \leq N} r_{f,s}(n) \\ &= \sum_{\substack{0 \leq n \leq N \\ r_{f,s}(n) \geq 1}} r_{f,s}(n) \\ &\ll W(N) P^{s-k} \\ &\ll \left(\frac{W(N)}{N} \right) P^s. \end{aligned}$$

Inoltre per il Lemma 10.3.4, per $N \gg 0$,

$$R_{f,s}(N) > \frac{1}{2}\left(\frac{2N}{3a_k s}\right)^{s/k} \geq \frac{1}{2}\left(\frac{2N}{3cs}\right)^{s/k} \gg P^s.$$

Pertanto abbiamo provato che

$$P^s \ll R_{f,s}(N) \ll \left(\frac{W(N)}{N}\right) P^s$$

(dove le costanti dipendono solo da k e da c), ovvero

$$\frac{W(N)}{N} \gg 1.$$

Ma ciò significa proprio che esiste una costante positiva $h > 0$ tale che $\frac{W(N)}{N} \geq h$ per N sufficientemente grande, ovvero che:

$$d_L^S(sA(f)) = d_L^S(W) = \liminf_n \frac{W(n)}{n} > 0,$$

che è quello che si voleva provare. ■

Dimostrazione del Teorema 10.3.3.
Assumiamo che $0, 1 \in A(f)$ e proviamo che questa è una base additiva d'ordine finito per $\mathbb{N}$. Per il Teorema 10.3.7, esiste un intero positivo s per cui $d_L^S(sA(f)) > 0$. Poiché $0, 1 \in A(f)$ si ha che $1 \in sA(f)$, quindi per il Corollario 10.1.7, $d^S(sA(f)) > 0$. Per il Teorema 10.1.2, $sA(f)$ è una base additiva d'ordine finito, diciamo $h > 0$. Pertanto

$$\mathbb{N} = h(sA(f)) = hs(A(f))$$

ovvero $A(f)$ è base additiva d'ordine finito hs. ■

APPENDICE

La congettura abc

Ottenuta la dimostrazione del Teorema di Fermat, la cosiddetta *congettura abc* è da molti ritenuta uno dei problemi più importanti della teoria dei numeri. Si tratta di una congettura molto potente, che collega la struttura additiva dei numeri interi con quella moltiplicativa; se dimostrata, da essa seguirebbe la correttezza di diverse singole congetture ancora aperte.

Sia z un intero non nullo. Il *radicale* di z è il massimo divisore positivo di z privo di quadrati; ovvero il prodotto dei primi positivi distinti che dividono z:

$$\mathrm{rad}(z) = \prod_{p|z} p.$$

Si noti che $\mathrm{rad}(1) = \mathrm{rad}(-1) = 1$.

Congettura abc *Per ogni numero reale $\epsilon > 0$, esiste un numero $K(\epsilon) > 0$ tale che, se a, b e c sono interi non nulli e $a + b + c = 0$, allora*

$$\max\{|a|, |b|, |c|\} \leq K(\epsilon)\,\mathrm{rad}(abc)^{1+\epsilon}.$$

Illustriamo con qualche esempio la forza di questa congettura, cominciando con il Teorema di Fermat.

Per $n \geq 2$, chiamiamo n-esima equazione di Fermat, l'equazione:

$$x^n + y^n = z^n.$$

Il Teorema di Fermat afferma che per $n \geq 3$ l'n-esima equazione di Fermat non ammette soluzioni intere (positive) con $xyz \neq 0$.

Proposizione 10.4.1 *La congettura abc implica che esiste un intero $N \geq 3$ tale che per ogni $n \geq N$, l'equazione n-esima di Fermat non ha soluzioni intere non banali.*

Dimostrazione. Osserviamo, innanzi tutto, che se una equazione di Fermat ha una soluzione $x^k + y^k = z^k$, e p è un divisore primo comune di x, y e z, allora anche la terna $(x/p, y/p, z/p)$ è una soluzione della stessa equazione. Possiamo quindi limitarci a provare, assumendo la congettura abc, che esiste N tale che per $n \geq N$ l'equazione n-esima di Fermat non ha soluzioni con interi positivi tra loro coprimi.

Supponiamo che, per un qualche $m \geq 3$, esistano interi coprimi x, y e z tali che

$$x^m + y^m = z^m.$$

Osserviamo che

$$\mathrm{rad}(x^m y^m z^m) = \mathrm{rad}(xyz) \leq xyz \leq z^3.$$

Ora, poiché $m \geq 3$, deve essere $z \geq 3$. Applichiamo la congettura abc, con $\epsilon = 1$. Esiste una costante $C := \max\{1, K(1)\}$ tale che

$$z^m = \max\{x^m, y^m, z^m\} \leq C\,\mathrm{rad}(x^m y^m z^m)^2 < Cz^6.$$

Da ciò segue

$$m < 6 + \log_z C \leq 6 + \log_3 C.$$

Dunque, per $n \geq 6 + \log_3 C$ l'equazione n-esima di Fermat non ammette soluzioni. ∎

Il nostro secondo esempio riguarda la congettura di Catalan (di cui abbiamo parlato alla fine del Capitolo 1).

Proposizione 10.4.2 *La congettura abc implica che la congettura di Catalan ha un numero finito di soluzioni.*

DIMOSTRAZIONE. L'equazione di Catalan è

$$y^m - x^n = 1$$

dove si cercano soluzioni non banali (cioè con $n, m \geq 2$, e $xy \neq 0$) in x, y, n, m.

È noto che non esistono soluzioni con $n = 2$, e che la sola soluzione con $m = 2$ è $n = 3$, $x = 2$, $y = 3$.

Supponiamo dunque che (x, y, m, n) sia una soluzione dell'equazione di Catalan, con $\min\{m, n\} \geq 3$. Chiaramente, x e y sono coprimi.

Applichiamo la congettura abc con $\epsilon = \frac{1}{4}$. Esiste un numero $K = K(1/4)$ tale che

$$x^n < y^m \leq K \operatorname{rad}(y^m x^n)^{\frac{5}{4}} = K \operatorname{rad}(yx)^{\frac{5}{4}} \leq K(yx)^{\frac{5}{4}}.$$

Da ciò seguono le diseguaglianze

$$n \log x < \log K + \frac{5}{4} \log y + \frac{5}{4} \log x$$

$$m \log y \leq \log K + \frac{5}{4} \log y + \frac{5}{4} \log x.$$

E da queste,

$$n \log x + m \log y < 2 \log K + \frac{5}{2}(\log x + \log y),$$

e di conseguenza,

$$(n - 5/2) \log x + (m - 5/2) \log y < 2 \log K.$$

Poiché $x, y \geq 2$, si ricava

$$(n + m - 5) \log 2 < 2 \log K$$

e quindi

$$m + n < \frac{2 \log K}{\log 2} + 5.$$

Dunque l'equazione di Catalan ha un numero finito di soluzioni, dato che per fissati $m \geq 3$ e $n \geq 3$, l'equazione $y^m - x^n = 1$ ha un numero finito di soluzioni intere. ■

Definire i primi di Wieferich e aggiungere dimostrazione abc implica primi di Wieferich

ESERCIZI

Esercizio 10.1 *Provare che per ogni $k \leq 0$ il polinomio binomiale*

$$b_k(x) = \binom{x}{k} = \frac{x(x-1)\dots(x-k+1)}{k!}$$

è integer-valued. (Suggerimento: $b_k(-n) = (-1)^k b_k(n + k - 1)$).

Esercizio 10.2 *Sia* $f(x) = \sum_{i=0}^{k} a_k x^k \in \mathbb{C}[x]$ *un polinomio a coefficienti complessi. Mostrare che esistono unici* $u_0, u_1, \dots u_k \in \mathbb{C}$ *(con* $u_k \neq 0$*) tali che* $f(x) = \sum_{i=0}^{k} u_i b_i(x)$.

Esercizio 10.3 *Per ogni* $f(x) \in \mathbb{C}[x]$ *sia* $\Delta g(x) = g(x+1) - g(x)$. *Provare che* $\Delta b_0(x) = 0$ *e* $\Delta b_i(x) = b_{i-1}(x)$ *per ogni* $i \geq 1$. *Provare inoltre che se* $f(x) = \sum_{i=0}^{k} u_i b_i(x)$, *allora* $\Delta f(x) = \sum_{i=0}^{k-1} u_{i+1} b_i(x)$.

Esercizio 10.4 *Sia* $f(x) \in \mathbb{C}[x]$ *tale che* $f(z) \in \mathbb{Z}$ *per ogni* z *sufficientemente grande. Provare che esistono unici* $u_0, u_1, \dots u_k \in \mathbb{Z}$ *(con* $u_k \neq 0$*) tali che* $f(x) = \sum_{i=0}^{k} u_i b_i(x)$. *Quindi, in particolare* $f(x)$ *è integer-valued.*

Esercizio 10.5 *Sia* $f(x) = \sum_{i=0}^{k} a_k x^k \in \mathbb{C}[x]$ *un polinomio integer-valued di grado* k. *Provare che* $|a_k| \geq \frac{1}{k!}$.

Si presentava-no alle lezioni in uniforme, accompa-gnati da un sottuffi-ciale. Un gior-no per ottene-re un po' di silenzio, chie-si a costui di far-li mettere sull'atten-ti. Uno di lo-ro, una volta, mi domandò: «Non capisco cosa sia questa x». La do- manda era più profonda di quan- to lui stesso po-tesse immaginare, ma non tentai nemmeno di spiegar- gli il per-ché. ([62])

11 PARTIZIONI

In questo Capitolo ci occuperemo di partizioni. Se n è un arbitrario numero naturale indicheremo con $p(n)$ il numero di rappresentazioni di n come somma (non ordinata) di interi positivi.

Dopo una prima sezione dedicata alle partizioni con parti limitate, studieremo il comportamento asintotico della funzione $p(n)$, proponendo completamente la dimostrazione di P. Erdös del fatto che

$$\log p(n) \sim \pi \sqrt{\frac{2n}{3}}.$$

Nelle ultime due sezioni, fissato un sottoinsieme (infinito) A di numeri naturali, studieremo la funzione $p_A(n)$, definita come il numero di partizioni di n aventi ogni parte in A. Mostreremo come il comportamento asintotico di questa funzione e la densità del sottoinsieme A siano due concetti matematicamente equivalenti.

PARTIZIONI CON PARTI LIMITATE

Dato un sottoinsieme non vuoto A di numeri naturali positivi, indicheremo con $p_A(n)$ il numero di partizioni di $n \in \mathbb{N}^*$ con parti appartenenti ad A (più semplicemente indicheremo con $p(n)$ il numero $p_{\mathbb{N}^*}(n)$). Riserveremo la notazione $\mathsf{P}_A(n)$ per indicare l'insieme di tutte queste partizioni, cosicché $|\mathsf{P})A(n)| = p_A(n)$. Spesso scriveremo una partizione π nella forma

$$\pi : n = a_1 + a_2 + \ldots a_k,$$

dove ogni parte $a_i \in A$ e penseremo

$$a_1 \geq a_2 \geq \ldots \geq a_k.$$

Ad esempio se $n = 5$ abbiamo che $p(5) = 7$ e $p_A(5) = 5$, se $A = \{1, 2, 3\}$. Infatti abbiamo:

$$\begin{aligned} 5 &= 5 \\ &= 4 + 1 \\ &= 3 + 2 \\ &= 3 + 1 + 1 \\ &= 2 + 2 + 1 \\ &= 2 + 1 + 1 + 1 \\ &= 1 + 1 + 1 + 1 + 1 \end{aligned} \qquad \begin{aligned} 5 &= 3 + 2 \\ &= 3 + 1 + 1 \\ &= 2 + 2 + 1 \\ &= 2 + 1 + 1 + 1 \\ &= 1 + 1 + 1 + 1 + 1 \end{aligned}$$

Poniamo inoltre $p_A(0) = 1$, per ogni $A \subseteq \mathbb{N}^*$. La funzione p_A viene chiamata *funzione di partizione su* A, mentre la funzione p, *funzione di partizione non ristretta*.

Esempio 11.1.1 *In quanti modi è possibile cambiare una banconota da* n *euro utilizzando solamente monete da* $1, 2$ *e* 3 *euro? (Si assume l'esistenza di monete da* 3 *euro)*

Svolgimento. Ogni partizione di n tramite elementi di $A = \{1, 2, 3\}$ compare nello sviluppo del seguente prodotto

$$(1 + z + z^2 + \ldots)(1 + z^2 + z^{2\cdot 2} + \ldots)(1 + z^3 + z^{2\cdot 3} + \ldots),$$

ovvero di

$$\frac{1}{1-z} \cdot \frac{1}{1-z^2} \cdot \frac{1}{1-z^3}.$$

Dal punto di vista delle funzioni generatrici possiamo pertanto scrivere

$$\sum_{n\geq 0} p_A(n) z^n = \frac{1}{(1-z)(1-z^2)(1-z^3)}.$$

Scrivendo l'espressione di destra tramite frazioni parziali e risolvendo il sistema, si trova che

$$\sum_{n\geq 0} p_A(n) z^n = \frac{1}{6(1-z)^3} + \frac{1}{4(1-z)^2} + \frac{1}{4(1-z^2)} + \frac{1}{3(1-z^3)} \quad (55)$$

Questa si risolve andando a derivare successivamente la serie geometrica. Infatti

$$\frac{1}{(1-z)^2} = \frac{d}{dz}\left(\frac{1}{1-z}\right) = \frac{d}{dz}\left(\sum_{n\geq 0} z^n\right) = \sum_{n\geq 0}(n+1)z^n$$

e

$$\frac{1}{(1-z)^3} = \frac{d}{dz}\left(\frac{1}{2(1-z)^2}\right) = \sum_{n\geq 0} \frac{(n+2)(n+1)}{2} z^n.$$

Tenendo conto che $\frac{1}{1-z^2} = \sum_{j\geq 0} z^{2j}$ e $\frac{1}{1-z^3} = \sum_{j\geq 0} z^{3j}$, da (55) si ottiene

$$\begin{aligned} p_A(n) &= \frac{(n+2)(n+1)}{12} + \frac{n+1}{4} + \frac{1}{4}u_1(n) + \frac{1}{3}u_2(n) \\ &= \frac{n^2}{12} + \frac{n}{2} + \frac{5}{12} + \frac{1}{4}u_1(n) + \frac{1}{2}u_2(n). \end{aligned}$$

dove $u_1(n) = 1$ se $2|n$, altrimenti $u_1(n) = 0$ e $u_2(n) = 1$ se $3|n$, altrimenti $u_2(n) = 0$.
Si ossservi che $p_a(n) \sim \frac{n^2}{12}$. ■

Prima di affrontare il caso generale, notiamo che se $MCD(A) = d > 1$ allora è ovvio che solo gli interi multipli di d possono ammettere partizioni con parti tutte in A. Si vede inoltre facilmente che, detto $A' = \{a/d | a \in A\}$, allora $MCD(A') = 1$ e per ogni $n \in \mathbb{N}$

$$p_A(n) = \begin{cases} 0 & \text{se } n \not\equiv 0 (\text{mod } d) \\ p_{A'}(n/d) & \text{se } n \equiv 0 (\text{mod } d) \end{cases}$$

Possiamo ora enunciare e provare il primo Teorema di questo Capitolo, che è una formula asintotica per le funzioni di partizione su insiemi finiti.

Teorema 11.1.1 *Sia A un sottoinsieme non vuoto di $\mathbb{N}^*$ di cardinalità finita k, con $MCD(A) = 1$. Allora per ogni $n \in N^*$ vale:*

$$p_A(n) = \frac{n^{k-1}}{\left(\prod_{a\in A} a\right)\cdot(k-1)!} + O(n^{k-2}).$$

Dimostrazione. Facciamo induzione su k.
Per $k = 1$, poiché $MCD(A) = 1$, $A = \{1\}$ e il risultato è banale.
Sia $k \geq 2$ e sia $A = \{a_1, \ldots, a_k\}$. Detto $d = MCD(a_1, \ldots, a_{k-1})$, si ha $MCD(d, a_k) = 1$; inoltre posti $a'_i = \frac{a_i}{d}$, per $i = 1, \ldots, k-1$, il sottoinsieme $A' = \{a'_i | i = 1, \ldots, k-1\}$ soddisfa le ipotesi del Teorema e ha cardinalità $k-1$. Pertanto per l'ipotesi induttiva, per ogni $n \in \mathbb{N}^*$ vale:

$$p'_A(n) = \frac{n^{k-2}}{\left(\prod_{i=1}^{k-1} a'_i\right)\cdot(k-2)!} + O(n^{k-3}). \tag{56}$$

Sia ora $n \geq (d-1)a_k$. Essendo $MCD(d, a_k) = 1$, esiste un unico $u \in \mathbb{Z}$ tale che $0 \leq u \leq d-1$ e $n \equiv ua_k \pmod d$. Allora

$$m = \frac{n - ua_k}{d} \in \mathbb{N}$$

e $0 \leq m \leq n$. Ora, se $v \in \mathbb{N}^*$ è tale che $n \equiv va_k \pmod d$, allora $v \equiv u \pmod d$, cioè

$$v = u + ld \quad \text{per qualche } l \in \mathbb{N}.$$

Se inoltre $n - va_k = n - (u + ld)a_k > 0$ allora

$$0 \leq l \leq \left\lfloor \frac{n}{da_k} - \frac{u}{d} \right\rfloor = \left\lfloor \frac{m}{a_k} \right\rfloor =: r \leq m.$$

Prendiamo ora una partizione $\pi \in \mathsf{P}_A(n)$. Se π contiene esattamente v parti uguali ad a_k, allora $n - va_k \geq 0$ e $n - va_k \equiv 0 \pmod d$, essendo $n - va_k$ somma di elementi di A'. Da quanto detto sopra, segue che $v = u + ld$ con $0 \leq l \leq r$. Abbiamo così dimostrato che le partizioni di n con parti in A si suddividono in $r+1$ classi, dove per ogni $l = 0, 1, \ldots, r$ una partizione π appartiene alla classe l se contiene esattamente $u + ld$ parti uguali ad a_k. Il numero di partizioni di n con esattamente $u + ld$ parti uguali ad a_k coincide con il numero di partizioni di $n - (u + ld)a_k$ le cui parti appartengono ad $A \setminus \{a_k\}$, cioè coincide con il numero di partizioni di

$$\frac{n - (u + ld)a_k}{d} = m - la_k$$

aventi parti in A', ovvero con $p_{A'}(m - la_k)$.
Possiamo pertanto scrivere

$$p_A(n) = \sum_{l=0}^{r} p_{A'}(m - la_k)$$

e, sfruttando la (56), otteniamo

$$p_A(n) = \left(\frac{d^{k-1}}{\prod_{i=1}^{k-1} a_i}\right) \sum_{l=0}^{r} \frac{(m - la_k)^{k-2}}{(k-2)!} + O(n^{k-2}). \tag{57}$$

Ora studiamo in dettaglio $\sum_{l=0}^{r} \frac{(m-la_k)^{k-2}}{(k-2)!}$.
Applicando lo sviluppo di Newton e gli esercizi 11.1, 11.2, si ha:

$$\begin{aligned}
\sum_{l=0}^{r} \frac{(m - la_k)^{k-2}}{(k-2)!} &= \\
&= \frac{1}{(k-2)!} \sum_{l=0}^{r} \sum_{j=0}^{k-2} \binom{k-2}{j} m^{k-2-j} (-la_k)^j \\
&= \frac{1}{(k-2)!} \sum_{j=0}^{k-2} \binom{k-2}{j} m^{k-2-j} (-a_k)^j \sum_{l=0}^{r} l^j \\
&= \frac{1}{(k-2)!} \sum_{j=0}^{k-2} \binom{k-2}{j} m^{k-2-j} (-a_k)^j \left(\frac{r^{j+1}}{j+1} + O(r^j)\right) \\
&= \frac{1}{(k-2)!} \sum_{j=0}^{k-2} \binom{k-2}{j} m^{k-2-j} (-a_k)^j \left(\frac{m^{j+1}}{a_k^{j+1}(j+1)} + O(m^j)\right) \\
&= \frac{m^{k-1}}{a_k} \sum_{j=0}^{k-2} \binom{k-2}{j} \frac{(-1)^j}{(k-2)!(j+1)} + O(m^{k-2}) \\
&= \frac{m^{k-1}}{a_k} \sum_{j=0}^{k-2} \frac{(-1)^j}{(k-1-(j+1))!(j+1)!} + O(m^{k-2}) \\
&= \frac{m^{k-1}}{a_k(k-1)!} \sum_{j=0}^{k-2} \binom{k-1}{j+1} (-1)^j + O(m^{k-2}) \\
&= \frac{m^{k-1}}{a_k(k-1)!} + O(m^{k-2}).
\end{aligned}$$

Quindi

$$\begin{aligned}
p_A(n) &= \frac{d^{k-1}}{\prod_{i=1}^{k-1} a_i} \left(\frac{m^{k-1}}{a_k(k-1)!} + O(m^{k-2})\right) + O(n^{k-2}) \\
&= \left(\frac{1}{\prod_{i=1}^{k} a_i}\right) \frac{(n - ua_k)^{k-1}}{(k-1)!} + O(n^{k-2}) \\
&= \frac{n^{k-1}}{\left(\prod_{i=1}^{k} a_i\right)(k-1)!} + O(n^{k-2}),
\end{aligned}$$

e la dimostrazione è completata. ■

Sia π una arbitraria partizione del numero n

$$\pi : \quad n = a_1 + a_2 + \dots a_k$$

scritta secondo la convenzione $a_1 \geq a_2 \geq \dots \geq a_k$. È possibile rappresentare π geometricamente (mediante il cosiddetto diagramma di Ferrers)

$$\pi = \begin{array}{cccccc} * & * & * & * & * & * \\ * & * & * & * & * & \\ * & * & * & & & \\ * & * & & & & \\ * & & & & & \\ * & & & & & \\ * & & & & & \end{array}$$

dove sulla prima riga ci sono esattamente a_1 asterischi, sulla seconda a_2, e così via. Leggendo la tabella anziché per righe per colonne, troviamo un'altra partizione del numero n, che chiamiamo *coniugata di* π e che indichiamo con $\overline{\pi}$. Rispetto all'esempio di sopra, abbiamo

$$\overline{\pi} = \begin{array}{ccccccc} * & * & * & * & * & * & * \\ * & * & * & * & & & \\ * & * & * & & & & \\ * & * & & & & & \\ * & * & & & & & \\ * & & & & & & \end{array}$$

È ovvio che $\overline{\overline{\pi}} = \pi$, per ogni partizione π di n.

Corollario 11.1.2 *Sia $p_k(n)$ il numero di partizioni di n in al più k parti. Allora*

$$p_k(n) = \frac{n^{k-1}}{k!(k-1)!} + O(n^{k-2}).$$

DIMOSTRAZIONE. Basta osservare che l'applicazione che manda una partizione nella sua coniugata induce una biezione, tra l'insieme delle partizioni di n in al più k parti e quello delle partizioni di n con parti in $A = \{1, 2, \dots, k\}$. Ne segue che $p_k(n) = p_A(n)$; la tesi segue ora dal Teorema precedente. ∎

COMPORTAMENTO ASINTOTICO DI $p(n)$

In maniera indipendente, G. H. Hardy e S. Ramanujan nel 1918 ([25]) e Ya. V. Uspensky nel 1920 ([60]), provarono che

$$p(n) \sim \frac{e^{c_0\sqrt{n}}}{(4\sqrt{3})n}, \tag{58}$$

dove $c_0 = \pi\sqrt{\frac{2}{3}} \simeq 2,565$.

Entrambe le dimostrazioni fanno uso di variabili complesse e funzioni modulari. Nel 1942 ([19]), P. Erdös fornì una prova dell'equazione asintotica (58) che è un vero "tour de force" di metodi elementari. La dimostrazione di Erdös, davvero impressionante per quanto riguarda la difficoltà tecnica, mostra che il comportamento asintotico di $p(n)$ è semplicemente una conseguenza di una elementare formula ricorsiva (Teorema 11.2.1) e non dipende da profonde proprietà analitiche delle funzioni modulari.

In questa sezione, seguiremo il metodo di Erdös per provare qualcosa di leggemente più debole di (58); ovvero proveremo che

$$\log p(n) \sim c_0\sqrt{n}. \tag{59}$$

Come si diceva, il punto di partenza è la seguente formula ricorsiva

Teorema 11.2.1 *Posto $p(0) = 1$ e $p(n) = 0$ per ogni $n < 0$, se $n \in \mathbb{N}^*$ vale che:*

$$np(n) = \sum_{\substack{k,v\geq 1\\ kv\leq n}} vp(n - kv). \tag{60}$$

Dimostrazione. Sia v un intero positivo. Il numero di partizioni di n con *almeno* una parte uguale a v coincide con il numero di partizioni di $n - v$, cioè con $p(n - v)$. Similmente, se $k > 0$ Il numero di partizioni di n con *almeno* k parti uguali a v coincide con $p(n - kv)$. Ne segue che il numero di partizioni di n con *esattamente* k parti uguali a v è

$$p(n - kv) - p(n - (k + 1)v).$$

Inoltre possiamo aggiungere che il numero di parti uguali a v che compaiono in tutte le partizioni di n è dato dalla sommatoria

$$\sum_{k\geq 1} k\big(p(n - kv) - p(n - (k + 1)v)\big) = \sum_{k\geq 1} p(n - kv). \tag{61}$$

Scriviamo ora la lista di tutte le $p(n)$ partizioni di n, siano queste

$$\begin{aligned}
n &= a_{1,1} + a_{1,2} + \ldots + a_{1,k_1}\\
n &= a_{2,1} + a_{2,2} + \ldots + a_{2,k_2}\\
&\vdots \qquad\qquad \vdots\\
n &= a_{p(n),1} + a_{p(n),2} + \ldots + a_{p(n),k_{p(n)}}
\end{aligned}$$

Sommando memro a membro si ottiene

$$\begin{aligned} n\,p(n) &= \sum_{i=1}^{p(n)} \sum_{j=1}^{k_i} a_{i,j} \\ &= \sum_{v=1}^{n} v \sum_{a_{i,j}=v} 1 \\ &= \sum_{v=1}^{n} v \sum_{k\geq 1} p(n-kv) \\ &= \sum_{\substack{k,v\geq 1 \\ kv\leq n}} v\,p(n-kv) \end{aligned}$$

che completa la dimostrazione. ■

Lemma 11.2.2 *Sia $0 < l \leq n$, allora*

$$\sqrt{n} - \frac{l}{2\sqrt{n}} - \frac{l^2}{2\sqrt{n^3}} \leq \sqrt{n-l} < \sqrt{n} - \frac{l}{2\sqrt{n}}.$$

DIMOSTRAZIONE. Dallo sviluppo di $(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^\alpha$ per $|x| < 1$, si ha

$$(1-x)^{1/2} = 1 - \frac{x}{2} - \frac{x^2}{8} + o(x^2),$$

ed in particolare per $0 < x \leq 1$ si ha

$$1 - \frac{x}{2} - \frac{x^2}{2} \leq (1-x)^{1/2} < 1 - \frac{x}{2}.$$

Per $x = l/n$ si ottiene la tesi. ■

Lemma 11.2.3 *Sia x un numero reale positivo, allora*

$$\frac{e^{-x}}{(1-e^{-x})^2} < \frac{1}{x^2}.$$

Se inoltre $0 < x \leq 1$, allora

$$\frac{1}{x^2} - 2 < \frac{e^{-x}}{(1-e^{-x})^2}.$$

DIMOSTRAZIONE. Dallo sviluppo di $e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$ per ogni $x \in \mathbb{R}$, si ottiene

$$e^{\frac{x}{2}} - e^{-\frac{x}{2}} = 2\sum_{k=0}^{\infty} \frac{1}{(2k+1)!} \left(\frac{x}{2}\right)^{2k+1} = x + x^3 \sum_{k=1}^{\infty} \frac{x^{2k-2}}{(2k+1)!\,2^{2k}}.$$

Ora, se $x > 0$, $e^{x/2} - e^{-x/2} > x$ e quindi

$$\frac{e^{-x}}{(1-e^{-x})^2} = \frac{1}{(e^{\frac{x}{2}} - e^{-\frac{x}{2}})^2} < \frac{1}{x^2}.$$

Se inoltre $0 < x \leq 1$, allora

$$e^{x/2} - e^{-x/2} < x + x^3 \sum_{k=1}^{\infty} \frac{1}{2^{2k}} < x + x^3 < \frac{x}{1-x^2},$$

e quindi

$$\frac{1}{(e^{\frac{x}{2}} - e^{-\frac{x}{2}})^2} > \left(\frac{1}{x} - x\right)^2 > \frac{1}{x^2} - 2.$$

■

Lemma 11.2.4 *Siano $c \in \mathbb{R}_{>0}$ ed $n \in \mathbb{N}^*$. Per ogni intero $k \geq 1$ sia*

$$a_k = \frac{e^{-\frac{ck}{2\sqrt{n}}}}{\left(1 - e^{-\frac{ck}{2\sqrt{n}}}\right)^2}.$$

Allora

$$\sum_{k=1}^{\infty} a_k < \frac{2\pi^2 n}{3c^2}.$$

Se inoltre $n \geq \frac{c^2}{4}$, allora

$$\sum_{k=1}^{\infty} a_k > \frac{2\pi^2 n}{3c^2} - \frac{8\sqrt{n}}{c}.$$

Dimostrazione. Assegnato $k \in \mathbb{N}^*$, poniamo $x = \frac{ck}{2\sqrt{n}}$. Per il Lemma 11.2.3, abbiamo che

$$a_k < \frac{1}{x^2} = \frac{4n}{c^2k^2}.$$

Pertanto, utilizzando $\zeta(2) = \frac{\pi^2}{6}$ (Teorema 4.5.2), otteniamo

$$\sum_{k=1}^{\infty} a_k < \frac{4n}{c^2} \sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{4n}{c^2}\zeta(2) = \frac{2\pi^2 n}{3c^2}.$$

Sia adesso $\sqrt{n} \geq \frac{c}{2}$. Se $1 \leq k \leq \frac{2\sqrt{n}}{c}$, allora $0 < x \leq 1$ e per il Lemma 11.2.3 ancora,

$$a_k > \frac{1}{x^2} - 2 = \frac{4n}{c^2k^2} - 2.$$

Quindi,

$$\begin{aligned}
\sum_{k=1}^{\infty} a_k &> \sum_{k \leq \frac{2\sqrt{n}}{c}} a_k \\
&> \sum_{k \leq \frac{2\sqrt{n}}{c}} \left(\frac{4n}{c^2k^2} - 2\right) \\
&= \frac{4n}{c^2}\left(\sum_{k=1}^{\infty} \frac{1}{k^2} - \sum_{k > \frac{2\sqrt{n}}{c}} \frac{1}{k^2}\right) - \frac{4\sqrt{n}}{c} \\
&= \frac{2\pi^2 n}{3c^2} - \frac{4n}{c^2} \sum_{k=\left\lfloor \frac{2\sqrt{n}}{c} \right\rfloor + 1}^{\infty} \frac{1}{k^2} - \frac{4\sqrt{n}}{c}. \qquad (62)
\end{aligned}$$

Ora, se $k \geq 1$ abbiamo che:

$$\frac{1}{k^2} < \frac{1}{k^2 - \frac{1}{4}} = \int_{k-\frac{1}{2}}^{k+\frac{1}{2}} \frac{dt}{t^2}.$$

Ne segue che

$$\begin{aligned} \frac{4n}{c^2} \sum_{k=\left\lfloor \frac{2\sqrt{n}}{c} \right\rfloor + 1}^{\infty} \frac{1}{k^2} &< \frac{4n}{c^2} \int_{\left\lfloor \frac{2\sqrt{n}}{c} \right\rfloor + \frac{1}{2}}^{\infty} \frac{dt}{t^2} \\ &= \frac{4n}{c^2} \left(-\frac{1}{t} \Big|_{\left\lfloor \frac{2\sqrt{n}}{c} \right\rfloor + \frac{1}{2}}^{\infty} \right) \\ &< \frac{4n}{c^2} \frac{1}{\frac{2\sqrt{n}}{c} - \frac{1}{2}} < \frac{4\sqrt{n}}{c}, \end{aligned} \tag{63}$$

essendo $\sqrt{n} \geq \frac{c}{2}$. Infine da (62) e (63) si ha la tesi. ∎

Lemma 11.2.5 *Sia* $0 \leq t < 1$, *allora*

1. $\sum_{v=1}^{\infty} v t^v = \frac{t}{(1-t)^2}$, *e*
2. $\sum_{v=1}^{\infty} v^3 t^v = \frac{t^3+4t^2+t}{(1-t)^4} \leq \frac{6t}{(1-t)^4}$.

Dimostrazione. Differenziando successivamente la serie di potenze

$$\frac{1}{1-t} = \sum_{v=0}^{\infty} t^v$$

si ha

$$\begin{aligned} \frac{1}{(1-t)^2} &= \sum_{v=1}^{\infty} v t^{v-1} \\ \frac{2}{(1-t)^3} &= \sum_{v=2}^{\infty} v(v-1) t^{v-2} \\ \frac{6}{(1-t)^4} &= \sum_{v=3}^{\infty} v(v-1)(v-2) t^{v-3} \\ &= \sum_{v=3}^{\infty} (v^3 - 3v(v-1) - v) t^{v-3}. \end{aligned}$$

Da cui segue subito 1., e inoltre:

$$\sum_{v=3}^{\infty} v^3 t^v = \frac{6t^3}{(1-t)^4} + 3t^2 \sum_{v=3}^{\infty} v(v-1) t^{v-2} + t \sum_{v=3}^{\infty} v t^{v-1}.$$

Si nota direttamente che tale formula rimane valida pure per $v = 2$ e $v = 1$, cioè che vale

$$\begin{aligned}\sum_{v=1}^{\infty} v^3 t^v &= \frac{6t^3}{(1-t)^4} + 3t^2 \sum_{v=2}^{\infty} v(v-1)t^{v-2} + t \sum_{v=1}^{\infty} v t^{v-1} \\ &= \frac{6t^3}{(1-t)^4} + \frac{6t^2}{(1-t)^3} + \frac{t}{(1-t)^2} \\ &= \frac{t^3 + 4t^2 + t}{(1-t)^4} \\ &\leq \frac{6t}{(1-t)^4},\end{aligned}$$

ovvero la tesi. ■

Teorema 11.2.6 (Hardy, Ramanujan / Uspensky)

$$\log p(n) \sim \pi \sqrt{\frac{2n}{3}}.$$

Dimostrazione. [P. Erdös, 1942]
Indichiamo con $c_0 = \pi\sqrt{\frac{2}{3}}$, che possiamo approssimare con $2,565$.
1) Proviamo innanzitutto la stima superiore

$$p(n) \leq e^{c_0\sqrt{n}}, \quad \forall n \in \mathbb{N}. \tag{64}$$

Facciamo induzione su n. La stima è banale per $n = 0$ e $n = 1$.
Sia $n \geq 2$. Dalla formula (60) del Teorema 11.2.1, facendo induzione su n ed applicando nell'ordine i Lemmi 11.2.2, 11.2.5 e 11.2.4, abbiamo che:

$$\begin{aligned}np(n) &= \sum_{\substack{k,v\geq 1 \\ kv\leq n}} v\,p(n-kv) \\ &\leq \sum_{kv\leq n} v e^{c_0\sqrt{n-kv}} \\ &\leq \sum_{kv\leq n} v e^{c_0\sqrt{n} - \frac{c_0 kv}{2\sqrt{n}}} \\ &\leq e^{c_0\sqrt{n}} \sum_{k=1}^{\infty}\sum_{v=1}^{\infty} v \left(e^{-\frac{c_0 k}{2\sqrt{n}}}\right)^v \\ &\leq e^{c_0\sqrt{n}} \sum_{k=1}^{\infty} \frac{e^{-\frac{c_0 k}{2\sqrt{n}}}}{\left(1 - e^{-\frac{c_0 k}{2\sqrt{n}}}\right)^2} \\ &< \frac{2\pi^2}{3c_0^2} n e^{c_0\sqrt{n}} \\ &= n e^{c_0\sqrt{n}},\end{aligned}$$

da cui segue $p(n) \leq e^{c_0\sqrt{n}}$.

2) Proviamo ora che per ogni $0 < \epsilon < c_0$ esiste un $A = A(\epsilon) > 0$ tale che

$$p(n) \geq Ae^{(c_0-\epsilon)\sqrt{n}}, \quad \forall n \in \mathbb{N}. \tag{65}$$

Anche in questo caso, facciamo induzione su n. Per $n = 0$ e $n = 1$ basta prendere $A = e^{-c_0}$.
Sia $n \geq 2$ e assumiamo il risultato vero per ogni intero minore di n. Tenendo conto del Lemma 11.2.2, si ha

$$\begin{aligned} np(n) &= \sum_{\substack{k,v\geq 1 \\ kv\leq n}} vp(n-kv) \\ &\geq A \sum_{kv\leq n} ve^{(c_0-\epsilon)\sqrt{n-kv}} \\ &\geq A \sum_{kv\leq n} ve^{(c_0-\epsilon)\left(\sqrt{n}-\frac{kv}{2\sqrt{n}}-\frac{k^2v^2}{2n^{3/2}}\right)} \\ &\geq Ae^{(c_0-\epsilon)\sqrt{n}} \sum_{kv\leq n} ve^{-(c_0-\epsilon)\left(\frac{kv}{2\sqrt{n}}+\frac{k^2v^2}{2n^{3/2}}\right)}. \end{aligned}$$

Proveremo che $\sum_{kv\leq n} ve^{-(c_0-\epsilon)\left(\frac{kv}{2\sqrt{n}}+\frac{k^2v^2}{2n^{3/2}}\right)} \geq n$.
Poiché $e^{-x} \geq 1 - x$, abbiamo che

$$e^{-(c_0-\epsilon)\frac{k^2v^2}{2n^{3/2}}} \geq 1 - \frac{(c_0-\epsilon)k^2v^2}{2n^{3/2}}$$

e quindi

$$\begin{aligned} &\sum_{kv\leq n} ve^{-(c_0-\epsilon)\left(\frac{kv}{2\sqrt{n}}+\frac{k^2v^2}{2n^{3/2}}\right)} \\ &\qquad \geq \sum_{kv\leq n} ve^{-(c_0-\epsilon)\frac{kv}{2\sqrt{n}}} - \frac{(c_0-\epsilon)}{2n^{3/2}} \sum_{kv\leq n} k^2v^3e^{-(c_0-\epsilon)\frac{kv}{2\sqrt{n}}} \\ &\qquad =: S_1(n) - \frac{(c_0-\epsilon)}{2n^{3/2}} S_2(n). \end{aligned}$$

Stimiamo separatamente $S_1(n)$ e $S_2(n)$.
Se $kv > n$, allora

$$\frac{(c_0-\epsilon)kv}{2\sqrt{n}} > \frac{(c_0-\epsilon)\sqrt{n}}{2} > \frac{c_0-\epsilon}{2} > 0.$$

Essendo $e^{-t} \ll t^{-6}$; per $t \geq \frac{c_0-\epsilon}{2}$ abbiamo che

$$\begin{aligned}
\sum_{kv>n} v e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}} &\ll \sum_{kv>n} v \left(\frac{(c_0-\epsilon)kv}{2\sqrt{n}}\right)^{-6} \\
&\ll n^3 \sum_{kv>n} \frac{1}{k^6 v^5} \\
&\ll n^3 \sum_{kv>n} \frac{1}{(kv)^{7/2} k^{5/2} v^{3/2}} \\
&< \frac{1}{\sqrt{n}} \sum_{k=1}^{\infty} \frac{1}{k^{5/2}} \sum_{v=1}^{\infty} \frac{1}{v^{3/2}} \\
&\ll \frac{1}{\sqrt{n}}.
\end{aligned}$$

Quindi, per i Lemmi 11.2.4 e 11.2.5

$$\begin{aligned}
S_1(n) &= \sum_{kv\leq n} v e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}} \\
&= \sum_{k\geq 1} \sum_{v\geq 1} v e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}} - \sum_{kv>n} v e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}} \\
&= \sum_{k\geq 1} \frac{e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}}}{\left(1-e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}}\right)^2} + O\left(\frac{1}{\sqrt{n}}\right) \\
&> \frac{2\pi^2 n}{3(c_0-\epsilon)^2} + O(\sqrt{n}) \\
&> \left(1+\frac{2\epsilon}{c_0}\right) n + O(\sqrt{n}),
\end{aligned}$$

poiché

$$\frac{2\pi^2}{3(c_0-\epsilon)^2} = \left(\frac{c_0}{c_0-\epsilon}\right)^2 = \left(1+\frac{\epsilon}{c_0-\epsilon}\right)^2 > 1+\frac{2\epsilon}{c_0},$$

ovvero abbiamo provato che

$$S_1(n) > \left(1+\frac{2\epsilon}{c_0}\right) n + O(\sqrt{n}). \tag{66}$$

Per quanto riguarda $S_2(n)$, utilizzando i Lemmi 11.2.5 e 11.2.3, otteniamo

$$\begin{aligned}
S_2(n) &= \sum_{kv\le n} k^2 v^3 e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}} \\
&\le \sum_{k=1}^{n} k^2 \sum_{v=1}^{\infty} v^3 e^{-\frac{(c_0-\epsilon)kv}{2\sqrt{n}}} \\
&\le 6\sum_{k=1}^{n} \frac{k^2 e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}}{\left(1-e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}\right)^4} \\
&\le 6\sum_{k=1}^{n} \frac{e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}}{\left(1-e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}\right)^2} \frac{k^2}{\left(1-e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}\right)^2} \\
&< 6\sum_{k=1}^{n} \frac{4n}{(c_0-\epsilon)^2k^2} \frac{k^2}{\left(1-e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}\right)^2} \\
&\ll n\sum_{k=1}^{n} \frac{1}{\left(1-e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}\right)^2}.
\end{aligned}$$

Sia $x = \frac{(c_0-\epsilon)k}{2\sqrt{n}}$. Se $1 \le k \le \sqrt{n}$, allora $0 < x \le \frac{c_0}{2}$ e

$$1 - e^{-x} = \int_0^x e^{-t}dt \ge xe^{-x} > xe^{-c_0/2}.$$

Ne segue che

$$\sum_{k=1}^{\sqrt{n}} \frac{1}{\left(1-e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}\right)^2} < \frac{4ne^{c_0}}{(c_0-\epsilon)^2} \sum_{k=1}^{\sqrt{n}} \frac{1}{k^2} \ll n.$$

Se invece $k > \sqrt{n}$, allora

$$\sum_{k=\sqrt{n}+1}^{n} \frac{1}{\left(1-e^{-\frac{(c_0-\epsilon)k}{2\sqrt{n}}}\right)^2} < \sum_{k=\sqrt{n}+1}^{n} \frac{1}{\left(1-e^{-\frac{(c_0-\epsilon)}{2}}\right)^2} \ll n.$$

Ne segue che

$$S_2(n) \ll n^2. \tag{67}$$

Essendo ovviamente $S_1(n)$ ed $S_2(n)$ entrambi positivi, abbiamo

$$\begin{aligned}
S_1(n) - \frac{(c_0-\epsilon)}{2n^{3/2}} S_2(n) &\ge \left(1+\frac{2\epsilon}{c_0}\right) n + O(\sqrt{n}) - \frac{(c_0-\epsilon)}{2n^{3/2}} O(n^2) \\
&> \left(1+\frac{2\epsilon}{c_0}\right) n - c_1\sqrt{n},
\end{aligned}$$

per qualche costante $c_1 > 0$.
Riassumendo, abbiamo che

$$\begin{aligned} np(n) &\geq Ae^{(c_0-\epsilon)\sqrt{n}}\left(S_1(n) - \frac{(c_0-\epsilon)}{2n^{3/2}}S_2(n)\right) \\ &\geq Ane^{(c_0-\epsilon)\sqrt{n}} + A\sqrt{n}e^{(c_0-\epsilon)\sqrt{n}}\left(\frac{2\epsilon\sqrt{n}}{c_0} - c_1\right) \\ &> Ane^{(c_0-\epsilon)\sqrt{n}}, \end{aligned}$$

se $\frac{2\epsilon\sqrt{n}}{c_0} - c_1 > 0$, ovvero se $n > \left(\frac{c_0c_1}{2\epsilon}\right)^2$. Pertanto, a patto di scegliere $A > 0$ abbastanza piccolo per cui valga $p(n) \geq Ae^{(c_0-\epsilon)\sqrt{n}}$ anche per i valori di $n \leq \left(\frac{c_0c_1}{2\epsilon}\right)^2$, abbiamo provato la 2.

Da 1. e 2. segue che per ogni $\epsilon > 0$ esiste un $A = A(\epsilon) > 0$ tale che

$$(c_0 - \epsilon)\sqrt{n} + \log A < \log p(n) < c_0\sqrt{n},$$

per ogni naturale $n > 0$. Dividendo per $c_0\sqrt{n}$ e facendo tendere n all'infinito, si ottiene l'uguaglianza asintotica $\log p(n) \sim c_0\sqrt{n}$. ■

LA DENSITÀ DETERMINA L'ASINTOTO

Nel Capitolo 10 abbiamo introdotto il concetto di densità di Schnirel'man per un sottoinsieme di numeri naturali. Diamo ora la seguente

Definizione 11.3.1 *Diremo che un sottoinsieme A di numeri naturali positivi ha* densità (asintotica) *α se esiste $\lim_{x\to\infty}\frac{A(x)}{x}$ e*

$$\lim_{x\to\infty}\frac{A(x)}{x} = \alpha,$$

dove al solito, $A(x) = \sum_{\substack{1\leq a\leq x\\ a\in A}} 1$.

Indicheremo con $d(A)$ l'eventuale densità dell'insieme A.

In questa sezione proveremo il seguente

Teorema 11.3.1 *Sia A un sottoinsieme non vuoto di interi positivi. Se A ha densità $\alpha > 0$ e $MCD(A) = 1$, allora*

$$\log p_A(n) \sim c_0\sqrt{\alpha n}.$$

Incominciamo con l'osservare che se A ha densità α, allora per ogni $\epsilon > 0$ esiste un reale $x_0(\epsilon) > 0$ tale che per ogni $x \geq x_0(\epsilon)$,

$$(\alpha - \epsilon)x < A(x) < (\alpha + \epsilon)x. \tag{68}$$

In corrispondenza di tale $x_0(\epsilon)$, esiste un $k_0(\epsilon) > 0$ tale che se $a_k \in A$ e $k \geq k_0(\epsilon)$ allora $a_k \geq x_0(\epsilon)$. Ponendo $x = a_k$ in (68) otteniamo pertanto che: dato $\epsilon > 0$, esiste $k_0(\epsilon) > 0$ tale che se $k \geq k_0(\epsilon)$, allora:

$$\frac{k}{\alpha + \epsilon} < a_k < \frac{k}{\alpha - \epsilon}.$$

Lemma 11.3.2 *Sia A un sottoinsieme cofinito di $\mathbb{N}^*$ (ovvero tale che il suo complementare sia finito). Allora*

$$\log p_A(n) \sim c_0\sqrt{n}.$$

Dimostrazione. Poiché A è cofinito, ogni intero sufficientemente grande appartiene ad A; sia quindi $l > 1$ tale che $B = \{n | n > l\} \subseteq A$. Allora ovviamente

$$p_B(n) \leq p_A(n) \leq p(n), \quad \forall n \in \mathbb{N}^*.$$

Poiché per il Teorema 11.2.6 $\log p(n) \sim c_0\sqrt{n}$, basta provare che $\log p_B(n) \sim c_0\sqrt{n}$.

Sia $F = \{1, 2, \ldots, l\}$. Essendo F finito e $MCD(F) = 1$, per il Teorema 11.1.1, esiste una costante $c > 0$ tale che $p_F(n) \leq cn^{l-1}$ per ogni $n \in \mathbb{N}^*$. Ora, se π è un'arbitraria partizione di n, allora

$$\pi : n = r_1 + r_2 + \ldots + r_k + r_{k+1} + \ldots + r_t$$

per qualche $r_1, \ldots, r_k \in B$ e $r_{k+1}, \ldots, r_t \in F$, univocamente determinati da π. Ma allora le partizioni

$$\begin{aligned} \pi_1 : &\quad m = r_1 + r_2 + \ldots + r_k \\ \pi_2 : n - m &= r_{k+1} + \ldots + r_t \end{aligned}$$

sono rispettivamente elementi di $\mathsf{P}_B(m)$ e $\mathsf{P}_F(n-m)$. Ne segue che

$$p(n) \leq \sum_{m=0}^{n} p_B(m)p_F(n-m).$$

Pertanto

$$\begin{aligned} p(n) &\leq \sum_{m=0}^{n} p_B(m)p_F(n-m) \\ &\leq cn^{l-1} \sum_{m=0}^{n} p_B(m) \\ &\leq 2cn^l p_B(n) \\ &\leq 2cn^l p(n), \end{aligned}$$

dove si è usato il fatto che la funzione p_B è crescente (Esercizio 11.10). Passando ai logaritmi e dividendo per $c_0\sqrt{n}$, otteniamo

$$\begin{aligned} \frac{\log p(n)}{c_0\sqrt{n}} &\leq \frac{\log 2c + l\log n}{c_0\sqrt{n}} + \frac{\log p_B(n)}{c_0\sqrt{n}} \\ &\leq \frac{\log 2c + l\log n}{c_0\sqrt{n}} + \frac{\log p(n)}{c_0\sqrt{n}}, \end{aligned}$$

da cui la tesi facendo tendere $n \to \infty$. ■

Dimostrazione del Teorema 11.3.1.
Sia $A = \{a_1 < a_2 < \dots\} \subseteq \mathbb{N}^*$ e sia $d(A) = \alpha$. Preso un $0 < \epsilon < \alpha$ esiste un intero $l_0 = l_0(\epsilon) > 0$ tale che $MCD(a_1, \dots, a_{l_0}) = 1$ e

$$\frac{k}{\alpha + \epsilon} < a_k < \frac{k}{\alpha - \epsilon}, \quad \forall k \geq l_0.$$

Proviamo nell'ordine:

1. $\limsup_n \frac{\log p_A(n)}{c_0 \sqrt{\alpha n}} \leq 1$,

2. $\liminf_n \frac{\log p_A(n)}{c_0 \sqrt{\alpha n}} \geq 1$.

1. Siano $F = \{a_1, \dots, a_{l_0}\}$ e $B = \{a_k \in A | k > l_0\}$.
Preso un intero $m \leq n$ ad ogni partizione $\pi \in \mathsf{P}_B(m)$

$$\pi : m = a_{k_1} + a_{k_2} + \dots + a_{k_r},$$

con $a_{k_i} \in B$, associamo la partizione

$$\psi(\pi) : n' = k_1 + k_2 + \dots + k_r.$$

Essendo per ogni i, $k_i < (\alpha + \epsilon) a_{k_i}$ si ha

$$n' < (\alpha + \epsilon) \sum_{i=1}^{r} a_{k_i} = (\alpha + \epsilon) m \leq (\alpha + \epsilon) n.$$

Ne segue che l'applicazione

$$\begin{aligned} \psi : \mathsf{P}_B(m) &\longrightarrow \bigcup_{n'=1}^{(\alpha+\epsilon)n} \mathsf{P}(n') \\ \pi &\longmapsto \psi(\pi) \end{aligned}$$

è ben definita e iniettiva. Essendo $p(n)$ ovviamente crescente, otteniamo che

$$\begin{aligned} p_B(m) &\leq \sum_{n'=1}^{(\alpha+\epsilon)n} p(n') \\ &\leq (\alpha + \epsilon) n \, p(\lfloor (\alpha + \epsilon) n \rfloor) \\ &< 2n \, p(\lfloor (\alpha + \epsilon) n \rfloor). \end{aligned}$$

Ora $A = F \cup B$ e per il Teorema 11.1.1 esiste una costante $c > 0$ tale che per ogni naturale n

$$p_F(n) \leq c n^{l_0 - 1}.$$

Essendo ogni $\pi \in \mathsf{P}_A(n)$ decomponibile come somma di due partizioni appartenenti rispettivamente a $\mathsf{P}_B(m)$ e $\mathsf{P}_F(n-m)$, per qualche $0 \leq m \leq n$, otteniamo che

$$\begin{aligned} p_A(n) &= \sum_{m=0}^{n} p_F(n-m)p_B(m) \\ &\leq cn^{l_0-1} \sum_{m=0}^{n} p_B(m) \\ &\leq cn^{l_0-1} \sum_{m=0}^{n} 2np(\lfloor(\alpha+\epsilon)n\rfloor) \\ &\leq 4cn^{l_0+1} p(\lfloor(\alpha+\epsilon)n\rfloor). \end{aligned}$$

Ora $\log p(n) \sim c_0\sqrt{n}$ e quindi in corrispondenza di $\epsilon > 0$ esiste $n_0(\epsilon) \in \mathbb{N}$ per cui, per ogni $n \geq n_0(\epsilon)$:

$$\log p(\lfloor(\alpha+\epsilon)n\rfloor) < (1+\epsilon)\sqrt{\lfloor(\alpha+\epsilon)n\rfloor}.$$

Ne segue che

$$\begin{aligned} \log p_A(n) &\leq \log 4c + (l_0+1)\log n + \log p(\lfloor(\alpha+\epsilon)n\rfloor) \\ &< \log 4c + (l_0+1)\log n + (1+\epsilon)c_0\sqrt{(\alpha+\epsilon)n}, \end{aligned}$$

per ogni $n \geq n_0(\epsilon)$. Quindi

$$\frac{\log p_A(n)}{c_0\sqrt{\alpha n}} \leq \frac{\log 4c + (l_0+1)\log n}{c_0\sqrt{\alpha n}} + (1+\epsilon)\sqrt{1+\frac{\epsilon}{\alpha}},$$

e pertanto

$$\limsup_n \frac{\log p_A(n)}{c_0\sqrt{\alpha n}} \leq (1+\epsilon)\sqrt{1+\frac{\epsilon}{\alpha}},$$

che, valendo per ogni $\epsilon > 0$, implica $\limsup_n \frac{\log p_A(n)}{c_0\sqrt{\alpha n}} \leq 1$.

2. Essendo $MCD(A) = 1$ per la Proposizione 1.1.3 del Capitolo 1, abbiamo $p_A(n) \geq 1$ per ogni n sufficientemente grande. Scelto arbitrariamente $0 < \epsilon < \alpha$, sia $l_0 = l_0(\epsilon) \in \mathbb{N}$ tale che

$$MCD(a_1, \ldots, a_{l_0}) = 1 \quad \text{e} \quad \frac{k}{\alpha+\epsilon} < a_k < \frac{k}{\alpha-\epsilon}, \ \forall k > l_0.$$

Chiamiamo $U = \{l \in \mathbb{N} | l > l_0\}$. Ad ogni $\pi \in \mathsf{P}_U(n)$

$$\pi : \ n = k_1 + \ldots + k_t,$$

associamo

$$\varphi(\pi) : \ m = a_{k_1} + \ldots + a_{k_t}$$

e notiamo che $\varphi(\pi) \in \mathsf{P}_B(m)$, con

$$m \leq \sum_{i=1}^{t} \frac{k_i}{\alpha-\epsilon} = \frac{1}{\alpha-\epsilon}\sum_{i=1}^{t} k_i = \frac{n}{\alpha-\epsilon}.$$

Allora l'applicazione

$$\begin{aligned} \varphi : \mathsf{P}_U(n) &\longrightarrow \bigcup_{m \leq \frac{n}{\alpha-\epsilon}} \mathsf{P}_A(m) \\ \pi &\longmapsto \varphi(\pi) \end{aligned}$$

è ben definita ed iniettiva. Ne segue che

$$\begin{aligned} p_U(n) &\leq \sum_{m \leq \frac{n}{\alpha-\epsilon}} p_A(m) \\ &\leq \frac{n}{\alpha-\epsilon} \max\left\{ p_A(m) \,\middle|\, m \leq \frac{n}{\alpha-\epsilon} \right\} \\ &\leq \frac{n}{\alpha-\epsilon} p_A(u_n), \end{aligned}$$

per qualche intero u_n tale che $\frac{n}{\alpha-\epsilon} - a_1 < u_n \leq \frac{n}{\alpha-\epsilon}$, per l'Esercizio 11.6. La successione $\{u_n\}_n$ non è necessariamente crescente, anche se $\lim_n u_n = \infty$. Occorre trovare un'opportuna sottosuccessione crescente. Prendiamo $d \in \mathbb{N}$ tale che

$$0 < (\alpha-\epsilon)a_1 \leq d < (\alpha-\epsilon)a_1 + 1.$$

Per ogni $i, j \geq 1$ vale

$$\begin{aligned} u_{(i+j)d} - u_{id} &> \left(\frac{(i+j)d}{\alpha-\epsilon} - a_1 \right) - \frac{id}{\alpha-\epsilon} \\ &\geq \frac{jd}{\alpha-\epsilon} - a_1 \\ &\geq (j-1)a_1. \end{aligned}$$

Segue che $u_{(i+j)d} > u_{id}$, cioè $\{u_{id}\}_i$ è una sottosuccessione strettamente crescente.
In maniera simile a sopra, otteniamo che

$$\begin{aligned} u_{(i+j)d} - u_{id} &< \frac{(i+j)d}{\alpha-\epsilon} - \left(\frac{id}{\alpha-\epsilon} - a_1 \right) \\ &= \frac{jd}{\alpha-\epsilon} + a_1 \\ &< (j+1)a_1 + \frac{j}{\alpha-\epsilon}. \end{aligned}$$

Scegliamo ora un intero N_0 tale che $p_A(n) \geq 1$, per ogni $n \geq N_0$ (esiste poiché per l'Esercizio 11.10, p_A è definitivamente crescente). Sia $i_0 \in \mathbb{N}$ tale che

$$\frac{N_0}{a_1} + 1 \leq i_0 < \frac{N_0}{a_1} + 2.$$

Allora $u_{id} - u_{(i-i_0)d} > (i_0 - 1)a_1 \geq N_0$, per ogni $i \geq i_0$.
Inoltre, per ogni $n \geq u_{i_0 d}$ esiste un intero $j \geq i_0$ tale che $u_{jd} \leq n < u_{(j+1)d}$, e quindi

$$n - u_{(j-i_0)d} < u_{(j+1)d} - u_{(j-i_0)d} < (i_0+2)a_1 + \frac{i_0+1}{\alpha-\epsilon}$$

e

$$n - u_{(j-i_0)d} \geq u_{jd} - u_{(j-i_0)d} > N_0.$$

Ma allora abbiamo che:

$$p_A(n - u_{(j-i_0)d}) \geq 1.$$

Per l'Esercizio 11.5 e la definizione di $u_{(j-i_0)d}$,

$$\begin{aligned} p_A(n) &= p_A\big(u_{(j-i_0)d} + (n - u_{(j-i_0)d})\big) \\ &\geq p_A(u_{(j-i_0)d}) \\ &> \frac{(\alpha-\epsilon)p_U((j-i_0)d)}{(j-i_0)d}. \end{aligned}$$

Poiché $n < u_{(j+1)d} \leq \frac{(j+1)d}{\alpha-\epsilon}$, si ha $(j-i_0)d > (\alpha-\epsilon)n - (i_0+1)d$ e

$$p_A(n) > \frac{(\alpha-\epsilon)p_U\big((\alpha-\epsilon)n - (i_0+1)d\big)}{(j-i_0)d},$$

essendo p_U crescente (Esercizio 11.10). Ma U è cofinito, quindi per il Lemma 11.3.2, se $n \gg 0$ abbiamo che

$$\begin{aligned} \log p_A(n) &> \log(\alpha-\epsilon) + \log p_U\big((\alpha-\epsilon)n - (i_0+1)d\big) + \\ &\qquad - \log(j-i_0)d \\ &> \log(\alpha-\epsilon) + (1-\epsilon)c_0\sqrt{(\alpha-\epsilon)n - (i_0+1)d} + \\ &\qquad - \log(j-i_0)d. \end{aligned}$$

Dividendo per $c_0\sqrt{\alpha n}$ e passando al lim inf si ottiene

$$\begin{aligned} \liminf_n \frac{\log p_A(n)}{c_0\sqrt{\alpha n}} &\geq (1-\epsilon)\sqrt{\frac{(\alpha-\epsilon)n - (i_0+1)d}{\alpha n}} \\ &> (1-\epsilon)\sqrt{1 - \frac{\epsilon}{\alpha}} \end{aligned}$$

Poiché questo vale per ogni $0 < \epsilon < \alpha$ si ha

$$\liminf_n \frac{\log p_A(n)}{c_0\sqrt{\alpha n}} \geq 1.$$

■

L'ASINTOTO DETERMINA LA DENSITÀ

In questa sezione proviamo il Teorema inverso di 11.3.1, ovvero il seguente

Teorema 11.4.1 *Sia A un sottoinsieme non vuoto di numeri naturali tale che $MCD(A) = 1$ e sia $p_A(n)$ il numero di partizioni dell'intero n con parti in A. Se esiste un $\alpha > 0$ tale che $\log p_A(n) \sim c_0\sqrt{\alpha n}$, allora A ha densità α.*

La dimostrazione che daremo è dovuta a M.B. Nathanson ed usa due risultati significativi della teoria delle funzioni generatrici, i cosiddetti Teoremi "Abeliano e Tauberiano" (per i quali si rimanda all'Appendice del Capitolo).

Il punto di partenza per dimostrare il Teorema 11.4.1 è la seguente formula, di cui abbiamo già avuto modo di parlare e che ora dimostriamo in modo rigoroso (in tutta la sua generalità).

Lemma 11.4.2 (L. Eulero) *Sia A un sottoinsieme non vuoto di $\mathbb{N}^*$. Per $x \in \mathbb{R}$, $|x| < 1$ vale*

$$\sum_{n=0}^{\infty} p_A(n)x^n = \prod_{a\in A} \frac{1}{1-x^a}.$$

Dimostrazione. Occorre e basta provare il risultato per $A = \mathbb{N}^*$. A tale proposito restringiamo x all'intervallo $[0,1)$ e introduciamo le funzioni

$$F_m(x) = \prod_{n=1}^{m} \frac{1}{1-x^n} \quad \text{e} \quad F(x) = \prod_{n=1}^{\infty} \frac{1}{1-x^n} = \lim_{m\longrightarrow\infty} F_m(x).$$

Ora, il prodotto che definisce $F(x)$ converge assolutamente in $[0,1)$, essendo il reciproco di $\prod(1-x^n)$ (che converge assolutamente, poiché la serie $\sum x^n$ è assolutamente convergente). È immediato vedere che per ogni fissato $x \in [0,1)$ la successione $\{F_m(x)\}_m$ è crescente. Inoltre ogni $F_m(x)$ è il prodotto di un numero finito di serie assolutamente convergenti, pertanto è essa stessa una serie assolutamente convergente, che possiamo scrivere come

$$F_m(x) = 1 + \sum_{n=1}^{\infty} p_m(n)x^n,$$

dove $p_m(n)$ è essattamente il numero di partizioni di n con parti in $A = \{1,2,\ldots,m\}$. Ovviamente $\lim_{m\longrightarrow\infty} p_m(n) = p(n)$ e possiamo spezzare la serie $F_m(x)$ in due parti:

$$\begin{aligned} F_m(x) &= \sum_{n=0}^{m} p_m(n)x^n + \sum_{n=m+1}^{\infty} p_m(n)x^n \\ &= \sum_{n=0}^{m} p(n)x^n + \sum_{n=m+1}^{\infty} p_m(n)x^n. \end{aligned}$$

Poiché $x \geq 0$ abbiamo

$$\sum_{n=0}^{m} p_m(n)x^n \leq F_m(x) \leq F(x).$$

Questo mostra che la serie $\sum_{n=0}^{\infty} p(n)x^n$ è convergente. Inoltre, poiché $p_m(n) \leq p(n)$, abbiamo

$$\sum_{n=0}^{\infty} p_m(n)x^n \leq \sum_{n=0}^{\infty} p(n)x^n \leq F(x)$$

quindi, per ogni fissato x in $[0,1)$, la serie $\sum_{n=0}^{\infty} p_m(n)x^n$ converge uniformente in m. Mandando $m \longrightarrow \infty$ otteniamo

$$F(x) = \lim_{m\longrightarrow\infty} \sum_{n=0}^{\infty} p_m(n)x^n = \sum_{n=0}^{\infty} \lim_{m\longrightarrow\infty} p_m(n)x^n = \sum_{n=0}^{\infty} p(n)x^n,$$

che prova l'identità di Eulero nel caso $0 \leq x < 1$. Tramite prolungamento analitico la formula vale per ogni $|X| < 1$. ∎

Dimostrazione del Teorema 11.4.1
Sia

$$f(x) := \sum_{n=0}^{\infty} p_A(n)x^n = \prod_{a\in A} \frac{1}{1-x^a},$$

che sappiamo convergere per $|x| < 1$. Poiché $\log p_A(n) \sim c_0\sqrt{\alpha n} = 2\sqrt{\frac{\pi^2\alpha n}{6}}$, per il Teorema abeliano 11.5.1,

$$\log f(x) \sim \frac{\pi^2\alpha}{6(1-x)}.$$

Ora, applicando lo sviluppo $-\log(1-x) = \sum_{k=1}^{\infty} \frac{x^k}{k}$, per $|x| < 1$, si ottiene:

$$\begin{aligned}
\log f(x) &= \log \prod_{a\in A} (1-x^a)^{-1} \\
&= \sum_{a\in A} -\log(1-x^a) \\
&= \sum_{a\in A} \sum_{k=1}^{\infty} \frac{x^{ak}}{k} \\
&= \sum_{n=1}^{\infty} b_n x^n,
\end{aligned}$$

dove per ogni $n \geq 1$, $b_n = \sum_{\substack{a\in A \\ ak=n}} \frac{1}{k} = \sum_{\substack{a\in A \\ a|n}} \frac{a}{n} \geq 0$.
Applicando ora il Teorema tauberiano 11.5.2, si ha

$$S_B(x) := \sum_{n\leq x} b_n \sim \frac{\pi^2\alpha x}{6}.$$

Definiamo la funzione di resto $r(x)$ come

$$S_B(x) = \frac{\pi^2\alpha x}{6}(1 + r(x)).$$

È banale constatare che $S_B(x)$ è crescente, non negativa e $S_B(x) = 0$ se $x < 1$. Inoltre

$$\begin{aligned} S_B(x) &= \sum_{n \le x} \sum_{\substack{a \in A \\ ak = n}} \frac{1}{k} \\ &= \sum_{n \le x} \frac{1}{k} \sum_{\substack{a \in A \\ ak \le x}} 1 \\ &= \sum_{n \le x} \frac{1}{k} A\Big(\frac{x}{k}\Big) . \end{aligned}$$

Per la formula di inversione di Möbius (Teorema 4.2.5), abbiamo che

$$A(x) = \sum_{k \le x} \frac{\mu(k)}{k} S_B\Big(\frac{x}{k}\Big) .$$

Ora, preso un $\epsilon > 0$ esiste un reale positivo $x_0 = x_0(\epsilon)$ per cui $|r(x)| \le \epsilon$ per ogni $x \ge x_0$.
Se $k \le x/x_0$, allora $x/k \ge x_0$ e $|r(x/k)| \le \epsilon$. Se invece $k > x/x_0$, allora $x/k < x_0$ e $0 \le S_B(x/k) \le S_B(x_0)$. Otteniamo pertanto che

$$\begin{aligned} A(x) &= \sum_{k \le x} \frac{\mu(k)}{k} S_B\Big(\frac{x}{k}\Big) \\ &= \sum_{k \le \frac{x}{x_0}} \frac{\mu(k)}{k} \frac{\pi^2 \alpha x}{6k} \left(1 + r\left(\frac{x}{k}\right)\right) + \sum_{\frac{x}{x_0} < k \le x} \frac{\mu(k)}{k} S_B\Big(\frac{x}{k}\Big) \\ &= \frac{\pi^2 \alpha x}{6} \sum_{k \le \frac{x}{x_0}} \frac{\mu(k)}{k^2} + \frac{\pi^2 \alpha x}{6} \sum_{k \le \frac{x}{x_0}} \frac{\mu(k)}{k^2} r\Big(\frac{x}{k}\Big) + \\ &\qquad + \sum_{\frac{x}{x_0} < k \le x} \frac{\mu(k)}{k} S_B\Big(\frac{x}{k}\Big) \\ &= A_1(x) + A_2(x) + A_3(x). \end{aligned}$$

Stimiamo in dettaglio queste tre sommatorie.
Poiché $\sum_{k \le \frac{x}{x_0}} \frac{\mu(k)}{k^2} = \frac{6}{\pi^2} + O(\frac{x_0}{x})$ (Lemma 4.5.3), abbiamo

$$A_1(x) = \alpha x + O(x_0).$$

Similmente

$$\begin{aligned} A_2(x) &= \frac{\pi^2 \alpha x}{6} \sum_{k \le \frac{x}{x_0}} \frac{\mu(k)}{k^2} r\Big(\frac{x}{k}\Big) \\ &\le \frac{\pi^2 \alpha x \epsilon}{6} \sum_{k \le \frac{x}{x_0}} \frac{1}{k^2} \\ &= O(\epsilon x). \end{aligned}$$

Infine, applicando il Teorema 5.1.4,

$$\begin{aligned} A_3(x) &= \sum_{\frac{x}{x_0}<k\le x} \frac{\mu(k)}{k} S_B\Big(\frac{x}{k}\Big) \\ &\le S_B(x_0) \sum_{\frac{x}{x_0}<k\le x} \frac{1}{k} \\ &\le S_B(x_0)\big(\log x + \gamma + O(\frac{1}{x}) - (\log(\frac{x}{x_0}) + \gamma + O(\frac{x_0}{x}))\big) \\ &\le 2S_B(x_0)\log x_0 \\ &= O(x_0). \end{aligned}$$

Ne segue che

$$A(x) = A_1(x) + A_2(x) + A_3(x) = \alpha x + O(\epsilon x)$$

e pertanto

$$\lim_x \frac{A(x)}{x} = \alpha,$$

che è quanto si voleva dimostrare. ■

APPENDICE

Teoremi abeliani e tauberiani

Ad ogni successione di numeri reali $B = \{b_n\}_n$ è possibile associare la sua serie di potenze $f(x) = \sum_{n=0}^{\infty} b_n x^n$, che assumeremo essere convergente per $|x| < 1$. Parlando in modo informale, ogni teorema che dimostra una qualche proprietà della funzione $f(x)$ a partire da proprietà della successione B, si dice *di tipo abeliano*. Viceversa, un teorema è *di tipo tauberiano* fa l'opposto, ovvero se prova che peculiarità della serie $f(x)$ si traducono in proprietà della successione B.

I seguenti risultati sono esempi rispettivamente di Teoremi abeliani e tauberiani.

Teorema 11.5.1 *Sia $B = \{b_n\}_n \subseteq \mathbb{N}$ tale che la serie di potenze $f(x) = \sum_{n=0}^{\infty} b_n x^n$ converga in $|x| < 1$. Se*

$$\log b_n \sim 2\sqrt{\alpha n}, \quad \text{per } n \longrightarrow \infty,$$

allora

$$\log f(x) \sim \frac{\alpha}{1-x}, \quad \text{per } x \longrightarrow 1^-.$$

Teorema 11.5.2 (Hardy, Littlewood) *Sia $B = \{b_n\}_n \subseteq \mathbb{R}_{\ge 0}$ tale che la serie di potenze $f(x) = \sum_{n=0}^{\infty} b_n x^n$ converga in $|x| < 1$. Se*

$$f(x) \sim \frac{1}{1-x}, \quad \text{per } x \longrightarrow 1^-.$$

allora

$$\sum_{k=0}^{n} b_k \sim n, \quad \text{per } n \longrightarrow \infty.$$

Dimostrazioni di entrambi i Teoremi si trovano in [46, Chapter 16].

ESERCIZI

Esercizio 11.1 *Provare che* $\sum_{l=0}^{r} l^j = \frac{r^{j+1}}{j+1} + O(r^j)$.

Esercizio 11.2 *Provare che*

$$\sum_{j=0}^{k-2} \binom{k-1}{j+1} (-1)^j = -\sum_{j=1}^{k-1} \binom{k-1}{j} (-1)^j = 1$$

Esercizio 11.3 *Calcolare* $p(1), p(2), p(3), p(4)$ *e* $p(5)$. *Verificare la formula ricorsiva (61) per* $(n, v) = (4, 2)$. *Posto* $q(n)$ *il numero di partizioni di* n *in parti tutte distinte, calcolare* $q(6)$. *Detto infine* A *l'insieme dei naturali dispari, calcolare* $p_A(6)$.

Esercizio 11.4 *Posto* $A = \{1\} \cup \{2m | m \in \mathbb{N}^*\}$ *provare che* $p_A(2n) = p_A(2n+1)$ *per ogni* $n \in \mathbb{N}^*$.

Esercizio 11.5 *Sia* $A \subseteq \mathbb{N}^*$ *e sia* $n_0 \in \mathbb{N}$ *rtale che* $p_A(n_0) \geq 1$. *Provare che per ogni* $n \in \mathbb{N}^*$, *vale* $p_A(n) \leq p_A(n + n_0)$.

Esercizio 11.6 *Sia* $\varnothing \neq A \subseteq \mathbb{N}^*$ *e sia* $a_1 \in A$. *Provare che* $p_A(n) \leq p_A(n + a_1)$ *per ogni* $n \in \mathbb{N}$. *Se inoltre* x *è un numero reale* $x \geq a_1$, *provare che esiste un intero* u *tale che* $x - a_1 < u \leq x$ *e* $p_A(u) = \max\{p_A(n) | 0 \leq n \leq x\}$.

Esercizio 11.7 *Mostrare che i seguenti sottoinsiemi di* $\mathbb{N}$ *hanno densità* 0*:*

$$A = \left\{2^h | h \in \mathbb{N}\right\} \qquad B = \left\{2^h 3^k | h, k \in \mathbb{N}\right\}.$$

Esercizio 11.8 *Sia* A *un sottoinsieme di* $\mathbb{N}$. *Provare che se* $d(A) = \alpha$ *allora* $d(\mathbb{N} \setminus A) = 1 - \alpha$.

Esercizio 11.9 *Sia* $0 < N_1 < N_2 < \ldots$ *una successione crescente di numeri naturali positivi tale che* $\lim_i \frac{N_{i+1}}{N_i} = \infty$. *Provare che l'insieme*

$$A = \bigcup_{i \geq 1} (N_{2i-1}, N_{2i}]$$

non ha densità.

Esercizio 11.10 *Una partizione* π *di* n *ha un'unica parte massima se*

$$\pi : \ n = a_1 + a_2 + a_3 + \ldots + a_k$$

con $a_1 > a_2 \geq a_3 \geq \ldots \geq a_k$.

Sia $n_0 \in \mathbb{N}^*$ *e sia* $A = \{n | n \geq n_0\}$. *Provare quanto segue*

1. $p_A(n) = 1$ *per ogni* $n_0 \leq n < 2n_0$.
2. *Esiste una biezione tra le partizioni di* n *e le partizioni di* $n+1$ *aventi un'unica parte massima.*
3. *La funzione* $p_A(n)$ *è crescente per ogni* $n \geq 1$ *e strettamente crescente per ogni* $n \gg 1$.

BIBLIOGRAFIA

[1] M. Agrawal, N. Kayal e N. Saxena. «PRIMES is in P». In: *Annals of Mathematics* 160.2 (2004), pp. 781–793.

[2] W. R. Alford, A. Granville e C. Pomerance. «There are infinitely many Carmichael numbers». In: *Ann. of Math. (2)* 139.3 (1994), pp. 703–722.

[3] T. M. Apostol. «A proof that Euler missed: evaluating $\zeta(2)$ the easy way». In: *Math. Intelligencer* 5.3 (1983), pp. 59–60.

[4] T. M. Apostol. *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. New York-Heidelberg: Springer-Verlag, 1976.

[5] R. Balasubramanian, J.-M. Deshouillers e F. Dress. «Problème de Waring pour les bicarrés 1, 2». In: *C. R. Acad. Sci. Paris Sér. I Math.* 303 (1986), 85–88 and 161–163.

[6] K. D. Boklan e J. H. Conway. «Expect at Most One Billionth of a New Fermat Prime!» In: *The Math. Intelligencer* 39.1 (2017), pp. 3–5.

[7] C. Casolo. *Dispense di Algebra 1*. 2014. URL: http://web.math.unifi.it/users/casolo/dispense/algebra1_14.pdf.

[8] C. Casolo. *Dispense di Algebra 2*. 2012. URL: http://web.math.unifi.it/users/casolo/dispense/algebra2_11.pdf.

[9] J.-R. Chen. «Waring's Problem for $g(5) = 37$». In: *Sci. Sinica* 13 (1964), pp. 1547–1568.

[10] J. Chernick. «On Fermat's simple theorem». In: *Bull. Amer. Math. Soc.* 45.4 (1939), pp. 269–274.

[11] Curtis Cooper. *Mersenne Prime Number discovery - $2^{74207281} - 1$ is Prime!* Mersenne Research, Inc. 2016. URL: https://www.mersenne.org/primes/?press=M74207281.

[12] H. Davenport. «On Waring's Problem for Fourth Powers». In: *Ann. Math.* 40 (1939), pp. 731–747.

[13] J. M. De Koninck e F. Luca. *Analytic number theory: exploring the anatomy of integers*. Vol. 134. Graduate Studies in Mathematics. Providence, RI: Amer. Math. Soc., 2012.

[14] L. E. Dickson. «All integers except 23 and 239 are sums of eight cubes». In: *Bull. Amer. Math. Soc.* 45 (1939), pp. 588–591.

[15] U. Eco. *Il pendolo di Foucault*. I grandi tascabili. Bompiani, 2014.

[16] M. El Bacharaoui. «Primes in the Interval $[2n, 3n]$». In: *Int. J. Contemp. Math. Sci.* 1.13 (2006), pp. 617–621.

[17] P. Erdös. «A Theorem of Sylvester and Schur». In: *J. London Math. Soc.* 4 (1934), pp. 282–288.

[18] P. Erdös. «On amicable numbers». In: *Publicationes Mathematicae Debrecen* 4 (1955), pp. 108–111.

[19] P. Erdös. «On an elementary proof of some asymptotic formulas in the theory of partitions». In: *Ann. of Math. (2)* 43 (1942), pp. 437–450.

[20] H. Fürstenberg. «On the infinitude of primes». In: *American Mathematical Monthly* 62.5 (1955), p. 353.

[21] I. Ghersi. *Matematica dilettevole e curiosa*. Matematica. Hoepli, 1988.

[22] R. K. Guy. *Unsolved problems in number theory*. Third edition. Problem Books in Mathematics. New York: Springer-Verlag, 2004.

[23] J. Hadamard. *La psicologia dell'invenzione in campo matematico*. Minima. Cortina Raffaello Editore, 1993.

[24] G. H. Hardy. *A mathematician's apology*. Canto. With a foreword by C. P. Snow, Reprint of the 1967 edition. Cambridge University Press, Cambridge, 1992, p. 153.

[25] G. H. Hardy e S. Ramanujan. «Asymptotic Formulaae in Combinatory Analysis». In: *Proc. London Math. Soc. (2)* 17 (1918), pp. 75–115.

[26] G. H. Hardy e E. M. Wright. *An introduction to the theory of numbers*. Sixth edition. Oxford: Oxford University Press, 2008.

[27] J. Havil. *Gamma. Exploring Euler's Constant*. With a foreword by Freeman Dyson. Princeton, NJ: Princeton University Press, 2003.

[28] H. A. Helfgott. «The ternary Goldbach problem». In: *Annals of Math. Studies, to appear (see arXiv:1501.05438)* ().

[29] J. Hofbauer. «A simple proof of $1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}$ and related identities». In: *Amer. Math. Monthly* 109.2 (2002), pp. 196–200.

[30] P. Hoffman. *The Man Who Loved Only Numbers: The Story of Paul Erdös and the Search for Mathematical Truth*. London: Hachette Books, 1998.

[31] B. Huppert. *Character theory of finite groups*. De Gruyter Expositions in Mathematics. Berlin: Walter de Gruyter & Co., 1998.

[32] I. M. Isaacs. *Character theory of finite groups*. Providence, RI: AMS Chelsea Publishing, 2006.

[33] M. Jaban e M. Ram Murty. «Ramanujan's Proof of Bertrand's Postulate». In: *The American Mathematical Monthly* 120.7 (2013), pp. 650–653.

[34] N. Jacobson. *Basic algebra. I*. Second. W. H. Freeman e Company, New York, 1985.

[35] A. Kempner. «Bemerkungen zum Waringschen Problem». In: *Math. Ann.* 72.3 (1912), pp. 387–399.

[36] J. M. Kubina e M. C. Wunderlich. «Extending Waring's conjecture to 471,600,000». In: *Math. Comp. 55 (192): 815–820* 55.192 (1990), pp. 815–820.

[37] F. Lemmermeyer. *Reciprocity laws. From Euler to Eisenstein*. Springer Monographs in Mathematics. Berlin: Springer-Verlag, 2000.

[38] Yu. V. Linnik. «An elementary solution of the problem of Waring by Schnirelman's method». In: *Rec. Math. [Mat. Sbornik] N.S.* 12.54 (1943), pp. 225–230.

[39] Yu. V. Linnik. «On the representation of large numbers as sums of seven cubes». In: *Rec. Math. [Mat. Sbornik] N. S.* 12(54) (1943), pp. 218–224.

[40] A. Loo. «On the Primes in the Interval $[3n, 4n]$». In: *Int. J. Contemp. Math. Sci.* 6.38 (2011), pp. 1871–1882.

[41] K. Mahler. «On the fractional parts of the powers of a rational number II». In: *Math. Intelligencer* 4.2 (1957), pp. 122–124.

[42] F. Mertens. «in Beitrag zur analytyischen Zahlentheorie». In: *J. Reine Angew. Math* 78 (1874), pp. 46–62.

[43] T. Metsänkylä. «Catalan's conjecture: another old Diophantine problem solved». In: *Bull. Amer. Math. Soc.* 41.1 (2004), pp. 43–57.

[44] P. Mihăilescu. «Primary cyclotomic units and a proof of Catalan's conjecture». In: *J. Reine Angew. Math.* 572 (2004), pp. 167–195.

[45] M. B. Nathanson. *Additive number theory. The classical bases*. Vol. 164. Graduate Texts in Mathematics. New York: Springer-Verlag, 1996.

[46] M. B. Nathanson. *Elementary methods in number theory*. Vol. 195. Graduate Texts in Mathematics. New York: Springer-Verlag, 2000.

[47] P. P. Nielsen. «Odd perfect numbers, Diophantine equations, and upper bounds». In: *Math. Comp.* 84.295 (2015), pp. 2549–2567.

[48] I. M. Niven. «An unsolved case of the Waring problem». In: *American Journal of Mathematics* 66.1 (1944), pp. 137–143.

[49] P. Ochem e M. Rao. «Odd Perfect Numbers Are Greater than 10^{15000}». In: *Math. Comput.* 81 (2012), pp. 1869–1877.

[50] A. M. Odlyzko e H. J. J. te Riele. «Disproof of the Mertens conjecture». In: *J. Reine Angew. Math.* 357 (1985), pp. 138–160.

[51] L. Pantieri e T. Gordini. *L'arte di scrivere con LaTeX*. URL: http://www.lorenzopantieri.net/LaTeX_files/ArteLaTeX.pdf.

[52] S. Ramanujan. «A proof of Bertrand's postulate». In: *J. Indian Math. Soc.* Collected papers of Srinivasa Ramanujan 11 (1919). A cura di AMS Chelsea Publ., pp. 181–182.

[53] O. Ramaré. «On Schnirel'man's constant». In: *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)* 22.4 (1995), pp. 645–706.

[54] P. Ribenboim. *Catalan's conjecture. Are* 8 *and* 9 *the only consecutive powers?* Boston, MA: Academic Press Inc., 1994.

[55] P. Ribenboim. *The book of prime number records.* Second edition. New York: Springer-Verlag, 1989.

[56] H. E. Rose. *A course in number theory*. New York: Oxford University Press, 1994.

[57] P. Seeger. *We'll All Be A-Doubling*. If I Had a Hammer: Songs of Hope & Struggle. Folkways. 1988. URL: https://www.youtube.com/watch?v=OkFt-9KFrjQ.

[58] R. Taylor e A. Wiles. «Ring-theoretic properties of certain Hecke algebras». In: *Ann. of Math. (2)* 141.3 (1995), pp. 553–572.

[59] Trilussa. *Tutte le poesie*. I Meridiani. Mondadori, 2004.

[60] Uspensky. Ya. V. «Asymptotic expressions of numerical functions occurring in problem concerning the partition of numbers into summands». In: *Bull. Acad. Sci. de Russie* 14.6 (1920), pp. 199–218.

[61] R. C. Vaughan e T. Wooley. «Waring's Problem: A Survey». In: *Number Theory for the Millennium. III* (2002), pp. 301–340.

[62] A. Veil. *Ricordi di apprendistato. Vita di un matematico.* Ritratti. Castelvecchi, 2013.

[63] E. Waring. *Meditationes Algebraicae*. (Editio tertia recensita et aucta). Cantabrigi : typis Academicis excudebat J. Archdeacon; veneunt apud J. Nicholson; J. C. et al., 1782.

[64] A. Wieferich. «Beweis des Satzes, daß sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt». In: *Math. Ann.* 66.1 (1908), pp. 95–101.

[65] Wikipedia. *Record di velocità*. URL: https://it.wikipedia.org/wiki/Record_di_velocit%C3%A0.

[66] A. Wiles. «Modular elliptic curves and Fermat's last theorem». In: *Ann. of Math. (2)* 141.3 (1995), pp. 443–551.

[67] T. D. Wooley. «Large Improvements in Waring's Problem». In: *Ann. Math.* 135 (1992), pp. 131–164.

INDICE ANALITICO