Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Triennale in Matematica

I NUMERI PRIMI

Tesi di Laurea in Teoria dei Numeri

Relatore:
Chiar.mo Prof.
Calogero Tinaglia

Presentata da:
Caterina Cammera

Seconda Sessione
Anno Accademico 2009/2010

"La Matematica è la regina di tutte le scienze
e la Teoria dei Numeri è la regina della Matematica"
Carl Friedrich Gauss

Indice

Introduzione

La teoria dei numeri, o aritmetica superiore, è considerata la branca "più pura" della matematica pura ed ha come oggetto lo studio delle proprietà dei numeri interi.
Questi numeri hanno attirato la curiosità umana fin dai tempi antichi come dimostrato dalle documentazioni degli antichi greci.
Più in generale, la materia è giunta ad occuparsi di una più ampia classe di problemi che sono sorti naturalmente dallo studio degli interi e contiene molti problemi aperti che possono essere facilmente compresi anche da chi non è un matematico.
Vide la sua rinascita nel XVI e nel XVII secolo nelle opere soprattutto di Pierre de Fermat.
Nel XVIII secolo Eulero e Lagrange diedero importanti contributi alla teoria e, al suo termine, la disciplina iniziò ad avere una forma scientifica grazie ai grandi lavori di Legendre (1798), e Gauss (1801). Con le Disquisitiones Arithmeticae (1801) di Gauss può dirsi iniziata la moderna teoria dei numeri.
Una peculiarità della teoria dei numeri è la grande difficoltà che si è spesso incontrata nel dimostrare semplici teoremi generali che l'evidenza numerica aveva suggerito in modo naturale. Gauss affermava
"È proprio questo fatto che dà all'aritmetica superiore quel magico fascino che l'ha resa la scienza preferita dai più grandi matematici, per non parlare della sua ricchezza inesauribile, dove supera di gran lunga altre parti della matematica."
La teoria dei numeri può essere divisa in diversi campi a seconda dei metodi

utilizzati e dei problemi studiati.

Alcuni dei più formidabili problemi matematici sono appunto problemi di teoria dei numeri.

In particolare sappiamo ancora molto poco sui numeri primi. Quello di numero primo è uno dei concetti basilari della teoria dei numeri: alla base di questa importanza vi è la possibilità di costruire con essi, attraverso la moltiplicazione, tutti gli altri numeri interi, nonché l'unicità di tale fattorizzazione.

Capitolo 1

Premesse

1.1 Definizioni

Una prima definizione di numero primo è quella fornita da Euclide nel VII libro degli *Elementi*:

> *Numero primo è quello che è misurato (cioè diviso) soltanto dall'unità.*

Oggi la definizione è:

Definizione 1.1. Un naturale $a \neq 0$ si dice **PRIMO** quando è $\neq 1$ e non ha divisori propri.

Ricordando che:

Definizione 1.2. Si dice che un naturale $b \neq 0$ è un **DIVISORE** di un naturale a o che a è un **MULTIPLO** di b se esiste un naturale c tale che $a = bc$.

Definizione 1.3. Dato un naturale $a \neq 0$ i numeri 1 e a si dicono divisori **IMPROPRI**, gli altri divisori si dicono **PROPRI**.

I primi numeri primi sono quindi $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$.
Inoltre

Definizione 1.4. Un naturale $a \neq 0$ si dice **COMPOSTO** o **RIDUCIBILE** quando è $\neq 1$ e non è primo ossia quando ha divisori propri.

Definizione 1.5. Si chiama **FATTORIZZAZIONE STANDARD** di un naturale $a \neq 0$ e $a \neq 1$ una fattorizzazione $a = p_1^{r_1} \dots p_h^{r_h}$ con $p_1 \dots p_h$ primi $p_1 < \dots < p_h$ e $r_1 \geq 1$, $\dots$,$r_h \geq 1$.

Definizione 1.6. Dati a e b naturali si dice **MASSIMO COMUN DIVISORE** di a e b il numero naturale d che è il massimo tra i divisori comuni ad a e b e si scrive $d = MCD(a, b) = (a, b)$

Il MCD esiste sempre ed è unico.

Definizione 1.7. Dati a e b naturali si dice che sono **primi tra loro** o **COPRIMI** quando non hanno divisori propri in comune ossia quando $MCD(a, b) = 1$.

1.2 Alcuni cenni storici

Non è noto quando si è formato il concetto di numero primo, tuttavia la prima testimonianza di una qualche conoscenza della diversità di tali numeri si ha con l'Osso d'Ishango, un reperto osseo datato al 6500 a.C circa.
Trovato nel 1950 tra i monti dell'Africa equatoriale centrale è attualmente conservato presso il museo di storia naturale di Bruxelles. In una delle colonne in cui è suddiviso l'osso compaiono 11, 13, 17 e 19 tacche, cioè i numeri primi tra 10 e 20.

Per trovare un altro segno di questa consapevolezza bisogna aspettare il secondo millennio a.C.; a tale periodo appartengono infatti alcune tavolette egizie contenenti le soluzioni di alcuni problemi aritmetici che, per essere svolti, richiedono una buona conoscenza della fattorizzazione in primi.

La prima traccia incontestabile di un vero studio dei numeri primi è costituita dagli *Elementi* di Euclide, matematico greco antico, che visse molto

Figura 1.1: Euclide

probabilmente durante il regno di Tolomeo I (367 a.C. ca. - 283 a.C.).
È stato sicuramente il più importante matematico della storia antica, e uno dei più importanti e riconosciuti di ogni tempo e luogo.
Gli *Elementi* sono la più importante opera matematica giuntaci dalla cultura greca antica composto tra il IV e il III secolo a.C., che fornisce un quadro completo delle conoscenze matematiche del tempo.
Le parti dei libri degli *Elementi* di Euclide giunte fino a noi sono tra i più antichi testi matematici conosciuti. È un'opera in cui si trovano molte cose degne di nota; in particolare, il tentativo di fornire alla matematica un'adeguata base assiomatica l'ha resa, da questo punto di vista, di fatto insuperata fino a circa due millenni dopo. Probabilmente non sapremo mai quali parti siano originali di Euclide, anche se le dimostrazioni concise e indiscutibili indicano che Euclide sia stato uno dei principali esponenti di una cultura matematica sofisticata.
L'opera consiste in 13 libri nei quali si trova esposta sistematicamente tutta la geometria elementare.
I primi sei riguardanti la geometria piana, i successivi quattro i rapporti tra grandezze e gli ultimi tre la geometria solida.
Nei libri VII, VIII e IX Euclide trattò di numeri dando dei contributi originali. Il libro VII inizia con una serie di 22 definizioni sui diversi tipi di numero, e prosegue con 39 proposizioni tra le quali il famoso 'Algoritmo di Eucli-

de' per determinare il massimo comune divisore (o come dice Euclide stesso 'la misura') tra due numeri; il libro VIII tratta di numeri in progressione e di alcune proprietà di numeri 'quadrati' o 'cubi'; l'ultimo, il IX, contiene alcuni risultati molto interessanti, quali la dimostrazione dell'infinità dei numeri primi, e una proposizione riguardante i numeri perfetti, con la quale si afferma che $2^{p-1}q$ è un numero perfetto ogni volta che $q = 2^p - 1$ è primo.

All'antica Grecia dobbiamo anche il *Crivello di Eratostene*, un semplice algoritmo per determinare quali sono tutti i numeri primi inferiori ad un limite L prefissato, che deve il nome al matematico Eratostene di Cirene vissuto tra il 275 e il 195 a.C., che ne fu l'ideatore.

I secoli seguenti registrarono un certo disinteresse per lo studio dei numeri primi e per diverso tempo non furono provati risultati di particolare rilevanza su questo argomento. Questo periodo viene chiamato Era dell'oscurantismo.

Figura 1.2: Pierre de Fermat

L'interesse verso di essi riprese vigore nel XVII secolo, con le dimostrazioni

di nuovi e importanti risultati, alcuni dei quali dovuti a Pierre de Fermat, matematico francese vissuto tra il 1601 e il 1665. Egli espresse molte delle sue scoperte sottoforma di congettura, senza provvedere ad una dimostrazione, molte di queste furono trovate nel XVIII secolo dal matematico svizzero Leonhard Euler, noto in Italia come Eulero, vissuto tra il 1707 e il 1783.
In particolare congetturò che tutti i numeri nella forma $2^{2^n}+1$ (oggi chiamati in suo onore numeri di Fermat) fossero primi; Fermat stesso aveva verificato la sua congettura fino ad $n = 4$, ma Eulero mostrò che per $n = 5$ si otteneva un numero composto. Ad oggi non sono noti altri numeri di questo tipo che siano primi.
Fermat congetturò inoltre che ogni numero primo della forma $4n + 1$ può essere espresso come somma di due quadrati. Per la dimostrazione di questa congettura bisognerà aspettare Eulero. Il risultato è noto come Teorema di Fermat sulle somme di due quadrati. Fermat propose questo teorema in una lettera a Marin Mersenne datata 25 dicembre 1640, per questo motivo è noto anche come Teorema di Natale di Fermat.
Nello stesso periodo, il monaco francese Marin Mersenne (1588-1648) pose l'attenzione sui primi della forma $2^p - 1$, con p primo, che oggi sono chiamati in suo onore primi di Mersenne.

Figura 1.3: Carl Friedrich Gauss

Dall'inizio del XIX secolo, l'attenzione di molti matematici si rivolse allo

studio della distribuzione asintotica dei primi, ossia allo studio dell'andamento della funzione che conta i primi minori o uguali ad x. Legendre e Gauss congetturarono indipendentemente che tale funzione tende, al crescere di x, a x / ln(x), dove ln(x) indica il logaritmo naturale di x. Tale risultato è oggi noto col nome di teorema fondamentale sui numeri primi.

Capitolo 2

Teoremi importanti

2.1 Teorema fondamentale dell'aritmetica

Le idee chiave che intervengono nel teorema fondamentale dell'aritmetica sono state probabilmente individuate da ogni società che abbia riflettuto a fondo sulla matematica, e fu il genio dei matematici della Grecia antica e successivamente dell'intero bacino del Mediterraneo, a rendersi conto che tali affermazioni sarebbero state giustificate in un modo migliore facendo ricorso a dimostrazioni derivanti da proposizioni più evidenti.
La maggior parte di queste culture matematiche antiche compresero che gli interi possono essere fattorizzati in numeri primi, come passaggio essenziale per determinare tutti i divisori di un intero dato. Nel fare questo devono aver quasi sicuramente assunto, forse senza rendersene conto, che la fattorizzazione di un intero è unica.

Si ha :

Corollario 2.1.1. *Se a, b, d sono naturali e se* $d = (a, b)$ *allora è*

$$a = da', b = db' \qquad con \qquad (a', b') = 1.$$

Dimostrazione. Se fosse $(a', b') = d' > 1$ sarebbe $a' = d'a'', b' = d'b''$ e $a = dd'a'', b = dd'b''$ e quindi dd' è un divisore comune ad a e b.

Inoltre, poichè $d' > 1$, sarebbe $dd' > d$. Ciò è assurdo perchè $d = (a, b)$ è il massimo divisore comune ad a e b. □

Teorema 2.1.2. *Un naturale d è il massimo comun divisore di due naturali a e b, cioè $d = (a, b)$, se e solo se è un divisore comune ad a e b ed è multiplo di tutti i divisori comuni ad a e b.*

Dimostrazione. È ben noto che ogni divisore comune ad a e b è anche divisore del resto della divisione di a per b e viceversa ogni divisore comune a b e al resto è divisore anche di a.
Di conseguenza, applicando l'algoritmo euclideo, l'insieme dei divisori comuni ad $a, b; b, r_1; \ldots ; r_i, r_{i+1}; \ldots ; r_{n-1}, 0$ sono uguali e quindi tutti i divisori comuni ad a e b dividono r_{n-1} che è d.
Viceversa, se d è multiplo di tutti i divisori comuni ad a e b allora è $d = (a, b)$. Infatti sia $d' = (a, b)$, per ipotesi $d'|d$ e pertanto è $d' \leq d$. Poichè d' è il massimo dei divisori comuni ad a e b deve essere anche $d \leq d'$ e quindi è $d = d'$. □

Ne segue :

Lemma 2.1.3 (Lemma di Euclide)**.** *Se un intero positivo n divide il prodotto di due interi positivi a e b, e se n ed a sono coprimi, allora n divide b.*

Cioè:
Se $(a, n) = 1$ e se $n|ab$ allora $n|b$.

Dimostrazione. Poichè, per ipotesi, $n|ab$ allora n è un divisore comune a nb e ab e quindi, per il teorema precedente, $n|(nb, ab)$ essendo (nb, ab) il massimo dei divisori comuni.
Quindi è sufficiente provare che, nell'ipotesi $(a, n) = 1$, è $(nb, ab) = b$.
Sia $(nb, ab) = d$. Poichè $b|nb$ e $b|ab$ allora $b|d$ e quindi è $d = bh$ con h numero naturale ≥ 1.
Basta provare che è $h = 1$.
Si ha $nb = dm = bhm$ e $ab = dr = bhr$, con m e r naturali, quindi $n = hm$,

$a = hr$.
Poichè è $(a, n) = (hr, hm) = 1$ deve essere $h = 1$. □

Questa è una generalizzazione della Proposizione 30 esposta da Euclide nel libro VII:

Proposizione 2.1.4 (Proposizione 30, nota anche come Primo teorema di Euclide)**.** *Se un numero primo è un divisore del prodotto di due numeri, è divisore di uno dei due numeri.*

Ciò si può scrivere come:
Se $p|ab$ allora $p|a$ oppure $p|b$.

Dimostrazione. Poichè p è primo, se non divide a è $(p, a) = 1$. Per il Lemma di Euclide $p|b$. □

Un'altra generalizzazione della proposizione 30 è

Corollario 2.1.5. *Se p è un naturale primo e se $p|p_1 \dots p_n$ con $p, p_1, \dots, p_n$ primi, allora esiste almeno un indice i tale che $p = p_i$.*

Dimostrazione. Se p e p_1 sono primi e se $p|p_1$ allora $p = p_1$.
Se p non divide p_1 allora, per il Lemma di Euclide, $p|p_2 \dots p_n$. Poichè p e p_2 sono primi, se $p|p_2$ allora $p = p_2$.
Se p non divide p_2 allora $p|p_3 \dots p_n$.
In tal modo si trova un indice i tale che $p = p_i$. □

Proposizione 2.1.6 (Proposizione 31)**.** *Ogni numero composto (cioè, non primo) ha per divisore un numero primo.*

Successivamente, nel libro IX, proposizione 14, come se fosse frutto di una riflessione successiva, dimostra che un prodotto di numeri primi distinti non è divisibile per nessun altro numero primo, cioè dimostra il teorema di fattorizzazione unica per i numeri privi di fattori quadratici.

È facile ricavare il teorema fondamentale dell'aritmetica da queste proposizioni di Euclide, e non c'è dubbio che se l'avesse ritenuto un risultato fondamentale l'avrebbe dimostrato, invece esso non compare negli Elementi nonostante alcune proposizioni siano praticamente equivalenti.
Euclide, invece, era più interessato a elencare (con dimostrazione) tutti i divisori di alcuni numeri interi.

Fu solo grazie al genio del giovane Gauss che si capì che questa osservazione fondamentale richiede una dimostrazione e fu necessario attendere le Disquisitiones Arithmeticae di Gauss del 1801 per poter finalmente leggere, all'articolo 16:

> *"Un numero composto può essere fattorizzato in maniera unica come prodotto di primi".*

In questa sua opera, di grande bellezza, Gauss lo dimostra esplicitamente e riconosce a Euclide il merito di tutte le idee essenziali che si trovano all'interno di questa affermazione. In seguito questo risultato è stato celebrato come il più agile e abile ragionamento nella storia del pensiero umano.

Teorema 2.1.7 (Teorema fondamentale dell'aritmetica)**.**
Ogni naturale $a > 1$ o è primo o è decomponibile in un solo modo in fattori primi a meno dell'ordine dei fattori (ossia la fattorizzazione standard di ogni naturale $a > 1$ è unica).

Dimostrazione. Siano

$$a = a_1 = p_1 \dots p_n \qquad \text{e} \qquad a = a_1 = q_1 \dots q_m$$

due decomposizioni in fattori primi (non necessariamente distinti) di $a = a_1$. Possiamo supporre che i fattori primi siano ordinati in ordine crescente, ossia che si abbia

$$p_1 \leq \dots \leq p_n \qquad \text{e} \qquad q_1 \leq \dots \leq q_m.$$

Per provare il teorema basta provare che le due decomposizioni coincidono, ossia che

$$p_1 = q_1, \ldots, p_n = q_m \qquad \text{e} \qquad m = n.$$

Proviamo intanto che $p_1 = q_1$. Poichè $p_1|a$ allora $p_1|q_1 \ldots q_m$. Per (2.1.5), esiste almeno un indice tale i che $p_1 = q_i$.
Sia h il minimo indice tale che $p_1 = q_h$. Dobbiamo provare che è $h = 1$.
Se fosse $q_h \neq q_1$, poichè h è minimo e q_1 il minimo dei q_i, sarebbe $q_1 < q_h = p_1 \leq \ldots \leq p_n$.
Poichè $q_1|a$, per (2.1.5), esiste almeno un indice i tale che $q_1 = p_i$.
Sia k il minimo indice tale che $q_1 = p_k$. Poichè k è minimo e p_1 il minimo dei p_i, sarebbe $p_k > p_1$ e avremmo $p_1 = q_h > q_1 = p_k > p_1$.
Ciò è assurdo e quindi $p_1 = q_1$.
In modo analogo, considerando il numero naturale $a_2 = p_2 \ldots p_n = q_2 \ldots q_m$, si prova che $p_2 = q_2$ e considerando il numero naturale $a_i = p_i \ldots p_n = q_i \ldots q_m$, si prova che $p_i = q_i$.
Se fosse $n > m$ si avrebbe $a_{m+1} = p_{m+1} \ldots p_n = 1$ e ciò è assurdo perchè $1 < p_1 \leq p_{m+1} \leq p_{m+1} \ldots p_n$.
Se fosse $m > n$ si avrebbe $a_{n+1} = 1 = q_{n+1} \ldots q_m$ e ciò è assurdo perchè $1 < q_1 \leq q_{n+1} \leq q_{n+1} \ldots q_m$.
Quindi è $m = n$. □

Il teorema fondamentale dell'aritmetica ci mostra il motivo per cui questi numeri vennero chiamati 'primi', cioè perchè essi sono gli elementi a partire dai quali tutti i numeri naturali possono essere costruiti mediante moltiplicazione, eseguita in tutti i modi possibili.

2.1.1 Crivello di Eratostene

Corollario 2.1.8. *Un naturale $a > 1$ è composto se e solo se ammette un divisore primo p tale che $p^2 \leq a$.*

Dimostrazione. Sia a composto.
Se a è la potenza di un primo p allora è $p^n = a$ con $n \geq 2$ e quindi $p^2 \leq a$.
Se a non è la potenza di un primo, allora avrà almeno due fattori primi diversi p e q. Sia $p < q$. Sarà $p^2 < pq \leq a$.
Viceversa, se a ammette un divisore primo p tale che $p^2 \leq a$ allora è composto.
Infatti se $a = p^2$ o se $p^2 < a$, essendo p primo e quindi $p > 1$, sarà $p < a$ e quindi p è un divisore proprio e a è composto. □

Questo Corollario si può anche enunciare :

Corollario 2.1.9 (Caratterizzazione dei primi)**.** *Ogni naturale $a > 1$ è primo se e solo se non è un quadrato e non è divisibile per alcun primo p tale che $p^2 < a$.*

Il numero 97 non è divisibile per 2, 3, 5, 7. Poichè verifichiamo che $11^2 = 121 > 97$ allora certamente 97 non è divisibile per 11 e quindi 97 è primo.
Da questo segue:

Corollario 2.1.10. *Fissato un primo p, ogni fattore primo di un qualsiasi naturale m compreso tra p e p^2 (ossia $p \leq m \leq p^2$) ha al più un divisore primo maggiore di p.*
Ossia
Fissato un primo p, ogni naturale m tale che $p \leq m \leq p^2$ o è primo oppure ha almeno un divisore primo q è tale che $q \leq p$.

Ne segue il ben noto Crivello di Eratostene, un semplice algoritmo per determinare quali sono tutti i numeri primi inferiori ad un naturale M prefissato e quindi per vedere se M è primo.
Si costruisce un elenco dei naturali compresi tra 2 e M. Si cancellano tutti i multipli di 2 tranne 2. I numeri non cancellati compresi tra 2 e $2^2 = 4$, ossia 3, per il Corollario precedente, sono primi.
Dai numeri rimasti si cancellano tutti i multipli di 3 eccetto 3. I numeri non

cancellati compresi tra 3 e $3^2 = 9$, ossia 5 e 7, sono primi.
Dai numeri rimasti si cancellano tutti i multipli di 5 eccetto 5. I numeri non cancellati compresi tra 5 e $5^2 = 25$, ossia 7, 11, 13, 17, 19, 23, sono primi.
Si prosegue in questo modo fino a cancellare i multipli del primo numero p tale che $p < M \leq p^2$.
I numeri rimasti sono tutti e soli i primi che non superano M.
Ovviamente M sarà composto se viene cancellato (potendo aversi $M = p^2$), altrimenti sarà primo.
Questo algoritmo è a tutt'oggi utilizzato come algoritmo di calcolo dei numeri primi da molti programmi per computer.

2.2 Teorema dell'infinità dei numeri primi

" I numeri primi sono la materia grezza che serve a costruire l'aritmetica e il teorema di Euclide ci assicura che per tale compito noi disponiamo di gran quantità di materiale." di G.H.Hardy.
L'opera di Euclide, *Gli Elementi*, contiene alcuni risultati fondamentali tra cui il teorema dell'infinità dei primi che viene presentato nel IX libro, come proposizione 20, con le parole:

> *"I numeri primi sono più di una qualsiasi assegnata moltitudine di numeri primi."*

Teorema 2.2.1 (Secondo Teorema di Euclide)**.**
Esistono infiniti naturali primi.

Dimostrazione. Siano $p_1 < \ldots < p_n$ i primi n naturali primi ordinati in ordine crescente. Basta dimostrare che per ogni n esiste un primo $p > p_n$.
Sia $M = p_1 \ldots p_n$ e $N = M + 1$, è $N > p_n$.
Se N è primo è $N = p$.
Se N non è primo, per il teorema fondamentale dell'aritmetica, ammette un'unica decomposizione in fattori primi.

Sia p un divisore primo di N. Proviamo che $\forall i = 1, \ldots, n$ è $p \neq p_i$ e quindi, essendo $p_1 < \ldots < p_n$ i primi n naturali primi , $p > p_n$.
Se esiste un indice i tale che $p = p_i$, si ha $p|N$ e $p|M$ quindi $p|1 = N - M$.
Ciò è assurdo perchè p è primo e quindi $p > 1$. □

Una questione che sorge dalla dimostrazione è se i numeri nella forma $p_1 \ldots p_n + 1$, cioè il prodotto dei primi n primi più 1 (detti *numeri di Euclide*), siano o meno primi. Questo avviene nei primi casi ($2 \cdot 3 + 1 = 7$ è primo, così come $2 \cdot 3 \cdot 5 + 1 = 31$), ma è falso in generale: il più piccolo di tali numeri ad essere composto è
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.

La medesima argomentazione della dimostrazione di Euclide sull'infinità dei primi è sufficiente a dimostrare che esistono infiniti primi di un certo tipo prefissato.
Si ha:

Teorema 2.2.2 (Teorema di Dirichlet)**.** *In ogni progressione aritmetica* $y = mx + a$ *con* $(a, m) = 1$ *si trovano infiniti primi.*

Se a e m hanno un fattore comune allora ogni elemento della progressione ha lo stesso fattore, e dunque non è primo.
È necessario pertanto supporre che a e m siano coprimi.

Legendre sembra essere stato il primo a rendersi conto dell'importanza di questa proposizione, ad un certo punto credette di aver trovato una dimostrazione, ma questa si rivelò in seguito erronea.
La prima dimostrazione di questo famosissimo teorema fu prodotta da Johann Peter Gustav Lejeune Dirichlet matematico tedesco vissuto tra il 1805 e il 1859 in un'importante memoria che comparve nel 1837.
Essa fa uso di metodi dell'analisi e costituì la prima applicazione veramente rilevante di tali strumenti alla teoria dei numeri.

Questo teorema rappresenta una naturale generalizzazione di quanto affermato da Euclide, e cioè che esistono infiniti numeri primi.
È importante osservare che il teorema non dice affatto che esistono infiniti numeri primi *consecutivi* in progressione aritmetica.
Eulero affermò che ogni progressione aritmetica che cominci con 1 contiene un infinito numero di primi. Il teorema in questa forma fu prima congetturato da Gauss e dimostrato da Dirichlet nel 1835.
Il teorema di Dirichlet rappresenta l'inizio della moderna teoria dei numeri analitica.
La dimostrazione nel caso $m = 4$ ed $a = 3$ (ossia $a = -1$) si fa ragionando come nella dimostrazione del Secondo teorema di Euclide.

In particolare, poichè ogni primo, tranne 2, è dispari, si ha:

Proposizione 2.2.3. *Ogni* ***primo dispari*** *è della forma* $4k + 1$ *oppure* $4k - 1$ *con* $k \geq 1$ *naturale.*

Poichè $k \geq 1$, si ha $4k - 1 = 4(k - 1) + 3$, quindi $4k - 1$ equivale a $4n + 3$, con $n \geq 0$.
Tutti i naturali sono della forma $4m + r$ con m,r naturali e $0 \leq r < 4$.
Quelli della forma $4m$ oppure $4m + 2$ non sono primi.

Proposizione 2.2.4. *Ogni* ***primo*** > 3 *è della forma* $6k + 1$ *oppure* $6k - 1$ *con* $k \geq 1$ *naturale.*

Poichè $k \geq 1$, si ha $6k - 1 = 6(k - 1) + 5$, quindi $6k - 1$ equivale a $6n + 5$, con $n \geq 0$.
Tutti i naturali sono della forma $6m + r$ con m,r naturali e $0 \leq r < 6$.
Quelli della forma $6m$, $6m + 2$ oppure $6m + 3$ non sono primi.

Proposizione 2.2.5. *Esistono infiniti primi della forma* $4k + 3$.

Dimostrazione. Si scrivono in ordine crescente $3 < p_1 < \ldots < p_n$ tutti i primi n naturali primi > 3 della forma $4k + 3$ con $k > 0$ naturale.

L'insieme di questi primi non è vuoto perchè $p_1 = 7 = 4 \cdot 1 + 3$ e $p_2 = 11 = 4 \cdot 2 + 3$.
Basta provare che esiste $q = 4k + 3$ primo e $q > p_n$ o meglio basta provare che esiste $q > 3$ e $q \neq p_i \ \forall i = 1 \dots n$.
Siano $M = 4p_1 \dots p_n$ e $N = M + 3$.
3 non divide N perchè altrimenti dovrebbe dividere M e ciò è assurdo perchè 3 non divide 4 ed è minore di tutti i primi $p_1, \dots, p_n$.
Se N è primo, essendo $N > p_n$ abbiamo trovato q.
Se N non è primo, la sua fattorizzazione sarà $N = q_1 \dots q_s$, con $q_1, \dots, q_s$ primi (non necessariamente distinti).
Poichè tutti i primi dispari sono della forma $4k + 1$ oppure $4k + 3$, poichè il prodotto di primi della forma $4k + 1$ è un naturale di questa forma e poichè N è della forma $4k + 3$, esisterà un numero dispari (almeno uno) di fattori primi di N della forma $4k + 3$. Sia $q = 4m + 3$ il minimo. Abbiamo già visto che q non può essere 3.
Si ha che $q \neq p_i \ \forall i = 1 \dots n$ perchè altrimenti se fosse $q = p_i$ allora q dovrebbe dividere anche M e quindi anche $N - M = 3$.
Poichè $p_1, \dots, p_n$ sono tutti i primi n naturali primi > 3 della forma $4k + 3$ sarà $q > p_n$. □

Proposizione 2.2.6. *Esistono infiniti primi della forma* $4k + 1$.

Dimostrazione. Il fatto che un numero sia della forma $4k + 1$ non implica che esso abbia un fattore primo dello stesso tipo, quindi questo principio non può essere usato.
Si denotano allora i primi della forma $4k + 1$, (5, 9, 13, 17...), con $r_1, r_2, \dots$, e si considera il numero M definito da $M = (r_1 r_2 \dots r_n)^2 + 1$.
Si dimostra che ogni numero del tipo $a^2 + 1$, come ogni numero che sia somma di due quadrati diversi, ha un fattore primo della forma $4k + 1$, e che anzi è composto interamente da tali fattori ed eventualmente dal primo 2.
Poichè evidentemente M non è divisibile per nessuno tra $r_1, r_2, \dots, r_n$, si conclude che esistono infiniti primi della forma $4k + 1$. □

Poichè se $p = mx + a$, con $(a, m) = 1$ e $a > m$, è un primo allora sta anche nella successione $y = mx + r$ con r resto della divisione di a per m e se $p = mx + q$ è un primo con $x \geq q$ allora p sta nella successione $y = mx + b$ con $b = qm + r$, allora per provare il Teorema di Dirichlet basta provare che in ogni progressione aritmetica $y = mx + a$ con $(a, m) = 1$ e $a < m$ esistono infiniti primi; ossia fissato m, basta provare che il teorema è vero per i $\varphi(m)$ valori di $a < m$ e primi con m, essendo φ la funzione di Eulero definita da $\varphi(m) =$ numero dei naturali coprimi con m e minori di m.
Per quanto appena osservato, avendo provato che esistono infiniti primi della forma $4k + 3$ e della forma $4k + 1$, abbiamo provato il teorema di Dirichlet nel caso $m = 4$ e si può provare anche per progressioni con $m = 6$, infatti è possibile dimostrare con metodi simili che esistono infiniti primi anche di forma $6k + 1$ e $6k - 1$.
È interessante notare che

Proposizione 2.2.7. *L'unica terna di primi dispari consecutivi è* $(3, 5, 7)$.

Dimostrazione. Tutti i naturali sono della forma $3m + r$ con m, n naturali e $0 \leq r < 3$.
Consideriamo i 3 naturali : $n_1 = 3m + t, n_2 = 3m + t + 2, n_3 = 3m + t + 4$.
Uno dei 3 naturali è multiplo di 3 :
se $t = 0$ lo è n_1, se $t = 1$ lo è n_2, se $t = 2$ lo è n_3. Quindi l'unica terna di primi dispari consecutivi si ottiene per $t = 0$ e $m = 1$, cioè $(3, 5, 7)$. □

Nel 1845 Joseph Bertrand (1822-1900) affermò

Teorema 2.2.8 (Teorema di Bertrand)**.** *Se* $n \geq 2$ *allora esiste almeno un primo* p *tale che*

$$n < p < 2n.$$

Lo stesso Bertrand verificò la sua congettura per tutti i numeri minori di $3 \cdot 10^6$. La prima dimostrazione completa della congettura fu data da Pafnuty Lvovich Chebyshev (1821-1894) nel 1850, per cui questo teorema è anche chiamato teorema di Chebyshev.

Nel 1919 Ramanujan semplificò la dimostrazione.
Il teorema di Bertrand venne poi provato con metodi elementari da Paul Erdös, matematico ungherese, nel 1932. Egli dimostrò 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 $2n$. Erdös dimostrò anche che esistono sempre due numeri primi p e q con $n < p, q < 2n$ per ogni $n > 6$.

2.3 Teorema fondamentale sui numeri primi

Una volta dimostrato che i numeri primi sono infiniti, sorge spontaneo chiedersi come si distribuiscono all'interno della sequenza dei numeri naturali, cioè quanto sono frequenti. Un argomento studiato in profondità nei tempi moderni è quello della frequenza con cui i numeri primi si presentano, in altre parole di quanti numeri primi vi siano tra 1 e X quando X è molto grande. Questo numero è denotato con $\pi(X)$, essendo $\pi : \mathbb{N} \to \mathbb{N}$ la funzione aritmetica, cioè funzione che ha come dominio $\mathbb{N}$, detta funzione enumerativa dei primi, definita da $\pi(n)$=numero dei naturali primi minori di n.
La prima congettura riguardo all'ordine di grandezza di $\pi(X)$ come funzione di X sembra essere stata formulata indipendentemente da Legendre e Gauss attorno al 1800.
Essa stabiliva che $\pi(X)$ è approssimativamente $\frac{X}{\ln(X)}$.
Tale congettura sembra essersi basata sull'evidenza numerica, che può essere fuorviante.
Allora meglio asserire che il rapporto tra $\pi(X)$ e $\frac{X}{\ln(X)}$ tende al limite 1 quando X tende a infinito.

Teorema 2.3.1 (Teorema fondamentale sui numeri primi)**.** *Si ha*

$$\lim_{X\to\infty} \frac{\pi(X)}{\frac{X}{\ln(X)}} = 1$$

Questo è il famoso teorema fondamentale sui numeri primi, dimostrato per la prima volta da Hadamard e de la Vallèe Poussin indipendentemente nel

1896. con l'uso di nuovi e potenti metodi analitici. Nel 1948 il matematico norvegese Selberg produsse la prima dimostrazione 'elementare' del teorema, elementare significa che si opera unicamente con numeri naturali.

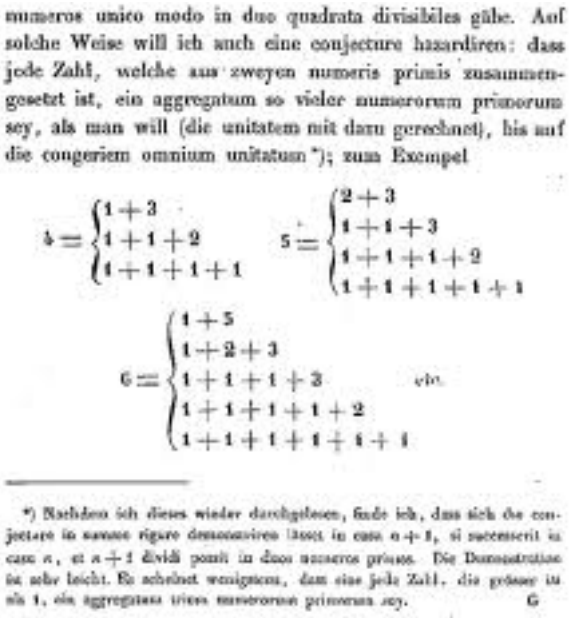
Capitolo 3

Alcuni Problemi Irrisolti

Si hanno molti problemi irrisolti di teoria dei numeri che coinvolgono i numeri primi.
Eccone alcuni:

3.1 Congettura di Goldbach

Nel 1742, il matematico prussiano Christian Goldbach (1690-1764), tutore del figlio dello Zar, scrisse una lettera a Eulero in cui propose la seguente congettura:
"Ogni intero dispari maggiore di 5 può essere scritto come somma di tre numeri primi."
Eulero, interessandosi al problema, rispose riformulandolo nella seguente versione equivalente:
"Ogni numero pari maggiore di 2 può essere scritto come somma di due numeri primi."
La prima delle due è oggi conosciuta come congettura 'debole' di Goldbach, la seconda come congettura 'forte' di Goldbach. L'enunciato della versione forte implica quello della congettura debole, poichè ogni numero dispari maggiore di 5 può essere ottenuto aggiungendo 3 ad ogni numero pari maggiore di 2.



numeros unico modo in duo quadrata divisibiles gäbe. Auf solche Weise will ich auch eine conjecture hazardiren: dass jede Zahl, welche aus zweyen numeris primis zusammengesetzt ist, ein aggregatum so vieler numerorum primorum sey, als man will (die unitatem mit dazu gerechnet), bis auf die congeriem omnium unitatum *); zum Exempel

$$4 = \begin{cases} 1+3 \\ 1+1+2 \\ 1+1+1+1 \end{cases} \qquad 5 = \begin{cases} 2+3 \\ 1+1+3 \\ 1+1+1+2 \\ 1+1+1+1+1 \end{cases}$$

$$6 = \begin{cases} 1+5 \\ 1+2+3 \\ 1+1+1+3 \\ 1+1+1+1+2 \\ 1+1+1+1+1+1 \end{cases} \text{ etc.}$$

*) Nachdem ich dieses wieder durchgelesen, finde ich, dass sich die conjecture in eadem figura demonstriren lässt in casu $n+1$, si successerit in casu n, et $n+1$ dividi possit in duos numeros primos. Die Demonstration ist sehr leicht. Es scheinet wenigstens, dass eine jede Zahl, die grösser ist als 1, ein aggregatum trium numerorum primorum sey. G

Figura 3.1: Lettera di Goldbach ad Eulero, 1742

Si conviene che il termine congettura di Goldbach sia sinonimo di congettura forte di Goldbach. Entrambi i problemi sono rimasti irrisolti fino ad oggi.

Congettura 3.1.1 (Congettura di Goldbach)**.** *Ogni numero naturale pari $n > 2$ è somma di due primi.*

Per esempio:

$$4 = 2 + 2, \qquad 6 = 3 + 3, \qquad 8 = 3 + 5, \qquad 10 = 3 + 7 = 5 + 5$$

È stato dimostrato che la congettura è vera per tutti i pari $n < 2 \cdot 10^{10}$.
La congettura di Goldbach è stata attaccata da molti teorici dei numeri. La maggior parte dei matematici ritiene che la congettura sia vera, basandosi principalmente su considerazioni statistiche e probabilistiche: più grande è il numero pari, più diventa probabile che possa essere scritto come somma di due primi.
Fu pubblicata per la prima volta dal matematico inglese Edward Waring nel 1770, ma non si ebbero grandi progressi fino al XX secolo.

Un primo risultato importante si ebbe con il matematico russo Ivan Vinogradov nel 1937 :

Teorema 3.1.2 (di Vinogradov)**.** *Ogni naturale dispari sufficientemente grande è somma di tre primi.*

Egli dimostrò che ogni numero dispari $n > 3^{3^{15}}$ è somma di tre primi e che quasi tutti i numeri pari possono essere scritti come somma di due primi.
Nel 1966 il matematico cinese Chen Jing-run annunciò e dimostrò :

Teorema 3.1.3 (di Chen Jing-run)**.** *Ogni naturale pari è somma di due naturali $p + a$ con p primo ed a primo oppure prodotto di due primi.*

3.2 Congettura dei primi gemelli

Definizione 3.1. Due naturali primi $p < q$ si dicono **GEMELLI** se $q = p+2$.

Tale denominazione è stata usata per la prima volta da Paul Stäckel nei primi anni del XX secolo.
La congettura dei numeri primi gemelli fu proposta per la prima volta da Euclide intorno al 300 a.C.

Congettura 3.2.1 (Congettura dei primi gemelli)**.** *Esistono infiniti primi gemelli.*

Molti teorici dei numeri hanno tentato di dimostrare questa congettura, ma, a tutt'oggi, non è stata ne' dimostrata ne' confutata.
La maggior parte dei matematici ritiene che questa congettura sia vera, basandosi principalmente sull'evidenza numerica.
Ciò che si ha è solo un lungo, ma finito, elenco di coppie di primi gemelli.
L'unica terna di primi gemelli è la terna $(3, 5, 7)$.
Ogni tanto qualcuno scopre una nuova coppia battendo il record che si era stabilito in precedenza.
Nel tempo, studiando le coppie di primi gemelli si è tentato di individuare

un criterio di distribuzione, ma senza successo. Si è comunque notato che la loro frequenza diminuisce all'aumentare della grandezza dei numeri con cui si opera, ma non si hanno prove per affermare che questo possa valere anche per le coppie ancora sconosciute.

Nel 1849 il matematico francese Alphonse de Polignac (1817 - 1890) enunciò la congettura più generale:

Postulato 1 (di Polignac)**.** *Ogni naturale pari* $2h$ *è differenza in infiniti modi di due primi.*

La cogettura dei primi gemelli si ottiene per $h = 1$.
Nel 1966, Chen Jingrun dimostrò il

Teorema 3.2.2 (dei Primi di Chen Jing-run)**.** *Esistono infiniti primi* p *tali che* $p + 2$ *o è primo oppure è prodotto di due primi.*

Il minore di una coppia di numeri primi gemelli è un *primo di Chen*, per definizione.

3.3 Congettura dei primi $N^2 + 1$

Congettura 3.3.1 (Congettura dei primi $N^2 + 1$)**.** *Esistono infiniti primi della forma* $N^2 + 1$.

Ovviamente se, per $N > 1$, $N^2 + 1$ è primo, necessariamente N è pari.
Primi di questa forma sono:

$$2^2 + 1 = 5, \qquad 4^2 + 1 = 17, \qquad 6^2 + 1 = 37, \qquad 10^2 + 1 = 101.$$

Il miglior risultato è stato provato da Hendrik Iwaniec, matematico polacco, nel 1978.
Egli provò che

Teorema 3.3.2. *Esistono infiniti valori di* N *tali che* $N^2 + 1$ *o è primo oppure è prodotto di due primi.*

Questa congettura è legata ai *Numeri di Fermat.*

3.4 Congettura dei primi di Fermat

Definizione 3.2. Un **numero di Fermat** è un naturale della forma $F_n = 2^{2^n} + 1$.

I primi quattro numeri di Fermat sono primi.
$F_0 = 2^{2^0} + 1 = 3$, $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^4 + 1 = 17$, $F_3 = 2^8 + 1 = 257$ e $F_4 = 2^{16} + 1 = 65537$.
Fermat ha congetturato che fossero tutti primi, ma Eulero ha provato che $F_5 = 641 \cdot 6700417$ e quindi non è primo.
Si ha :

Proposizione 3.4.1. *Due numeri di Fermat sono coprimi.*

Congettura 3.4.2 (Congettura dei primi di Fermat)**.** *Esiste solo un numero finito di primi di Fermat.*

Se questa congettura è falsa allora è vera quella sei primi $N^2 + 1$.

Più in generale per i naturali della forma $N^m \pm 1$ si ha:

Teorema 3.4.3. *Se $N > 1$ e se $N^m \pm 1$ è primo dispari allora N è pari.*
Se $N^m + 1$ è primo allora $m = 2^h$;
Se $N^m - 1$ è primo allora $N = 2$ e m è primo.

Dimostrazione. N deve essere pari altrimenti $N^m \pm 1$ è pari.
Se $N^m + 1$ è primo e se fosse $m = pq$ con q dispari si avrebbe
$N^{pq} + 1 = (N^p)^q + 1^q = (N^p + 1)(N^{p(q-1)} - N^{p(q-2)} + N^{p(q-3)} - \cdots + 1)$
e quindi non sarebbe primo. Perciò deve essere $m = 2^h$.
Se $N^m - 1$ è primo e se fosse $N > 2$ sarebbe $N - 1 \geq 2$ e, per m dispari, si avrebbe

$N^m - 1 = (N-1)(N^{m-1} + \cdots 1)$,
e per $m = 2r$ si avrebbe
$N^m - 1 = (N^r - 1)(N^r + 1)$.
In ogni caso se $N > 2$ allora $N^m - 1$ non è primo.
Quindi è $N = 2$.
Se fosse $m = 2r$ allora deve essere $r = 1$ e quindi $m = 2$ primo;
Se $m = pq$ dispari e p, q divisori propri,si avrebbe
$2^{pq} - 1 = (2^p)^q - 1^q = (2^p - 1)(2^{p(q-1)} + 2^{p(q-2)} + 2^{p(q-3)} + \cdots + 1)$
e $2^m - 1$ non sarebbe primo.
Perciò m deve essere primo.

□

3.5 Numeri di Mersenne e Numeri Perfetti

3.5.1 Numeri di Mersenne

Figura 3.2: Marin Mersenne

Dal precedente teorema abbiamo che $N^m - 1$ può essere primo solo se è della forma $2^p - 1$ con p primo.

Definizione 3.3. I naturali $2^p - 1$ con p primo si chiamano **numeri di Mersenne**, quelli tra questi che sono primi si chiamano **primi di Mersenne**.

Così chiamati in onore di Marin Mersenne teologo, filosofo e matematico francese vissuto fra il 1588 ed il 1648.
Egli insegnò filosofia a Nevers, ma poi rientrò a Parigi dove si dedicò alla matematica ed ebbe contatti con Cartesio e Pascal.
Nel 1611 entrò nell'ordine dei Frati minori e ricevette i voti definitivi a Parigi, nel 1613.
Nel 1644 nel Cogitata Physica Mathematica scrisse che i numeri $2^p - 1$ sono primi per

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

e che questi sono gli unici primi minori di 258 per i quali $2^p - 1$ è primo.
Anche se la sua congettura risultò più tardi non del tutto vera, resta impressionante pensare che ci fosse arrivato senza avere a disposizione nemmeno una macchina calcolatrice. Era evidente ai coetanei di Mersenne che egli non poteva aver calcolato tutti questi numeri, ma neanche loro ci riuscirono.
Oltre 100 anni dopo, nel 1750, Eulero verificò che $2^{31} - 1$ era primo.
Dopo un altro secolo, nel 1876, Lucas verificò che anche $2^{127} - 1$ è primo.
Sette anni più tardi Pervouchine mostrò che $2^{61} - 1$ era primo, quindi Mersenne non aveva considerato questo.
Nei primi anni del 1900 Powers ha mostrato che Mersenne avrebbe dovuto includere nella sua lista anche i numeri primi $2^{89} - 1$ e $2^{107} - 1$.
La primalità di $2^{67} - 1$ non venne messa in discussione per più di 250 anni, finchè, nel 1903, Frank Nelson Cole della Columbia University tenne, ad un incontro della American Mathematical Society, una relazione umilmente intitolata "Sulla fattorizzazione dei grandi numeri". Cole andò alla lavagna ed elevò 2 alla 67ma potenza, per poi sottrarvi 1. Il risultato era un numero composto. Allora, Mersenne aveva torto.
Si è scoperto anche che $2^{257} - 1$ non è primo.

Infine, nel 1947 si stabilì che la lista di Mersenne corretta è:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127.$$

I primi di Mersenne sono strettamente legati al più antico ed irrisolto problema di teoria dei numeri quello dei numeri perfetti.

3.5.2 Numeri Perfetti

Definizione 3.4. Un numero naturale si dice **PERFETTO** quando è uguale alla somma di tutti i suoi divisori escluso se stesso.

Se si include tra i divisori il numero stesso si può dare la seguente definizione:

Definizione 3.5. Un numero naturale si dice **PERFETTO** se il suo doppio è uguale alla somma di tutti i suoi divisori.

Gli antichi Greci osservarono che il numero 6 ha la proprietà interessante di essere uguale alla somma dei suoi divisori, escluso se stesso.
Euclide, nel VII libro dei suoi Elementi, dà la seguente definizione:
"Si dice perfetto ogni numero uguale alla somma dei suoi divisori"(diversi da se stesso)
Capirono che era una proprietà rara e cercarono un metodo per trovare altri numeri perfetti.
Il metodo era strettamente collegato ai Primi che oggi chiamiamo di Mersenne.
Si ha:
Formula di Euclide sui Numeri Perfetti.
Se $2^p - 1$ è un primo (di Mersenne) allora $2^{p-1}(2^p - 1)$ è un numero perfetto.
Sono numeri perfetti :
$6 = 2 \cdot 3 = 2(2^2 - 1) = 1 + 2 + 3,$
$28 = 2^2 \cdot 7 = 2^2(2^3 - 1) = 1 + 2 + 4 + 7 + 14,$
$496 = 2^4 \cdot 31 = 2^4(2^5 - 1) = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248,$

Eulero, circa 2000 anni dopo, ha provato che la formula di Euclide non vale per tutti i numeri perfetti, ma

Teorema 3.5.1 (di Eulero sui numeri perfetti pari)**.** *Ogni numero perfetto pari è della forma* $2^{p-1}(2^p-1)$ *con* 2^p-1 *primo di Mersenne.*

Per dimostrare questo importantissimo teorema definiamo prima la funzione aritmetica σ.
Si chiama funzione aritmetica una funzione che ha come dominio $\mathbb{N}$.

Definizione 3.6. Una funzione aritmetica f si dice MOLTIPLICATIVA se quaunque siano a,b coprimi, si ha $f(ab) = f(a)f(b)$.

La funzione $\sigma : \mathbb{N} - \{0\} \to \mathbb{N}$ è definita da $\sigma(n) =$ somma dei divisori di n. Si ha:

Teorema 3.5.2. *Se* $n = p_1^{r_1} \dots p_h^{r_h}$ *allora*

$$\sigma(n) = \sum_{d|n} d = \prod_{i=1}^{h}(1+p_i+p_i^2+\ldots+p_i^{r_i}) = (1+p_1+\ldots+p_1^{r_1})\dots(1+p_h+\dots p_h^{r_h}).$$

Dimostrazione. Sia $n = p_1^{r_1} \dots p_h^{r_h}$. Un naturale d è un divisore di n se e solo se i suoi fattori primi sono tra quelli di n con esponente non maggiore ossia se e solo se

$$(i) \qquad d = p_1^{s_1} \dots p_h^{s_h} \qquad \text{con } 0 \le s_1 \le r_1, \dots, 0 \le s_h \le r_h.$$

Ogni addendo dello sviluppo del prodotto

$$(ii) \qquad (1 + p_1 + \ldots + p_1^{r_1}) \dots (1 + p_h + \dots p_h^{r_h})$$

è un divisore di n perchè è della forma (i).
Viceversa, d è un divisore di n allora è della forma (i) e quindi d è l'addendo dello sviluppo (ii) che si ottiene prendendo dalla prima parentesi $p_1^{s_1}$, dalla i-esima $p_i^{s_i}$, dall'ultima $p_h^{s_h}$.
Ciò prova che i divisori sono tutti e soli gli addendi dello sviluppo.
La somma di questi addendi ($\sigma(n)$) è proprio lo sviluppo (ii). □

Ad esempio sia $n = 2520 = 2^3 3^2 5 \cdot 7$ si ha
$\sigma(n) = (1+2+4+8)(1+3+9)(1+5)(1+7) = 9360$;
Il divisore $a = 45 = 3^2 5$ è l'addendo dello sviluppo che si ottiene prendendo 1 dalla prima parentesi, 9 dalla seconda, 5 dalla terza e 1 dall'ultima.

Allora un numero n si dice perfetto se vale $\sigma(n) = 2n$.
Per un numero primo p vale $\sigma(p) = p + 1$.

Corollario 3.5.3. *La funzione aritmetica $\sigma(n)$ è moltiplicativa.*

Possiamo ora dimostrare il Teorema di Eulero sui numeri perfetti pari

Dimostrazione. Proviamo prima la parte dovuta ad Euclide ossia se
$N = 2^{p-1}(2^p - 1)$ con $2^p - 1$ primo (di Mersenne) allora è perfetto.
Infatti si ha :
$\sigma(N) = (1 + 2 + \ldots 2^{p-1})[1 + (2^p - 1)] = (2^p - 1)[2^p] = 2 \cdot 2^{p-1}(2^p - 1) = 2N$.
Proviamo ora che se N è perfetto pari allora è $N = 2^{p-1}(2^p - 1)$ con $2^p - 1$ primo di Mersenne.
Poichè N è pari sarà $N = 2^{p-1}M$ con $p > 1$ e M dispari. Ovviamente è $(2^{p-1}, M) = 1$.
Poichè N è perfetto e poichè σ è moltiplicativa, abbiamo:
$2N = 2^p M = \sigma(2^{p-1}M) = \sigma(2^{p-1})\sigma(M) = (2^p - 1)\sigma(M)$.
Quindi è $2^p M = (2^p - 1)\sigma(M)$. Poichè $(2^p - 1, 2^p) = 1$ sarà
$M = (2^p - 1)m$ e $\sigma(M) = 2^p m$.
Proviamo che $m = 1$.
Tenendo conto di queste due relazioni, poichè, se $m > 1$, i quattro naturali $1, 2^p - 1, m, M$ sono divisori distinti di M, sarà

$$\sigma(M) \geq 1 + (2^p - 1) + m + M = 2^p + m + (2^p - 1)m = 2^p + 2^p m = 2^p + \sigma(M) > \sigma(M).$$

Quindi $\sigma(M) \geq 2^p + \sigma(M) > \sigma(M)$. Ciò è assurdo, perciò è $m = 1$.
Si ha $M = 2^p - 1$, $\sigma(M) = 2^p = (2^p - 1) + 1 = M + 1$.

Poichè gli unici naturali n tali che $\sigma(n) = n+1$ sono i primi, sarà $M = 2^p - 1$ primo. □

Non si sa niente sul numero dei numeri perfetti pari, è un argomento talmente incerto che non si fanno congetture.
Nessun numero perfetto dispari è conosciuto e si congettura che non ne esistano.

Bibliografia

[1] H. Davenport, *Aritmetica Superiore*. Zanichelli, 1995.

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

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

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

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

Ringraziamenti

Innanzitutto voglio ringraziare i miei adorati genitori perchè sono speciali.
Per come mi hanno cresciuta, perchè non mi hanno mai fatto mancare niente, per avermi sempre sostenuto, per aver sempre creduto in me e per tutti i sacrifici che hanno sempre fatto.
Papi, per avermi trasmesso la passione per i numeri!! Perchè è buono e onesto e l'unica cosa che desidera è vederci felici.
Per aver lavorato sempre e solo per permetterci di studiare, perchè è la cosa più importante!!
Mami, perchè è sempre presente e comprensiva. Perchè vive solo per noi figlie e per averci trasmesso i valori importanti.
Per essere stata sempre la prima a gioire con me per ogni esame e per avermi capita sempre!!
Le mie meravigliose sorelle perchè le adoro!!
Eli, per avermi sempre appoggiato e incoraggiato, per aver capito i miei tanti "Devo studiare...".
Per avermi detto dopo ogni esame : "Sei il mio genietto".
Soni, per avermi sempre capito e festeggiato!! Perchè crede in me ed io in lei!!
Perchè da brava sorellina cerca di seguire i miei consigli.
La mia Dolce Metà, per avermi fatto riflettere su ciò che realmente desideravo e avermi fatto capire che la mia strada era questa!!
Per avermi sempre spronato, confortato e festeggiato ad ogni esame!!

Per aver creduto in me e per avermi sopportata sempre, soprattutto nell'ultimo periodo!
Per avermi sempre detto :"Certo che ce la farai!!"
Per tutta la sua pazienza e i sacrifici che sta facendo per me ed i miei studi.
Anna e Gianni, perchè mi fanno sentire loro figlia!! Ed Ale una sorella!!
Per aver sempre creduto in me e per avermi sempre festeggiato e incoraggiato.
Tutti i miei cari zii e cugini perchè, anche se lontani, li ho sempre sentiti vicini.
Gioia, perchè se non fosse stato per lei questo sarebbe rimasto solo un sogno!!
Per avermi 'obbligato' ad iscrivermi all'Università!
Per aver creduto che ce l'avrei fatta quando non lo pensavo neanch'io!! Per avermi sempre spronato e spinto a studiare.
Perchè anche se sono un'amica 'disgraziata' mi vuole bene lo stesso!!
Annina, Paola, Ali, Eri, perchè sono le mie amiche adorate!! Per avermi sempre incitato e invogliato a finire, nelle nostre meravigliose seratine.
Ale!! Il mio 'Coach'!! Senza di lei non ce l'avrei fatta!! La ringrazio per essermi stata accanto, soprattutto in questo periodo, per avermi spronato a fare in fretta, per avermi convinto che stavo finendo anch'io!! Per tutti i suoi consigli, per essermi stata vicina nei momenti più importanti e per avermi accompagnato ovunque. Nonchè per i nostri 'Spritz' di festeggiamento.
Katia, perchè è una delle prime ragazze che ho conosciuto in facoltà. Per la sua sincerità e il suo entusiasmo e per tutti gli appunti che mi ha recuperato!!
Ringrazio tutti per aver creduto in me e perchè questo giorno è finalmente arrivato!