Università degli Studi di Bologna, Alma Mater Studiorum

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

Tesi di laurea triennale

Note sul ruolo dell'infinito in matematica

dalla filosofia classica ai frattali e alla crittografia

Candidato:
Sara Chiappelli
Matricola 0000621781

Relatore:
Alessandro Gimigliano

Correlatore:
Davide Aliffi

Anno Accademico 2013-2014

A chi ha sempre creduto in me
ieri, oggi, domani.

Indice

Elenco delle figure

Elenco delle tabelle

Notazioni

Queste sono le principali notazioni utilizzate:

t.c. ..... tale che
$\mathbb{N}$ ..... numeri naturali
$\mathbb{Z}$ ..... numeri interi
$\mathbb{Q}$ ..... numeri razionali
$\mathbb{R}$ ..... numeri reali
$\aleph_0$ ..... cardinalità del numerabile
$\aleph_1$ ..... (cardinalità del continuo)
$p_x(y(x))$ ..... probabilità si $y(x)$ rispetto alla variabile x

Introduzione

Uno dei concetti più affascinanti della matematica, e non solo, è quello di infinito; questo argomento non è proprio solo della matematica, ma è di fondamentale importanza anche in molti altri campi di studio, anche non scientifici, basti pensare alla filosofia.
Il concetto di infinito iniziò ad essere usato dagli antichi greci, seppur con diffidenza; ad oggi, tutte le applicazioni scientifiche moderne non possono farne a meno.
Il mio elaborato nasce con un duplice intento; quello di affascinare, anche chi non si occupa di matematica, con questo concetto così pieno di diversi significati; e con l'intento di mostrare alcune applicazioni moderne e non del tutto banali, dell'infinito a campi matematici molto diversi tra loro, quali l'analisi (dalle serie ai frattali) e la crittografia.
Questo progetto ha come scopo principale la realizzazione di un sito all'interno di quello del "progettomatematic@" del dipartimento di matematica di Bologna; dedicato appunto all'infinito con tre principali soggetti: l'infinito e la sua storia, l'infinito e i frattali, l'infinito in crittografia.

Capitolo 1

L'infinito e la sua storia

E' risaputo che la visione greca del mondo fosse basata su concetti come l'armonia, la proporzione, l'equilibrio, la perfezione, la determinatezza e la razionalità; questa visione rende quindi particolarmente problematici l'accettazione e l'utilizzo del concetto di infinito. La parola greca per infinito, apeiron ($\alpha\pi\epsilon\iota\rho o\nu$), e cioè, letteralmente, senza limite, ha un costrutto tipicamente negativo (la lettera iniziale a- nega ciò che segue), con un senso di senza forma, senza definizione. Per trattare questo concetto i greci hanno preferito adottarne due diverse concezioni: quella "potenziale" e quella "attuale".
Questa distinzione si deve in primo luogo ad Aristotele: l'infinito attuale è qualcosa di completo e compiuto, costituito da infiniti elementi, in contrapposizione all'infinito potenziale che è qualcosa di non completo a cui possono essere sempre aggiunti elementi ma in numero finito. Si avrà poi un rifiuto del concetto di infinito attuale, mentre una accettazione del concetto di infinito potenziale come processo di ecceterazione (cioè come possibilità di "andare sempre oltre", ma facendo passi "finiti"). Facciamo un esempio; l'insieme dei numeri naturali era considerato un infinito potenziale, infatti fissato qualsiasi numero naturale ne posso sempre trovare uno maggiore di esso (basta aggiungere 1) ma non posso coglierne il senso in toto, cioè non posso parlarne come di un infinito attuale. Queste concezioni di infinito furono concepite anche per superare le difficoltà poste da alcuni ben noti problemi, che non tardarono ad emergere e che ora esamineremo; tratteremo del problema dei segmenti incommensurabili, scoperti dai Pitagorici, dei paradossi di Zenone e del problema della rettificazione della circonferenza.

1.1 Segmenti incommensurabili

Definizione 1.1 (grandezze commensurabili)**.**
Date due grandezze omogenee, queste si dicono commensurabili se esiste una grandezza omogenea alle prime due e tale che è contenuta un numero intero di volte in entrambe.

Per Pitagora tutto era costituito da corpuscoli uguali tra loro e anche i punti, seppur piccoli, avevano una loro dimensione; ne discendeva allora che i segmenti erano costituiti da un numero finito di punti e che quindi ogni coppia di segmenti dovesse essere tra loro commensurabile, con, come grandezza contenuta in entrambi, il punto.
Purtroppo però, una applicazione del teorema di Pitagora ad un triangolo rettangolo iscoscele mostrerà l'incommensurabilità tra diagonale e lato di un quadrato. Prima di dimostrare il teorema enunciamo e proviamo un lemma:

Teorema 1.1.1. *Siano $m, n \in N$ allora è impossibile che $(\frac{m}{n})^2 = 2$.*

Dimostrazione. Supponiamo per assurdo che $\exists\ m, n \in \mathbb{N}$ t.c. $(\frac{m}{n})^2 = 2$, riduciamo poi la frazione ai minimi termini ed otterremo $\exists\ p, q \in \mathbb{N}$ t.c. $(\frac{p}{q})^2 = 2$, con
MCD(p, q)=1; ne verrà quindi che $p^2 = 2q^2$ e quindi che p^2 è pari e anche p è pari, cioè $\exists\ p' \in \mathbb{Z}$ t.c. $p = 2p'$. Ma allora $(2p')^2 = 2q^2$ cioè $q^2 = 2p'^2$ e anche q è pari, ma questo è un assurdo poichè avevamo assunto MCD(p, q)=1, cosicchè questo conclude la prova del teorema. □

Teorema 1.1.2 (Teorema di incommensurabilità)**.** *Lato e diagonale di un quadrato sono segmenti incommensurabili.*

Dimostrazione. Siano rispettivamente l, d lato e diagonale del quadrato; supponiamo per assurdo che essi siano commensurabili, cioè supponiamo che
$\exists\ s, m, n \in \mathbb{N}$ *t.c.* $\frac{l}{d} = \frac{sm}{sn} = \frac{m}{n}$; ma ora, per il teorema di Pitagora: $d^2 = 2l^2$ cioè $\frac{d^2}{l^2} = 2$ cioè $\frac{n^2}{m^2} = 2$ ma questo è assurdo per il teorema di cui sopra, quindi l e d sono incommensurabili. □

Questi teoremi, che oggi potremmo considerare come prova della necessità dell'introduzione dei numeri irrazionali, crearono non pochi problemi al concetto di infinito per i greci; infatti provando "geometricamente e manualmente" a riportare sulla diagonale il lato si otteneva un rapporto fra grandezze che poteva essere infinitamente approssimato, non era *attuale*.

1.2 Paradossi di Zenone

Ci occuperemo di due tra i più famosi paradossi di Zenone: tra quelli sul moto, discuteremo il paradosso di Achille e la tartaruga e quello della dicotomia.

1.2.1 Achille e la tartaruga

Possiamo enunciare il paradosso come segue:
"In una corsa, il corridore più veloce non potrà mai superare quello più lento a cui avrà dato un certo vantaggio"
ovviamente nel nostro caso si parla del corridore più veloce che è Achille e di quello più lento che è la tartaruga.

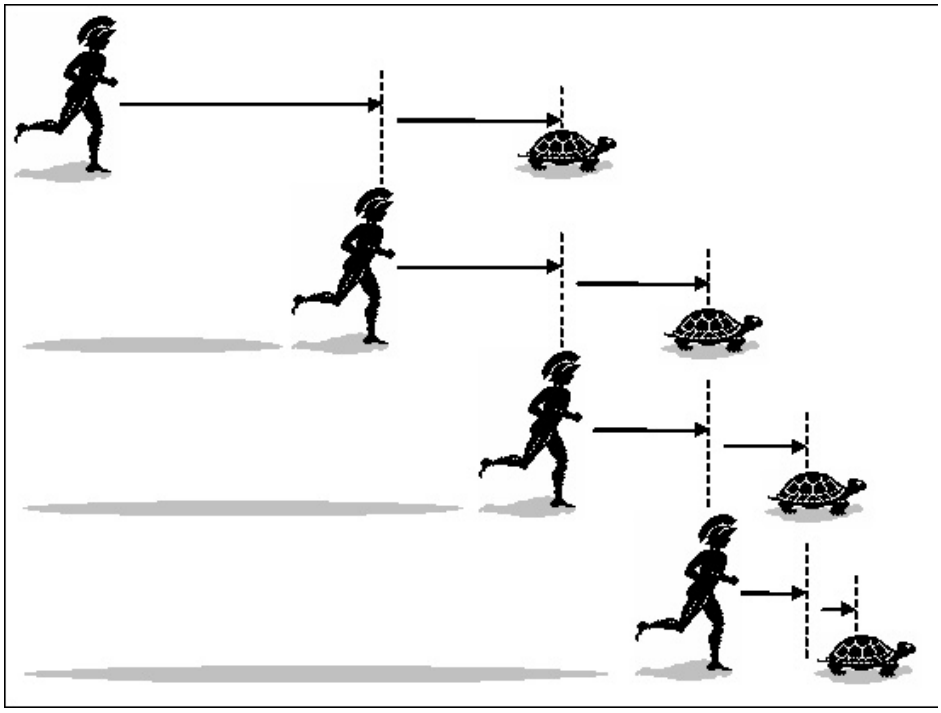

Figura 1.1: Achille e la tartaruga

Ragionando un po' come Zenone e ricordando che nell'antica Grecia si pensava che la somma di infinite grandezze non nulle fosse infinita, potremmo descrivere il paradosso in questi termini: Achille dovrà percorrere in un certo tempo lo spazio che lo separa dalla tartaruga ma questa, nello stesso tempo, avrà percorso uno spazio, seppur piccolo; di nuovo Achille in un tempo successivo percorrerà questo spazio ma, nel frattempo, la tartaruga si sarà

spostata ancora leggermente più avanti e così, iterando il procedimento, ne sorge il paradosso dato dal fatto che Achille dovrebbe percorrere infiniti intervalli non nulli per raggiungere la tartaruga. Diamo una dimostrazione "matematica" che ci permetterà di confutare questo paradosso.

Dimostrazione. indichiamo rispettivamente con i pedici A e T le grandezze riferite ad Achille e alla tartaruga, con L_i la lunghezza del tratto i-esimo percorso dalla tartaruga e con t_i i tempi i-esimi impiegati da Achille per percorrere questi tratti; supponiamo $v_A > v_T$, ora:

$$t_0 = \frac{L_0}{v_A}$$

in tale tempo la tartaruga percorrerà uno spazio

$$L_1 = t_0 v_T = \frac{L_0}{v_A} v_T$$

e Achille percorrerà questa distanza in un tempo pari a

$$t_1 = \frac{L_1}{v_A} = \frac{L_0}{v_A}\frac{v_T}{v_A}$$

Quindi iterando il procedimento, al passo n-esimo avrò che:

$$L_n = L_0(\frac{v_T}{v_A})^n \qquad\qquad t_n = \frac{L_0}{v_A}(\frac{v_T}{v_A})^n.$$

Considerando allora le rispettive serie e passando al limite, avrò che:

$$L = \sum_{k=0}^{\infty} L_k = \sum_{k=0}^{\infty} L_0(\frac{v_T}{v_A})^k = L_0 \sum_{k=0}^{\infty}(\frac{v_T}{v_A})^k$$

poichè abbiamo una serie geometrica di ragione < 1 per ipotesi, avremo che è essa convergente e vale:

$$L = L_0 \frac{1}{1 - (\frac{v_T}{v_A})} = L_0 \frac{v_A}{v_A - v_T}.$$

Infine

$$T = \sum_{k=0}^{\infty} t_k = \sum_{k=0}^{\infty} \frac{L_0}{v_A}(\frac{v_T}{v_A})^k = \frac{L_0}{v_A - v_T}.$$

per gli stessi ragionamenti fatti sopra. Ma allora il tempo T impiegato da Achille per raggiungere la tartaruga è un tempo finito, cioè questa dimostrazione che utilizza le serie, "smonta" il paradosso di Achille e la tartaruga.
□

1.2.2 Paradosso della dicotomia

Questo paradosso, noto anche come paradosso dello stadio, ci permette di avvicinarci sempre di più al concetto di serie; esso afferma che:
"non si può giungere all'estremità di uno stadio senza prima averne raggiunto la metà, ma poi si dovrà raggiungere la metà della metà rimanente e così via senza quindi mai riuscire ad arrivare alla fine"
Confutare questo paradosso è molto più facile che nel caso precedente, infatti consideriamo la seguente immagine:

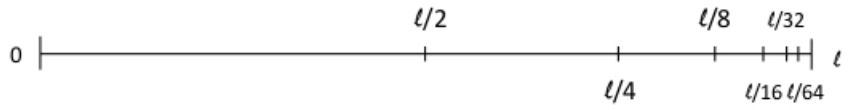

Figura 1.2: Il paradosso della dicotomia

essa mostra come il percorso totale che il nostro atleta dovrà compiere può essere espresso come

$$\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ... = \sum_{k=1}^{\infty} \frac{1}{2^k}.$$

Questa è una serie geometrica di ragione $\frac{1}{2}$ che, come vedremo in seguito,converge a $\frac{1}{1-\frac{1}{2}}$-1=1; questo spiega perchè il nostro atleta arriverà tranquillamente alla fine dello stadio.
Vediamo quindi che il "semplice" concetto di *serie geometrica convergente* smonta completamente la vecchia concezione che la somma di infiniti numeri non nulli sia necessariamente infinita.

1.3 Rettificazione del cerchio

Questo problema classico in geometria consiste nel voler calcolare l'area del cerchio. La prima risoluzione del tutto corretta e rigorosamente dimostrata è quella basata sul metodo di esaustione (concetto non molto lontano da quello intuitivo di integrale di Riemann, visto come area sottesa al grafico di una funzione) ovvero:

Il metodo di esaustione permette di calcolare aree di certe figure geometriche approssimandole con una successione di poligoni che convergono alla figura data; in termini moderni diremmo che l'area cercata è il limite delle aree dei poligoni per n (=numero di lati)$\to \infty$.

Questo concetto anche basato sul fondamentale lemma di Eudosso, che sarà utilizzato nel calcolo della misura della circonferenza, e in molte altre applicazioni (ad esempio da Archimede).

Teorema 1.3.1 (Lemma di Eudosso)**.** *Date due grandezze (non nulle) in un certo rapporto, allora è sempre possibile trovare un multiplo di una che superi l'altra.*

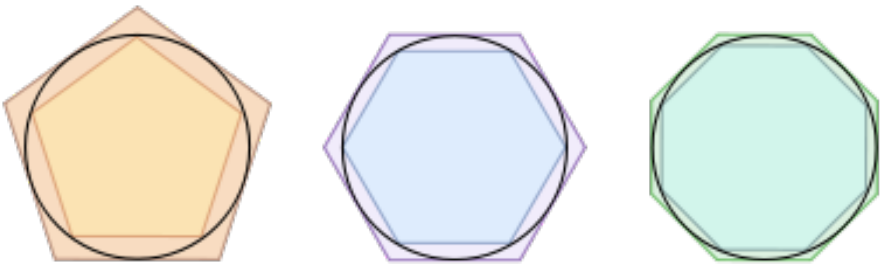

Figura 1.3: Il metodo di esaustione

Ovviamente l'idea di inscrivere/circoscrivere nella circonferenza poligoni ed aumentarne sempre più il numero di lati era già presente da tempo, ma ci si chiedeva se, alla fine, sarebbe stato possibile identificare i lati infinitesimi di un "ultimo poligono" con archi di circonferenza. Aristotele non era di questo avviso, infatti, sfruttando il suo concetto di infinito potenziale, sosteneva che dato un poligono con n lati era sempre possibile trovarne uno con $n+1$ lati che meglio avrebbe approssimato la circonferenza; la soluzione di questo problema si trova nell'uso del metodo di esaustione (attribuito ad Eudosso ed usato sia da Euclide che da Archimede), con il quale si potranno formulare

importanti teoremi per il calcolo delle aree e dei volumi di molte figure. Qui vedremo come si può calcolare l'area del cerchio senza prendere in causa il concetto di infinito, e come approssimando la misura della circonferenza, che vale $2\pi r$, si può trovare un'approssimazione di π.

Teorema 1.3.2. *L'area del cerchio (A) è uguale all'area del triangolo avente per base la circonferenza e per altezza il raggio.*

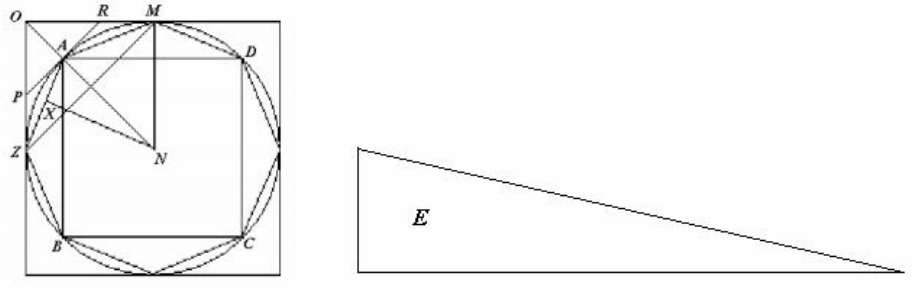

Figura 1.4: Costruzione del poligono inscritto

Dimostrazione. Supponiamo per assurdo che i due non siano equivalenti, allora o il cerchio ha area maggiore rispetto al triangolo, o minore.
(1) Supponiamo per assurdo che il cerchio abbia area minore del triangolo; supponiamo cioè che $\exists\ k > 0$ t.c. $A = \frac{r \cdot C}{2} - k$; inscriviamo poi nel cerchio un poligono regolare t.c. il suo apotema a sia: $a > r - \frac{k}{C}$ e il suo perimetro p sia: $p > C - \frac{k}{r}$.
Questo lo posso sempre fare poichè basta considerare un poligono con un numero alto di lati affinchè a sia vicino a r e p sia vicino a C.
Quindi l'area A' del poligono è $A' = \frac{p \cdot a}{2}$ ma allora:

$$A' = \frac{p \cdot a}{2} > \frac{1}{2}(r - \frac{k}{C})(C - \frac{k}{r}) = \frac{1}{2}(r \cdot C - 2k + \frac{k^2}{C \cdot r}) = \frac{r \cdot C}{2} - k + \frac{k^2}{2C \cdot r} > \frac{r \cdot C}{2} - k$$

di conseguenza:

$$A > A' > \frac{r \cdot C}{2} - k.$$

Ma questo è un assurdo poichè avevamo supposto che $A = \frac{r \cdot C}{2} - k$, ne verrà che l'area del cerchio non può avere area minore del triangolo.
(2) Analogamente, per la disuguaglianza inversa, si procede supponendo PA che il cerchio abbia area maggiore, e considerando poligoni circoscritti.
Ma allora, questo prova che area del cerchio e area del triangolo costruito

come da ipotesi sono uguali. Nella raccolta dei lavori di Archimede, dopo questa proposizione si trova la prima approssimazione che Archimede ha dato del numero π e cioè:

$$3 + \frac{10}{71} < \pi < 3 + \frac{1}{7};$$

questa approssimazione è stata data grazie alla proposizione seguente:

Proposizione 1.3.3. *Se un angolo di un triangolo è diviso dalla bisettrice congiungente il lato opposto, allora i segmenti di questo lato sono nello stesso rapporto con i restanti lati del triangolo; e, se i segmenti della base sono nello stesso rapporto con i restanti lati del triangolo, allora la linea retta che congiunge il vertice al punto di separazione sarà la bisettrice dell'angolo del triangolo.*

Nonostante questo valore sia molto preciso, Archimede non aveva i mezzi per dimostrare che π non si può scrivere come frazione; successivamente è stato provato che π è un numero irrazionale (la dimostrazione di ciò è del 1761) e per di più trascendente (dimostrato nel 1882).
Quindi riassumendo possiamo dire che il concetto di infinito dei greci fu ben presto messo in discussione soprattutto dal fatto che la somma di infiniti numeri potesse non essere infinita; è proprio su questo ultimo argomento che si basa il concetto di serie.

1.4 Serie numeriche

Definizione 1.2 (serie numerica)**.**
Sia $(a_k)_{k\in\mathbb{N}}$ una successione in $\mathbb{C}$; si chiama serie numerica di termine k-esimo a_k la successione:

$$(\sum_{k=1}^{n} a_k)_{n\in\mathbb{N}}.$$

Definiamo inoltre le somme parziali della serie:

$$S_n = \sum_{k=1}^{n} a_k$$

e diciamo che la serie è convergente, divergente o oscillante a seconda che lo sia il $\lim_{n\to\infty} S_n$.

Diamo ora una spiegazione matematica, in termini di convergenza di serie, al perchè il paradosso dello stadio non è più un paradosso.

Proposizione 1.4.1. *Sia $z \in \mathbb{C}$, si dice serie geometrica di ragione z, la serie:*

$$S_n = \sum_{k=0}^{n} z^k;$$

questa converge $\Longleftrightarrow |\, z \,| < 1$ ed in tal caso

$$\sum_{k=0}^{\infty} z^k = \frac{1}{1-z}.$$

Dimostrazione. Scriviamo la somma parziale della nostra serie:

$S_n = \sum_{k=0}^{n} z^k = 1 + z + ... + z^n$ e analizziamo i vari casi al variare di z:
- $z \neq 1$:

$$S_n = (1+z+...+z^n)(1-z)\frac{1}{1-z} = \frac{1 + z + ... + z^n - z - ... - z^{n+1}}{1-z} = \frac{1-z^{n+1}}{1-z}$$

- $z = 1$:

$$S_n = n + 1.$$

Quindi per z=1 se considero il $\lim_{n\to\infty} S_n$=∞ e cioè la serie diverge per z=1. Per $z \neq 1$ invece S_n è convergente $\Leftrightarrow \exists \lim_{n\to\infty} z^{n+1} = \lim_{n\to\infty} z^n < \infty$; distinguiamo quindi 3 casi al variare di $|z|$:
1) $|z| < 1$: $|z^n| = |z|^n \to 0$ per $n \to \infty$ e quindi $\exists \lim_{n\to\infty} S_n = \frac{1}{1-z}$
2) $|z| > 1$: $|z^n| = |z|^n \to \infty$ per $n \to \infty$ e quindi la serie diverge.
3) $|z| = 1$ e $z \neq 1$: supponiamo per assurdo che $\exists \lim_{n\to\infty} z^n = \alpha$ ma allora

$$\alpha = \lim_{n\to\infty} z^{n+1} = z \lim_{n\to\infty} z^n = z\alpha;$$

cioè

$$\alpha = z\alpha.$$

Quindi le ipotesi sono 2: o z=1 e questo è assurdo per ipotesi oppure $\alpha = 0$, ma se $\alpha = 0$ ne viene che:

$$0 = |\alpha| = \lim_{n\to\infty} |z^n| = \lim_{n\to\infty} |z|^n = 1$$

per quanto visto all'inizio, e questo è assurdo.
Quindi in questo caso la serie non converge. □

Definizione 1.3 (Serie telescopica)**.**
Una serie si dice serie telescopica se è della forma:

$$S_n = \sum_{k=0}^{\infty}(b_n - b_{n+1}).$$

Proposizione 1.4.2. *Una serie telescopica*

$$S_n = \sum_{n=0}^{\infty}(b_n - b_{n+1})$$

è convergente $\Leftrightarrow \exists \lim_{n\to\infty} b_n = \beta$ *ed in tal caso:*

$$\sum_{n=0}^{\infty}(b_n - b_{n+1}) = b_0 - \beta.$$

Dimostrazione. La dimostrazione è immediata scrivendo per esteso S_n, infatti $S_n = b_0 - b_1 + b_1 - b_2 + ... + b_{n-1} - b_n + b_n - b_{n+1} = b_0 - b_{n+1}$ e quindi la serie converge $\Leftrightarrow \exists \lim_{n\to\infty} b_n = \beta$ ed in tal caso abbiamo provato anche la formula data nell'enunciato. □

Analizziamo più attentamente la serie di Grandi:

$$S_n = \sum_{k=0}^{\infty}(-1)^n;$$

abbiamo già visto che non converge (nel senso di cui sopra, mentre si ha convergenza secondo Cesaro a $\frac{1}{2}$) ma facciamo vedere come questa serie sia stata, nel corso dei secoli, oggetto di grandi discussioni.
1) si potrebbe pensare di procedere in questo modo:

$$S_n = 1 - 1 + 1 - 1 + 1 - 1 + ... = 1 - (1 - 1 + 1 - 1 + ...) = 1 - S_n$$

e ne verrebbe che S_n=$\frac{1}{2}$
2) alternativamente potremmo pensare: S_n=(1-1)+(1-1)+...=0
3) o ancora: S_n=1+(-1+1)+(-1+1)+...=1
Questi esempi sono molto importanti perchè mostrano come per le serie non valgano le classiche proprietà (come l'associatività e la commutatività della addizione) che valgono per le somme finite.
Proprio su questa serie è basato il paradosso della lampada di Thomson:
"si consideri una lampada accesa con un tasto di accensione e si consideri il seguente procedimento: dopo un minuto si spenga la lampada, dopo mezzo minuto la si accenda di nuovo e si ripeta il procedimento dimezzando sempre

i tempi. Dopo due minuti la lampada sarà accesa o spenta ? "
Possiamo interpretare questo paradosso tramite la serie di Grandi

$$S_n = \sum_{k=0}^{\infty} (-1)^n;$$

e cioè se ne può dedurre che in realtà questo paradosso non ha una risposta perchè la nostra serie è oscillante e quindi nulla si può dire sul risultato.
Fino ad ora abbiamo quindi smontato l'idea dell'infinito greca in 3 modi differenti; abbiamo fatto vedere che somma di infiniti numeri può benissimo dare infinito ma può anche dare un numero finito oppure può non essere determinata (si veda la proposizione di cui sopra); quindi l'idea di una distinzione netta tra infinito in potenza e in atto sembra non essere più molto sicura. Vediamo come si svilupperà il concetto di infinito in anni succcessivi.

1.5 Galileo e l'infinito

Fra i primi a superare l'avversione per l'infinito attuale ci fu Galilei; questi afferma che un qualsiasi oggetto limitato può essere ridotto in infiniti elementi che però non hanno estensione e sono indivisibili; infatti se queste infinite parti avessero estensione finita e quindi fossero divisibili non si spiegherebbe la limitatezza del segmento.
"Io non veggo che ad altra decisione si possa venire, che a dire, infiniti essere tutti i numeri, infiniti i quadrati, infinite le loro radici, né la moltitudine de' quadrati esser minore di quella di tutti i numeri, né questa maggior di quella, ed in ultima conclusione, gli attributi di eguale maggiore e minore non aver luogo ne gli infiniti, ma solo nelle quantità terminate."
Galileo, con il paradosso dei quadrati, ha mostrato come non si possa parlare di infinito nel modo in cui si parla comunemente degli altri numeri ma come tuttavia, dati due insiemi infiniti, si possano confrontare e stabilire o meno se hanno "lo stesso numero di elementi" creando una biezione fra un insieme e l'altro.
Paradosso di Galileo: dato $\mathbb{N}$ l'insieme dei numeri naturali e Q l'insieme dei quadrati perfetti, allora $Q \subset \mathbb{N}$ ma si può stabilire una corrispondenza biunivoca tra questi due insiemi associando ad ogni numero naturale il suo quadrato; quindi un insieme può essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.
Questa affermazione potenzialmente problematica, diventerà la definizione moderna di insieme di cardinalità infinita e questo paradosso, noto come paradosso dei quadrati, non sarà altro che una prima versione del paradosso

dell'albergo di Hilbert.

1.6 Infiniti e Infinitesimi del calcolo differenziale

Il concetto di infinito potenziale tornò ad assumere un ruolo principale nel calcolo differenziale di Newton e Leibniz; questi, utilizzando una scrittura particolare per distinguere infiniti e infinitesimi (o flussioni come li chiamava Newton) (il simbolo ∞ per l'infinito (potenziale) ed il simbolo dt per l'infinitesimo), daranno il via ad un ramo della matematica, che è, ad oggi, uno dei più famosi: il calcolo infinitesimale dell'analisi matematica.
Oggi questi due matematici sono ritenuti i padri di questa disciplina, ma, ai loro tempi, questi non erano molto ben disposti a dividersi il merito; infatti sono passate alla storia numerose dispute tra i due riguardo a chi per primo avesse davvero scoperto il calcolo infinitesimale; attualmente si preferisce nominarli assieme, poichè hanno entrambi ottenuto risultati sorprendenti seppur lavorando separatamente.
Questa disputa nasce dal fatto che l'atto di nascita del calcolo infinitesimale è considerato il lavoro di Leibniz: "Nuovo metodo per trovare i massimi e minimi, e anche le tangenti, non ostacolato da quantità frazionarie e irrazionali e un unico genere di calcolo per quei problemi" pubblicato nel 1684 negli Acta Eruditorum; Newton però aveva raggiunto simili risultati già dal 1669, nonostante li avesse pubblicati col nome di "De Analysi per Aequationes Numero Terminorum Infinitas" solo successivamente all'opera di Leibniz nel 1711.
Dopo le scoperte di Cavalieri, Cartesio, Fermat, negli anni a cavallo tra il 1700 Newton e Leibniz formalizzarono questi concetti: a Newton si deve soprattutto l'aver introdotto: regola della catena, serie di Taylor e funzioni analitiche applicate a fondamentali problemi della fisica, mentre si devono a Leibniz la gran parte delle nozioni usate ad oggi nel calcolo infinitesimale.
Quando vennero pubblicati, questi risultati non accolsero il favore della critica, si contestava infatti la certezza dei presupposti su cui questi risultati si basavano: solo successivamente grazie ad una revisione dei risultati fatta da Cauchy, e grazie ai contributi dati da matematici come d'Alembert, Poisson, Liouville, Fourier e infine Riemann, il calcolo infinitesimale, che già era divenuto una parte fondamentale della matematica, acquistò delle besi rigorose, liberandosi di criteri non ben definiti come le "quantità infinitesime", e basandosi soprattutto sulla nozione di limite. Questa fa un uso solo potenziale

dell'infinito: dire che $lim_{x\to a} f(x) = \infty$ significa solo che il valore di $f(x)$ supera qualsiasi quantità fissata M purchè si prenda x abbastanza vicino ad a.
Il calcolo infinitesimale fu importante non solo per la matematica; infatti molti rami della scienza e della tecnologia usano quanto appena descritto come strumento fondamentale nelle loro "descrizioni del mondo".
Analizziamo ora più approfonditamente alcuni dei problemi principali che furono studiati e/o risolti grazie a questi nuovi strumenti, mostrando le maggiori scoperte effettuate dai due protagonisti di questa sezione.
In questo secolo, il legame tra matematica e scienza era molto stretto; infatti i principali quesiti irrisolti riguardavano argomenti di tipo "geometrico" che presentavano applicazioni pratiche: l'identificazione tra curve ed equazioni e quindi trovare la tangente ad una curva e risolvere problemi di massimo e minimo.

Newton Newton, iniziò a considerare quale relazione ci fosse fra l'equazione di una curva e l'area ad essa sottostante; supponendo di avere una curva di area data da $z = \alpha x^m$ e sfruttando il concetto di incremento infinitesimo, arrivò a ricavare l'equazione della curva $y = m\alpha x^{m-1}$, sfruttando il teorema del binomio da lui dimostrato in precedenza:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Si deve quindi a Newton, non tanto l'aver scoperto la formula di derivazione dei polinomi, che era già nota, ma l'aver dato una prima formulazione del teorema fondamentale del calcolo integrale.
In questa dimostrazione Newton fa uso del concetto di incrementi infinitesimi e li fa "svanire" per ottenere il rapporto finale; questa non è altro che una formulazione non rigorosa dell'idea di limite di una funzione.
Newton quindi non considera più le grandezze come quantità statiche ma come quantità variabili chiamate *fluenti* e la loro variazione *flussione*.

Leibniz Il ruolo di Leibniz è fondamentale nell'aver introdotto una nuova operazione, la differenziazione, che opera soprattutto su differenze infinitesime di variabili che verrano nominate dx, come incremento rispetto alla variabile x. In questi procedimenti alcuni triangoli importanti in matematica (come il triangolo caratteristico) furono fondamentali; infatti Leibniz capì l'importanza dei rapporti e definì, al contrario di quanto si fa oggi, il differenziale mediante il concetto di tangente.

Formulò molte delle principali regole di derivazione (anche se senza una spiegazione rigorosa della cancellazione degli infinitesimi) e diede un'altra formulazione del teorema fondamentale del calcolo integrale, introducendo l'attuale scrittura degli integrali e cioè:

$$\int y\,dx.$$

Grazie a queste scoperte vennero risolti la maggior parte dei problemi di tangente e massimo e minimo, che allora riguardavano anche funzioni piuttosto semplici (combinazioni di potenze). Si dovette aspettare l'800 per avere una base rigorosa su cui poter affrontare questi argomenti; il merito fu principalmente di Cauchy (ed anche di Weierstrass), che introdusse il concetto di limite (quello in uso ad oggi) con le notazione di ε e δ; Cauchy soprattutto riconfermò l'uso dell'infinito potenziale, in un campo così importante della matematica.
L'unico, o comunque, uno dei più importanti problemi non ancora risolto era quello di dare una definizione rigorosa dei numeri reali; fino ad allora infatti i numeri reali erano stati usati in modo piuttosto libero, cioè senza preoccuparsi di darne una vera definizione rigorosa; sarà proprio questo il punto di partenza per lo studio dei problemi legati all'infinito moderno.

1.7 L'infinito moderno

Si deve a Dedekind l'aver risolto due dei maggiori problemi incontrati fino ad allora lavorando con l'infinito potenziale i numeri irrazionali e il continuo.

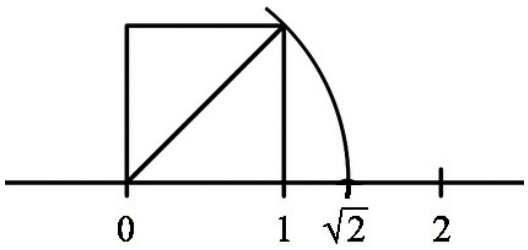

Figura 1.5: Costruzione della diagonale di un quadrato e sua proiezione sulla retta

Secondo Newton e Leibniz, la continuità dei punti di una retta era dovuta alla loro densità (cioè al fatto che tra due punti se ne potesse trovare sempre

un altro); ma questa proprietà valeva anche per i numeri razionali che però, non formavano un continuo, (basta vedere il punto $\sqrt{2}$ della figura 1.5, che sicuramente non appartiene a $\mathbb{Q}$). Dedekind si inventò così una nuova definizione; quella di *sezione* dell'insieme $\mathbb{Q}$ e tramite questo concetto diede una definizione dei numeri reali (compresi quelli che definirà irrazionali).
In generale una sezione di Dedekind di un insieme totalmente ordinato $(X, <)$ è una partizione di questo in due insiemi non vuoti A, B con A t.c.

$$b \in A \Rightarrow \forall a \in X(a < b \Rightarrow a \in A),\ A\ taglio\ iniziale,$$

senza massimo e B t.c.

$$b \in B \Rightarrow \forall a \in X(b < a \Rightarrow a \in B),\ B\ taglio\ finale;$$

se il più piccolo elemento di B è un razionale, allora questo corrisponderà al taglio, altrimenti, se B non ha minimo, il taglio sarà proprio un numero irrazionale (l'unico che "riempie" il gap tra A e B).
Quindi ogni taglio irrazionale corrisponde ad un numero irrazionale che non sta né in A né in B, che è minore di tutti gli elementi razionali di B e maggiore di tutti gli elementi razionali di A; quindi preso un segmento c'è uno ed un solo punto che determina una divisione come sopra, questo punto sarà univocamente determinato dalla coppia (A, B) e, ogni volta che in tale coppia B non ha minimo, questo punto verrà detto irrazionale.
Questa nozione è quella che definisce anche la continuità, senza più dover far ricorso al concetto di densità.

Torniamo all'infinito attuale; la definizione di infinito che si usa oggi e molti dei concetti legati ad esso si devono in larga misura a Cantor.

Definizione 1.4. Dati due insiemi M, N si dice che questi sono *equipotenti* (o che hanno la stessa cardinalità) se e solo se posso mettere in corrispondenza M, N in modo tale che ad ogni elemento di un insieme ne corrisponda uno ed uno soltanto dell'altro(corrispondenza biunivoca).

Cantor per primo, applicò questo concetto di cardinalità anche a insiemi infiniti; infatti fino ad allora, forse come retaggio della mentalità greca, si pensava che contare o confrontare non potesse essere fatto quando si trattava di infinito, e che in tal caso questo avrebbe portato a dei paradossi (si pensi a come conclude il suo discorso Galilei).
A Cantor si devono soprattutto due intuizioni che hanno la loro base nella scoperta che nell'infinito si possono fare distinzioni: la prima è che ci sono insiemi infiniti che sono equipotenti ad un loro sottoinsieme proprio, mentre

la seconda è che non tutti gli insiemi infiniti possono essere messi in corrispondenza biunivoca tra di loro.
Da queste idee nascerà la definizione di infinito data da Dedekind, rovesciando completamente il modo di vedere l'infinito; si passa dall'infinito come negazione del finito, al finito come "non infinito":

Definizione 1.5 (insieme infinito)**.**
Un insieme è infinito quando lo si può mettere in corrispondenza biunivoca (cioè se è equipotente) con un suo sottoinsieme proprio; viceversa l'insieme si dirà finito.

Ricordiamo che un insieme si dice numerabile se è equipotente ad $\mathbb{N}$ e mostriamo due tra i teoremi più famosi di Cantor: $\mathbb{Z}, \mathbb{Q}$ sono numerabili mentre $\mathbb{R}$ non lo è; per fare questo faremo uso dell'altrettanto famoso argomento diagonale di Cantor.

Teorema 1.7.1. *L'insieme dei numeri interi è numerabile.*

Dimostrazione. Per provare il teorema basta mettere in corrispondenza biunivoca l'insieme dei numeri interi con quello dei numeri naturali; si può considerare una funzione che associa ai numeri naturali pari, gli interi positivi ed ai numeri naturali dispari, gli interi negativi; nel modo seguente:

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ pari} \\ \frac{-n-1}{2} & \text{se } n \text{ dispari} \end{cases}$$

Questa funzione è ovviamente iniettiva e suriettiva e quindi dà la corrispondenza cercata e cioè prova il teorema. □

Molto più interessante è invece il procedimento inventato da Cantor per dimostrare che anche i numeri razionali sono numerabili;

Teorema 1.7.2. *L'insieme dei numeri razionali è numerabile.*

Dimostrazione. Possiamo identificare $\mathbb{Q}^+$ con un quoziente di $\mathbb{N} \times \mathbb{N}$ considerando la frazione $\frac{a}{b}$ come la coppia (a, b), e mettiamo tutti gli elementi nella tabella di Figura 1.6.
Ordiniamo poi gli elementi partendo da (0,0) e seguendo le diagonali secondarie, ottenendo la successione: $(0,0), (1,0), (0,1), (2,0), (1,1), ..., (i,0), (i-1,1), (i-2,2), ..., (1,i-1), (0,i), ...$
Poichè posso contare gli elementi di $\mathbb{N} \times \mathbb{N}$ come: 0,1,2,3... avrò una corrispondenza biunivoca tra i due insiemi come segue:

$$\mathbb{N} \times \mathbb{N} \ni (a,b) \mapsto (\frac{1}{2}(a+b)(a+b+1)) + b \in \mathbb{N};$$

(0,0) (0,1) (0,2) (0,3) (0,4) (0,5) (0,6) (0,7) ...

(1,0) (1,1) (1,2) (1,3) (1,4) (1,5) (1,6) (1,7) ...

(2,0) (2,1) (2,2) (2,3) (2,4) (2,5) (2,6) (2,7) ...

(3,0) (3,1) (3,2) (3,3) (3,4) (3,5) (3,6) (3,7) ...

(4,0) (4,1) (4,2) (4,3) (4,4) (4,5) (4,6) (4,7) ...

(5,0) (5,1) (5,2) (5,3) (5,4) (5,5) (5,6) (5,7) ...

...

Figura 1.6: Tabella dei numeri razionali

Questa è infatti la corrispondenza biunivoca cercata in cui il numero naturale indica la posizione occupata dalla coppia (a, b). □

Teorema 1.7.3. *L'insieme dei numeri naturali non si può mettere in corrispondenza biunivoca con i numeri reali dell'intervallo* A=$[0, 1]$.

Dimostrazione. Supponiamo per assurdo che esista una corrispondenza biunivoca tra $\mathbb{N}$ ed A, allora dovrei poter contare ogni elemento di A; costruiamo quindi la seguente tabella:

$$\begin{array}{lccccccc}
\mathsf{A}1 = & 0. & [a_{11}] & a_{12} & a_{13} & \cdots & a_{1n} & \cdots \\
\mathsf{A}2 = & 0. & a_{21} & [a_{22}] & a_{23} & \cdots & a_{2n} & \cdots \\
\mathsf{A}3 = & 0. & a_{31} & a_{32} & [a_{33}] & \cdots & a_{3n} & \cdots \\
\vdots & & & & & \ddots & \vdots & \\
\mathsf{A}n = & 0. & a_{n1} & a_{n2} & a_{n3} & \cdots & [a_{nn}] & \cdots \\
\vdots & & & & & & \vdots & \ddots
\end{array}$$

Figura 1.7: Procedimento diagonale di Cantor

dove con $a_{i,j}$ si indica la j-esima cifra decimale dell'i-esimo elemento di A. Sia ora $y = 0, b_1 b_2 b_3 ...$ t.c. $b_i \neq a_{i,i}$ $\forall i$; ma ora, sicuramente $y \in A$ ma è diverso da ognuno degli elementi della tabella (poichè è diverso per almeno una cifra, per come è stato costruito), allora questo prova che A non è numerabile. □

Da questo teorema discende immediatamente che i numeri reali non sono numerabili; si dirà che un insieme ha la potenza del continuo se può essere messo in corrispondenza biunivoca con l'insieme dei numeri reali.
E' noto che l'insieme delle parti $P(A)$ di un insieme A di n elementi, ha 2^n elementi; Cantor mostrò che per un insieme infinito A, l'insieme delle parti $P(A)$ non può essere messo in corrispondenza biunivoca con A; quindi $P(A)$ ha una cardinalità infinita e maggiore di A. Si può dimostrare che la cardinalità di $P(\mathbb{N})$ (anche indicata con $2^{\aleph_0}$ è pari a quella di $\mathbb{R}$, la cardinalità del continuo.
Cantor si spinse così oltre; introducendo i numeri transfiniti: il più piccolo numero cardinale transfinito è Aleph-zero $\aleph_0$ (la cardinalità del numerabile), seguito da Aleph-uno $\aleph_1$.
Quindi oggi, in teoria degli insiemi, si trattano insiemi infiniti di ogni cardinalità anche non numerabile né continua. Per vario tempo è stata un problema l'ipotesi del continuo, secondo cui non esistono insiemi di cardinalità intermedia tra quella del numerabile e quella del continuo. Nel 1962 è stato dimostrato che questa ipotesi fa parte dei problemi indecidibili (in teoria degli insiemi non si può né negare né dedurre l'ipotesi del continuo a partire dagli altri assiomi).
Quindi l'accettazione o meno del fatto che $\aleph_1$ sia la cardinalità del continuo ha portato la matematica a diramarsi ulteriormente; oggi la posizione più comune assume per vera l'ipotesi del contiuo.

La teoria degli insiemi, con il suo uso dell'infinito in atto, si portò dietro non pochi problemi; i più conosciuti sono l'antinomia di Cantor e quella di Russel, che adesso enunceremo brevemente.

Antinomia di Russel: se $R = \{x \mid x \notin x\}$, allora $R \in R \iff R \notin R$; cioè l'insieme di tutti gli insiemi che non appartengono a sé stessi, appartiene a sé stesso se e solo se non appartiene a sé stesso.

Antinomia di Cantor: Si consideri la totalità degli insiemi, la classe totale A, ovvero l'insieme di tutti gli insiemi. Sia poi $P(A)$ l'insieme delle parti di A; allora $P(A)$ dovrebbe avere potenza maggiore di A, ma essendo A l'insieme di tutti gli insiemi, esso contiene $P(A)$ come suo sottoinsieme, quindi $P(A)$ non potrebbe avere cardinalità maggiore di quella di A.

Iniziò così una crisi dei fondamenti della matematica (che si era cercata di fondare sulla teoria degli insiemi), che portò alla nascita e allo sviluppo di vari settori (in toeria degli insiemi ed in logica matematica), che in modi diversi posero rimedio alle contraddizioni che sorgevano (per esempio grazie

a *Gödel* e *Cohen*).
Il metodo assiomatico moderno che portò così alla creazione di rami diversi della matematica e anche a possibili logiche matematiche diverse.

Questa che abbiamo brevemente ripercorso è una piccola storia dell'infinito dai tempi più antichi ad oggi; si vede come questo concetto sia strettamente legato a come si intende la matematica. Oggi nessuno si fa problemi ad utilizzare l'infinito potenziale in limiti e derivate, e ad utilizzare l'infinito attuale nella cardinalità degli insiemi.
Nonostante questo, i dibattiti sul ruolo, la giustificazone, l'utilizzo o meno e la validità del concetto di infinito sono tutt'ora aperti; l'unica cosa certa e riconosciuta da tutti è la centralità del ruolo che l'infinito ha avuto e ha tutt'ora nella matematica.

Capitolo 2

L'infinito e i frattali

Tutti hanno avuto a che fare, nella loro quotidianità, con oggetti simili a frattali, forse senza rendersene conto; la natura infatti è piena di oggetti che hanno in comune la medesima caratteristica, e cioè di essere tali che loro parti più piccole sono simili all'oggetto stesso.
Questa proprietà, meglio nota come autosimilarità è una caratteristica comune a molti oggetti matematicamente classificati come frattali.
Uno dei nomi più importanti in questo campo di studi è sicuramente quello di Benoit Mandelbrot; egli fu il primo a sentire la necessità di ideare un nuovo tipo di geometria per studiare queste figure geometriche naturali (la geometria euclidea non era adatta).
Il primo libro in cui trattò di questi argomenti fu: "Les objets fractals: forme, hasard et dimension" pubblicato nel 1975; egli si proponeva con questo scritto di spiegare in modo rigorosamente matematico il concetto di autosomiglianza, il caos e il caso, e il nuovo concetto di dimensione (non intera).

2.0.1 I frattali in natura e il concetto di autosimilarità

La natura è un buon punto di partenza per questo tipo di studio; infatti molte figure geometriche che troviamo in natura non possono essere ricondotte ai poligoni o ai poliedri (regolari o non), della geometria euclidea; presentano infatti un carattere molto più frammentario.
Partiamo da due esempi, che sono forse i più conosciuti; una felce (ma anche un cavolfiore) e le coste della Bretagna (ma anche quelle della Norvegia o della Sardegna).

Felce:
Osserviamo una felce e notiamo subito una certa regolarità; infatti ogni foglia ha la stessa forma di tutta la felce, così come ogni fogliolina della foglia ha

la stessa forma della foglia stessa.
Generalizzando questa idea in un oggetto frattale, supponendo di avere una lente di ingrandimento, ad ingrandimenti sempre maggiori, ciò che vediamo mantiene sempre le stesse proprietà dell'oggetto di partenza. Questa proprietà mi dice che ogni parte dell'oggetto è simile (ha la stesssa forma) al tutto; prende il nome di autosimilarità:

Definizione 2.1. (struttura autosimilare) La terna (X, S, f_s) si dice essere una struttura autosimilare se: X è uno spazio topologico compatto, S è una famiglia finita di indici t.c. $\{f_s\}_{s\in S}$ sia una famiglia di omeomorfismi suriettivi per cui $X = \bigcup_{s\in S} f_s(X)$.

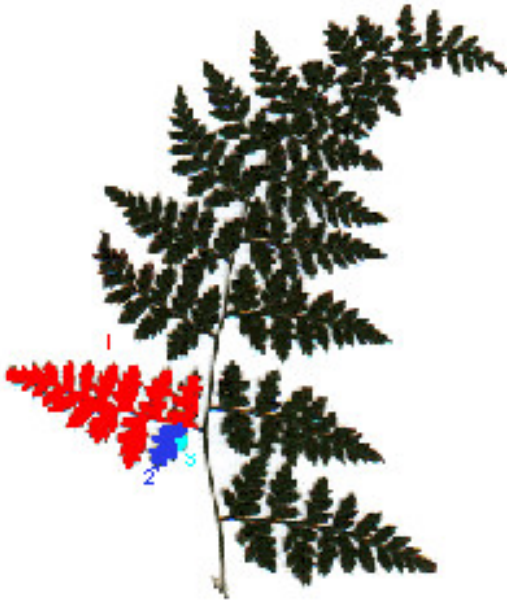

Figura 2.1: Proprietà di autosimilarità della felce

Questa è una prima proprietà che devono avere tutti i frattali, la felce frattale (vedi Figura 2.1) è considerata un esempio di frattale biomorfo (anche se in realtà, per i frattali perfetti si richiede che la proprietà di autosimilarità si mantenga all'infinito, mentre ovviamente, per gli oggetti naturali, ad un certo punto dell'ingrandimento si troveranno le singole cellule e si perderà la struttura).

Coste della Bretagna:
partendo dal classico concetto di dimensione, Mandelbrot affermò che la lunghezza di una costa aveva dimensione d:

$$1 < d < 2;$$

Mandelbrot infatti propose il seguente metodo di misura:
ovviamente la lunghezza di un tratto di costa sarebbe stata più di quella del segmento che congiungeva i due estremi dato che la costa era piuttosto frastagliata, allora si poteva prendere un compasso di apertura fissata e farlo avanzare lungo la costa in modo che ogni passo iniziasse dove finiva il precedente.
In questo modo moltiplicando il numero dei passi per l'ampiezza del compasso si sarebbe ottenuta la lunghezza cercata. Più si riduce l'ampiezza del compasso, più la lunghezza della costa tende ad aumentare.
Ma allora si è visto che, a seconda dell'ampiezza dell'apertura del compasso, si possono ottenere sia i dettagli che il carattere generale della costa, senza però riuscire a dare una vera misura della sua lunghezza.
Poichè si può approssimare una costa al merletto di Koch e sappiamo (si vedrà successivamente) che questo ha lunghezza infinita, ne verrà che anche la lunghezza della costa della Bretagna è infinita.

Figura 2.2: Costa dell'Inghilterra a misurazioni sempre più precise

Da queste osservazioni si arrivò a definire un'altra importante proprietà dei frattali, e cioè quella di avere dimensione non intera; in particolare Mandelbrot osservò che una curva per avere dimensione compresa tra 1 e 2 deve avere superficie nulla e lunghezza infinita (analogamente una superficie con dimensione compresa tra 2 e 3, deve avere area infinita e volume nullo).
La parola stessa frattale deriva da questo suo carattere caotico, frazionario, spezzato; sta infatti ad indicare la dimensione non intera.

Definizione 2.2. (frattale) Un frattale è un oggetto matematico di dimensione frazionaria pari a

$$d = \frac{\log N}{\log \frac{1}{k}};$$

dove N sono le parti simili all'oggetto intero in cui questo può essere diviso e k è il rapporto di omotetia.
(Infatti per ogni frattale possiamo vedere N copie autosimili, tutte ottenute mediante una omotetia di rapporto k).

In generale un frattale ha tre proprietà principali: è autosimile, ad ogni ingrandimento emergono altri dettagli, è definito da una funzione ricorsiva, e infine, è caratterizzato da una dimensione non intera (maggiore rispetto a quella in cui lo si può disegnare).

L'infinito nei frattali è molto importante, quando si parla di infinito non si intende infinitamente grande o piccolo, ma infinitamente ripetuto. Analogamente se si misurassero con la geometria classica alcuni frattali (come ad esempio le coste della Bretagna, o il fiocco di neve di Koch) si otterrebbe uno sviluppo infinito che non darebbe alcun risultato utile nella effettiva misurazione.
Proprio per la centralità del concetto di infinito, o meglio, di infinitamente ripetuto si è sentita la necessità di coniare un nuovo termine per identificare questi nuovi oggetti e una nuova misura per poter dare risposte più precise riguardo alle dimensione di questi oggetti; da qui nascerà quindi la dimensione e la misura di Hausdorff.

2.0.2 La matematica dei frattali

Misura e dimensione di Hausdorff

Definizione 2.3. $\forall \alpha \in \mathbb{R}, \alpha \geqslant 0$ definiamo

$$w_\alpha := \frac{\pi^{\frac{\alpha}{2}}}{\Gamma(\frac{\alpha}{2}+1)},$$

dove Γ è la funzione gamma di Eulero definita per $s > 0$:

$$\Gamma(s) = \int_0^{+\infty} e^{-t} t^{s-1}\, dt.$$

Si può osservare che w_α è una costante dimensionale che dipende solo da α e nel caso in cui α sia un numero intero positivo: w_α=misura di Lebesgue α dimensionale del disco unitario.

Definizione 2.4. Per ogni $A \subseteq \mathbb{R}^n$, A non vuoto, definiamo:
1)

$$diam(A) = sup\{d(x,y) : x, y \in A\};$$

2)

$$r(A) = \frac{1}{2} diam(A) = \frac{1}{2} sup\{d(x,y) : x, y \in A\};$$

(dove con $d(x,y)$ intendiamo la distanza euclidea tra x e y)
3)

$$m_\alpha(A) = w_\alpha (r(A))^\alpha;$$

$\forall \alpha$ reale positivo
4) se $A = \varnothing$ definiamo $m_\alpha(A) = 0$.

Per ogni $A \subseteq \mathbb{R}^n$, fissato δ reale positivo, si chiama δ-ricoprimento di A una famiglia $(B_k)_{k \in a}$ di sottoinsiemi di $\mathbb{R}^n$ t.c.:
i) a sia finito o numerabile
ii) $diam(B_k) \leqslant \delta \ \forall k \in a$
iii) $A \subseteq \bigcup_{k \in a} B_k$.

Definiamo inoltre:

$$H^\delta_\alpha(A) := inf\{\sum_{k \in a} m_\alpha \ (B_k) \ t.c. \ (B_k)_{k \in a} \ \delta - ricoprimento \ di \ A\}.$$

Vale che se $0< \delta' < \delta$, ogni δ'-ricoprimento di A è anche un δ-ricoprimento di A e quindi $H^\delta_\alpha(A) \leqslant H^{\delta'}_\alpha(A)$, cioè se consideriamo la funzione

$$\delta \mapsto H^\delta_\alpha(A),$$

questa sarà monotona decrescente e di conseguenza avrà limite per $\delta \mapsto 0^+$.

Definizione 2.5. Si chiama allora misura di Hausdorff α-dimensionale:

$$H_\alpha(a) = \lim_{\delta \mapsto 0^+} H^\delta_\alpha(A) = \sup_{\delta > 0} H^\delta_\alpha(A).$$

Proposizione 2.0.4. *H_α è una misura metrica rispetto alla distanza euclidea, cioè, valgono le seguenti proprietà:*
1)

$$H_\alpha(\varnothing) = 0;$$

2)

$$H_\alpha(A) \leqslant H_\alpha(B) \text{ con } A \subseteq B;$$

3)

$$H_\alpha \text{ e' subadditiva } (H_\alpha(\bigcup_k B_k) \leqslant \bigcup_k H_\alpha(B_k));$$

4)

$$H_\alpha(A \cup B) = H_\alpha(A) + H_\alpha(B) \text{ con } d(A,B) > 0.$$

Definizione 2.6. Si dice che $A \subseteq \mathbb{R}^n$ è un insieme H_α misurabile se per ogni E sottoinsieme di $\mathbb{R}^n$ vale che $H_\alpha(E) = H_\alpha(E \cap A) + H_\alpha(E \cap A^C)$.

In particolare si avrà che tutti gli insiemi aperti o chiusi di $\mathbb{R}^n$ sono H_α misurabili; inoltre vale che tutti gli insiemi A di $\mathbb{R}^n$ misurabili secondo Lebesgue, sono anche H_α misurabili e le due misure coincidono.
Mostriamo ora alcune proposizioni che ci permetteranno di dare la definizione di dimensione di Hausdorff.

Proposizione 2.0.5. *Sia $A \subseteq \mathbb{R}^n$ t.c. $H_\alpha(A) < \infty$ per un opportuno $\alpha \geqslant 0$, allora vale che*

$$H_{\alpha+t}(A) = 0 \ \forall t > 0$$

Dimostrazione. Sia $\delta > 0$ e sia $(B_k)_{k\in a}$ un δ-ricoprimento di A, consideriamo ora:

$$0 \leqslant H^\delta_{\alpha+t}(A) \leqslant \sum_{k\in a} m_{\alpha+t}(B_k) = \sum_{k\in a} w_{\alpha+t}(r(B_k))^{\alpha+t},$$

poichè per ipotesi $diam(B_k) < \delta$ allora $r(B_k) < \frac{\delta}{2}$ cioè:

$$0 \leqslant H^\delta_{\alpha+t}(A) \leqslant (\frac{\delta}{2})^t \frac{w_{\alpha+t}}{w_\alpha} \sum_{k\in a} w_\alpha(r(B_k))^\alpha = (\frac{\delta}{2})^t \frac{w_{\alpha+t}}{w_\alpha} \sum_{k\in a} m_\alpha(B_k);$$

considerando ora l'estremo inferiore rispetto ai δ-ricoprimenti di A avrò che:

$$0 \leqslant H^\delta_{\alpha+t}(A) \leqslant (\frac{\delta}{2})^t \frac{w_{\alpha+t}}{w_\alpha} H^\delta_\alpha(A);$$

e infine passando al limite per $\delta \mapsto 0^+$ e ricordando che $H_\alpha(A) < \infty$ per ipotesi:

$$H_{\alpha+t}(A) = lim_{\delta \mapsto 0^+} H^\delta_{\alpha+t}(A) = 0.$$

□

Proposizione 2.0.6. *Per ogni $A \subseteq \mathbb{R}^n$ vale che*

$$H_{n+t}(A) = 0 \ \forall t > 0.$$

Dimostrazione. Sia $B(0,k)$ il disco in $\mathbb{R}^n$ di centro 0 e raggio k, allora $A = \bigcup_{k=1}^{\infty}(A \cap B(0,k))$. Per la proprietà di subadditività della misura di Hausdorff:

$$0 \leq H_{n+t}(A) \leq \sum_{k=1}^{\infty} H_{n+t}(A \cap B(0,k)).$$

Inoltre vale che

$$H_n(A \cap B(0,k)) \leq H_n(B(0,k)) = \omega_n k^n < \infty.$$

Quindi per quanto visto sopra

$$H_{n+t}(A \cap B(0,k)) = 0 \ \forall t > 0, \ \forall \ k \in \mathbb{N},$$

e sostituendo nella prima equazione, questo prova l'asserto. □

Definizione 2.7. Sia $A \subseteq \mathbb{R}^n$; definiamo dimensione di Hausdorff di A, il numero reale non negativo

$$\alpha(A) = inf\{s > 0 \ t.c. \ H_s(A) = 0\}.$$

Per quanto appena provato nelle proposizioni di cui sopra avrò che $\alpha(A) \leqslant n$ e inoltre:

Proposizione 2.0.7. *Sia $A \subseteq \mathbb{R}^n$, $0 < \alpha(A)$, allora:*

$$H_t(A) = \begin{cases} 0 & se \ t > \alpha(A) \\ \infty & se \ 0 \leqslant t < \alpha(A) \end{cases}.$$

Dimostrazione. Nel primo caso $\exists s < t$ t.c. $H_s(A) = 0$; quindi per quanto visto sopra vale che:

$$H_t(A) = 0.$$

Nel secondo caso supponiamo PA che $H_t(A) < \infty$ allora, come sopra, si avrebbe che

$$H_s(A) = 0 \ \forall s > t,$$

cioè, per la definizione di dimensione di Hausdorff, $\alpha(A) \leqslant t$ ma questo è assurdo poichè va contro le ipotesi; questo conclude la prova del toerema. □

Insieme di Cantor

L'insieme di Cantor è il più noto sottoinsieme di $\mathbb{R}$ avente dimensione di Hausdorff non intera; vediamo di cosa si tratta.
Consideriamo l'intervallo chiuso $[0, 1]$ e costruiamo l'insieme di Cantor C in questo modo:

Figura 2.3: Insieme di Cantor

$$C_0 = [0,1], C_1 = [0, \frac{1}{3}] \cup [\frac{2}{3}, 1], C_2 = [0, \frac{1}{9}] \cup [\frac{2}{9}, \frac{1}{3}] \cup [\frac{2}{3}, \frac{7}{9}] \cup [\frac{8}{9}, \frac{1}{1}], ...$$

Iterando quindi il procedimento avrò che

$$C_k = \bigcup_{j=1}^{2^k} I_j,$$

dove I_j sono intervalli di lunghezza pari a $\frac{1}{3^k}$, e si definirà quindi l'insieme di Cantor C:

$$C = \bigcap_{j=0}^{\infty} C_j.$$

Mostriamo innanzitutto che la misura di Lebesgue (mis) dell'insieme di Cantor è pari a 0, mostriamo cioè che

$$0 = mis(C) = mis([0,1]) - mis(C^C) = 1 - mis(C^C),$$

equivalentemente mostriamo che mis(C^C)=1.

Ma ora, per come abbiamo costruito l'insieme di Cantor la parte "rimossa" sarà:

$$\frac{1}{3}+\frac{2}{9}+\frac{4}{27}+...=\sum_{n=0}^{\infty}\frac{2^n}{3^{n+1}}=\frac{1}{3}\sum_{n=0}^{\infty}(\frac{2}{3})^n=\frac{1}{3}\frac{1}{1-\frac{2}{3}}=1.$$

Ci rimane ora da provare che

$$\alpha(C)=\frac{log2}{log3}:$$

osserviamo innanzitutto che la famiglia (C_k) definita come sopra è un δ-ricoprimento di C con $\delta=(\frac{1}{3})^k$, quindi per definizione avrò che:

$$H^{\delta}_{\alpha}(C)\leqslant\sum_{j=1}^{2^k}m_{\alpha}(I_j)=\sum_{j=1}^{2^k}w_{\alpha}(\frac{1}{3^k}\frac{1}{2})^{\alpha}=2^kw_{\alpha}(\frac{1}{3^k}\frac{1}{2})^{\alpha}=2^{k-\alpha}3^{-k\alpha}w_{\alpha}.$$

Posto ora $s=\frac{log2}{log3}$ ne viene che

$$H^{\delta}_{\alpha}(C)\leqslant 2^{-\alpha}w_{\alpha}e^{k(s-\alpha)log(3)},$$

e quindi:

$$H_{\alpha}(C)=\lim_{\delta\mapsto 0^+}H^{\delta}_{\alpha}(C)=\lim_{k\mapsto\infty}H^{\delta}_{\alpha}(C)=0$$

per $\alpha>s$.

Osservando questo insieme da un punto di vista più generale, possiamo notare che è molto evidente la proprietà di autosimilarità, infatti ogni intervallo di un C_k è simile a C sono contenute tutte le informazioni necessarie per sapere come è fatto tutto l'insieme; proprio per questo l'insieme di Cantor è uno dei primi e più semplici esempi di frattali.
Ricordando la prima definizione di frattale, possiamo osservare che, in effetti, ad ogni passo da un segmento inziale vengono generati 2 segmenti, di lunghezza pari a $\frac{1}{3}$ di quella del segmento iniziale; cioè $N=2$ e $k=3$ proprio come si è appena provato.

La curva di Koch

Un altro famoso esempio di frattale è la curva di Koch, K (o fiocco di neve di Koch, o merletto di Koch); si tratta sempre di considerare l'intervallo

chiuso $[0, 1]$ e di dividerlo in 3 parti.
Nella parte centrale viene poi costruito un triangolo equilatero avente come base la parte centrale stessa, e si ripete così questo procedimento, dividendo ripetutamente in 3 parti ogni lato della costruzione e costruendo nel segmento in mezzo un triangolo equilatero, che ha il segmento stesso come base (la base viene sempre tolta dalla costruzione).
In questo caso, al contrario di quanto mostrato sopra, si ha che la misura di Lebesgue (mis) della curva di Koch è infinita mentre

$$\alpha(K) = \frac{log4}{log3},$$

basta osservare che ad ogni iterazione $k - esima$ la mis(K)=$(\frac{4}{3})^k$ ma allora al limite per $k \mapsto +\infty$: mis(K)=$+\infty$.

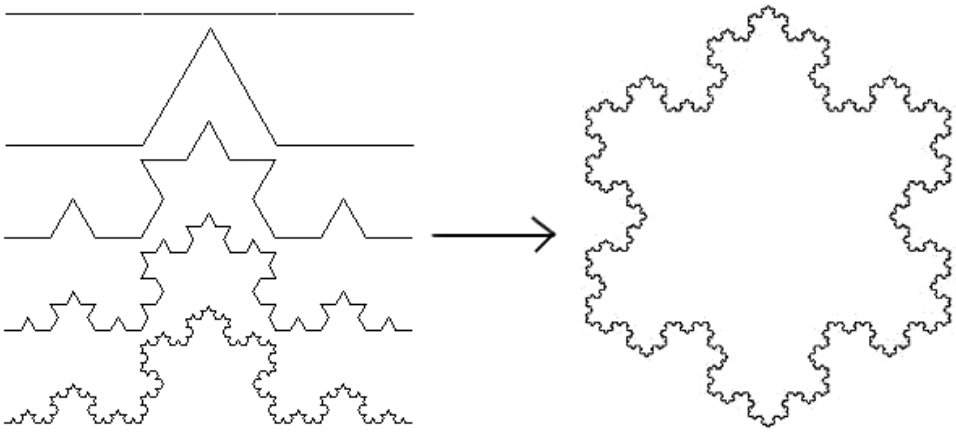

Figura 2.4: La curva e il fiocco di neve di Koch

Per la dimostrazione di $\alpha(K) = \frac{log4}{log3}$, si procede analogamente a sopra; osserviamo che in questo caso, ogni segmento viene diviso in 4 parti, ognuna delle quali ha lunghezza pari a $\frac{1}{3}$ di quella del segmento iniziale; cioè: $N = 4$ e $k = 3$.

2.0.3 Frattali famosi

Un altro frattale molto famoso è il triangolo di Sierpinski S; si può vedere che ha misura di Lebesgue (mis) pari a 0, mentre:

$$\alpha(K) = \frac{log3}{log2}.$$

Si considera un triangolo equilatero "pieno", poi lo si divide in 4 triangoli equilateri, unendo i punti medi dei lati, e si toglie quello centrale, si ripete infine questo ultimo passaggio su ognuno dei triangoli ottenuti, e si itera il procedimento, ottenendo:

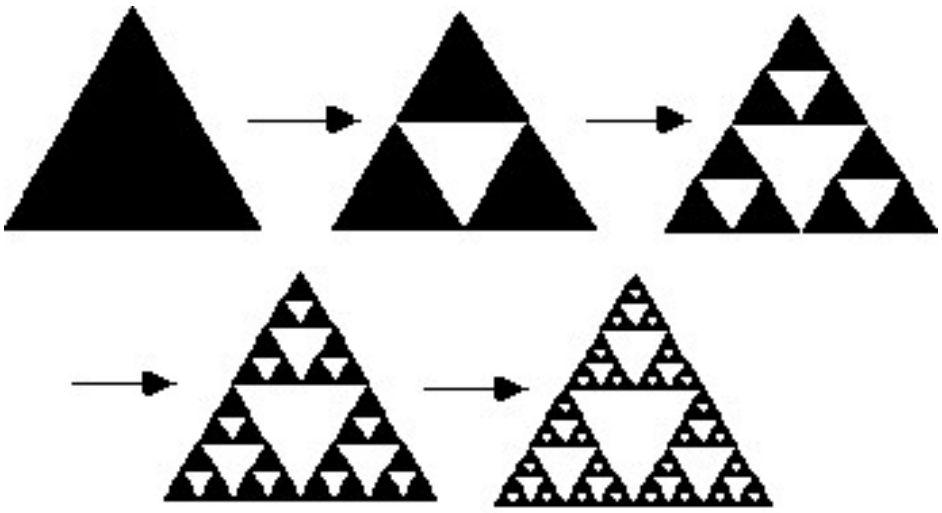

Figura 2.5: Triangolo di Sierpinski

Gli esempi appena visti sono frattali lineari, è cioè frattali il cui algoritmo generatore è lineare; oltre a questi però abbiamo anche frattali non lineari (in cui l'algoritmo generatore presenta equazioni di ordine superiore a 1) e frattali aleatori (che, come dice il nome, derivano la loro forma da quantità scelte a caso).
Da frattali, relativamente semplici come quelli visti sopra, oggi si studiano frattali come quelli di Mandelbrot o quelli di Julia, estremamente complessi. Questo uso dell'infinito come infinitamente ripetuto non ha affascinato solo i matematici, ma ha contagiato molti campi del sapere, infatti esistono numerose opere artistiche, letterarie o musicali ispirate proprio alla geometria frattale; come detto nell'introduzione, il concetto di infinito non appartiene solo ai matematici.

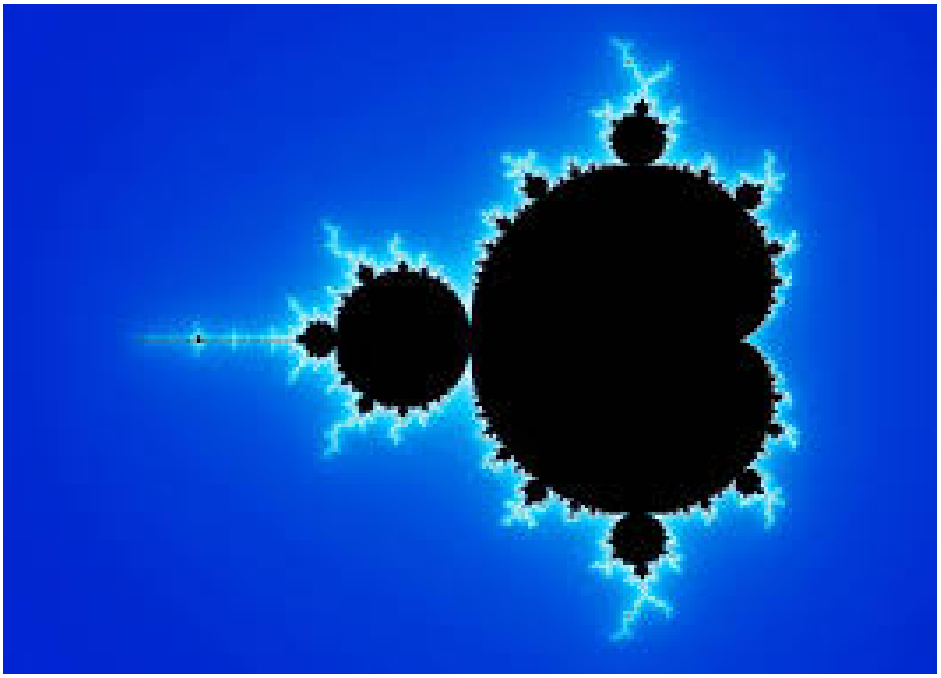

Figura 2.6: Insieme di Mandelbrot

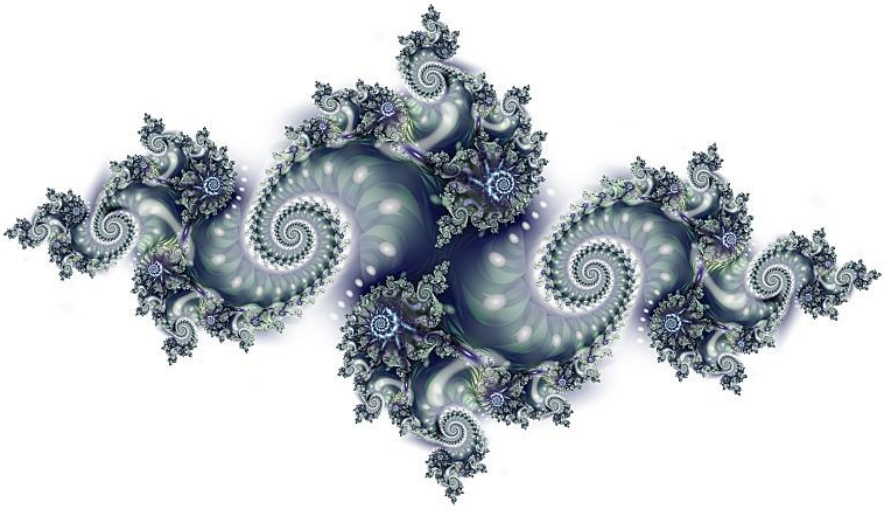

Figura 2.7: Insieme di Julia

Capitolo 3

L'infinito in crittografia

Sin da tempi molto antichi si è sentita la necessità di poter comunicare in modo segreto, cioè in modo che terze parti, differenti da emissario e ricevente del messaggio, non potessero in alcun modo capire il testo del messaggio.
Il campo di studi che si occupa di quanto sopra è la *crittografia*; facciamo alcune premesse necessarie per un uso chiaro di alcuni termini. Si parlerà di *testo in chiaro* per il messaggio da inviare, di *testo cifrato* per il messaggio cifrato, e di *chiave* (ciò che permette al messaggio di essere segreto).

Definizione 3.1 (crittosistema)**.**
Data la quintupla (P, C, K, E, D) questa definisce un *crittosistema* se:
- P è l'insieme finito dei possibili testi in chiaro
- C è l'insieme finito dei possibili testi cifrati
- K è l'insieme delle chiavi
- $\forall k \in K \ \exists \ f_k \in E$ ed $\exists \ g_k \in D$ t.c. $f_k : P \to C$, $g_k : C \to P$ sono t.c. $g_k(f_k(x)) = x$, $\forall \ x \in P$; f_k sarà detta *funzione di cifratura* e g_k *funzione di decifrazione.*

Figura 3.1: Schema di un crittosistema

Chiaramente la funzione f_k deve essere iniettiva (infatti esiste la funzione inversa g_k) altrimenti non si potrebbe avere l'unicità nella decifrazione; si vedrà poi nei cifrari affini come questa proprietà sarà di notevole importanza. L'immagine di Figura 3.1 rappresenta lo schema classico di un crittosistema (si ricordi che nella crittografia moderna si assume sempre che l'intercettatore conosca l'algoritmo usato per cifrare/decifrare).
In questo capitolo ci occuperemo di cifrari a chiave simmetrica: ovvero cifrari (e cioè uno strumento crittografico che cifra ogni stringa di caratteri) la cui chiave è conosciuta da mittente e ricevente. La sicurezza di questi sistemi è basata principalmente sulla difficoltà per terze parti di trovare la chiave; si definisce *attacco a forza bruta* quello consistente nel provare tutte le chiavi possibili. Ovviamente questa è l'ultima risorsa a cui si deve fare ricorso e spesso questi tentativi richiederebbero un tempo superiore alla stessa età dell'universo !! Si fa perciò ricorso ad altri metodi, come l'analisi di frequenza. Esiste un sistema indecifrabile che ha, ovviamente un costo altissimo, ed è un crittosistema sviluppato in prima sede da Vernam e successivamente da Mauborgne; sarà di questo sistema che ci occuperemo con un particolare interesse al ruolo che l'infinito ha avuto nel garantire a questo crittosistema il primato di inviolabilità.

3.1 Cifrario di Vigenère

testo in chiaro	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x
testo cifrato (C.)	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	a	b	c
testo cifrato (A.)	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	aa

Tabella 3.1: Cifrari di Cesare e di Augusto

Uno dei più antichi cifrari di cui sia rimasta traccia è il cifrario di Giulio Cesare; grazie allo storico Svetonio è giunto fino a noi il racconto di come Giulio Cesare comunicasse con le sue truppe; ovvero con un cifrario a sostituzione monoalfabetica che consisteva nello spostare di 3 posizioni ogni lettera, mandando le ultime lettere dell'alfabeto nelle prime. Si sa che anche Augusto usava questo metodo però leggermente modificato; infatti ogni

lettera era spostata di 1 sola posizione ed alla lettera X corrispondeva AA; facciamo quindi vedere lo schema di questi due metodi di cifratura e diamo un esempio di trasformazione da testo in chiaro a testo cifrato:

Esempio:
-testo in chiaro:ipse dixit
-testo cifrato (C.):msxhgmcma -testo cifrato (A.):kqtfekaaku

La decifrazione quindi (che a quei tempi era comunque ritenuta molto difficile se non impossibile, basti pensare al tasso di alfabetizzazione), consisteva nel far scorrere ogni lettera indietro di rispettivamente 3 o 1 posizione (ricordando nel caso di Augusto che la x viene cifrata con aa) e nel riposizionare gli spazi (si ricordi che in ogni testo cifrato punteggiatura e spazi sono sempre omessi).
Più in generale, considerando il moderno alfabeto inglese composto da 26 caratteri, si definisce la funzione: $x \mapsto x + k \mod(26)$ con $k \in [0, 25]$ come funzione per la cifratura, e si definisce la funzione g_k: $x \mapsto x - k \mod(26)$ con $k \in [0, 25]$ come funzione per la decifrazione, k sarà così la chiave.

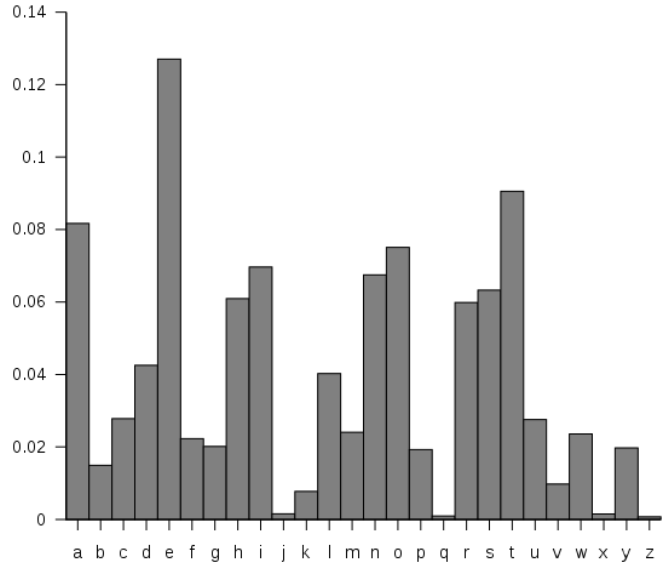

Figura 3.2: Tabella delle frequenze delle lettere della lingua inglese

Questo cifrario può facilmente essere attaccato con un attacco a forza bruta; supponiamo infatti di possedere soltanto il testo cifrato, allora basterà semplicemente provare tutti i valori di k che sappiamo essere 26 e si otterrà praticamente sempre un solo messaggio di senso compiuto. Un'altra tecni-

ca (avendo un messaggio non troppo corto) può essere quella di sfruttare la frequenza delle lettere; esistono tabelle di frequenza delle lettere di ogni lingua, basterà allora cercare la lettera più frequente in questa tabella e vedere la lettera più frequente nel testo cifrato, se ne potrà così ricavare la chiave. Quelli che abbiamo visto sono esempi di cifrario a sostituzione (cioè un cifrario in cui ad ogni lettera viene applicata sempre la stessa fissata permutazione dell'alfabeto); in contrapposizione ai cifrari a permutazione, in cui il testo viene diviso in blocchi e vengono applicate permutazioni degli elementi di ogni blocco, che cambiano solo l'ordine dei caratteri.

Come abbiamo mostrato, questo tipo di cifrario è facilmente attaccabile; un modo per aumentarne la sicurezza è quello di passare ai cifrari affini.
Si tratta questa volta di considerare una funzione f_k per la cifratura t.c. : $x \mapsto \alpha x + \beta \pmod{26}$ con $\alpha, \beta \in \mathbb{Z}_{26}$ e $\text{MCD}(\alpha, 26) = 1$; poichè α è unità avrà un inverso moltiplicativo e quindi la funzione di decifrazione g_k sarà t.c. $y \mapsto \alpha^{-1}(y - \beta)$.
Si osservi che la condizione MCD(α,26)=1 è necessaria per avere l'iniettività della f_k e per poter calcolare quindi la funzione di decifrazione g_k; mostriamo infatti un esempio in cui mancando questa ipotesi sul MCD, viene a meno l'iniettività di f_k:
siano $\alpha = 13$ e $\beta = 4$ cioè la nostra f_k sarà: $x \mapsto 13x + 4$; allora si avrà:

input $\mapsto$ *errer*
alter $\mapsto$ *errer*

Proprio per ovviare a questo problema si è aggiunta l'ipotesi $\text{MCD}(\alpha, 26) = 1$ infatti si possono dimostrare i seguenti teoremi:

Teorema 3.1.1. *Siano a,b*$\in \mathbb{Z}$ *t.c.* $MCD(a, b) = 1$*; se* $\exists x, y \in \mathbb{Z}$ *t.c.* $bx \equiv by$ *(mod a), allora* $x \equiv y$ *(mod a).*

Dimostrazione. $bx \equiv by \pmod{a} \Leftrightarrow b(x - y) \equiv 0 \pmod{a}$ ma per ipotesi $MCD(a, b) = 1$ cioè b è un'unità nell'anello $\mathbb{Z}_a$ e quindi b non può essere uno 0-divisore in questo; allora deve per forza essere $x \equiv y \pmod{a}$, e questo prova l'asserto. □

Teorema 3.1.2. *Sia f:*$I \to I$*, con* I *intervallo di* $\mathbb{R}$*, t.c.* $f(x)=\alpha x + \beta$ *con* $\alpha, \beta \in \mathbb{Z}$*; f è iniettiva (mod k),* $k \in \mathbb{N} \Leftrightarrow MCD(\alpha, k) = 1$.

Dimostrazione. Per definizione f è iniettiva $\pmod{k} \Leftrightarrow (\forall x, z \in I$ t.c. $f(x) \equiv f(z) \pmod{k} \Rightarrow x \equiv z \pmod{k}) \Leftrightarrow (\forall x, z \in \text{I}$ t.c. $\alpha x + \beta \equiv \alpha z + \beta \pmod{k} \Rightarrow x \equiv z \pmod{k}) \Leftrightarrow (\forall x, z \in \text{I}$ t.c. $\alpha x \equiv \alpha z \pmod{k} \Rightarrow x \equiv z \pmod{k})$.
Per il teorema di cui sopra se MCD(α, k)=1 allora f è iniettiva.
Viceversa supponiamo che f sia iniettiva, allora vogliamo provare che

MCD(α, k)=1, che è equivalente a provare che $\alpha \pmod k$ non è uno 0-divisore; supponiamo PA che α sia uno 0-divisore allora $\exists d \in I$ t.c. $\alpha \cdot d$=0, ma questo d lo posso vedere come $d = x - z$ e cioè $\alpha x \equiv \alpha z \pmod k \nRightarrow x \equiv z \pmod k$) ma questo è assurdo poichè avevamo supposto f iniettiva, allora α non è uno 0-divisore cioè MCD(α, k)=1. □

Quindi in conclusione la chiave di questi cifrari affini è una coppia (α, β) con $\alpha, \beta \in \mathbb{Z}_{26}$; β può assumere 26 valori mentre α deve essere t.c.
MCD(α,26)=1, cioè α deve appartenere a $\mathbb{Z}_{26}^*$ e poichè $|\mathbb{Z}_{26}^*|=\phi(26)$ (con ϕ=funzione indicatrice di Eulero)=(13-1)(2-1)=12.
In totale si avranno quindi 12*26=312 possibili chiavi. Valutiamo ora come sia possibile attaccare questo codice: per quanto detto nelle righe precedenti le possibili chiavi totali sono 312, quindi possedendo solo il testo cifrato, il miglior modo per provare a decifrarlo è far svolgere al computer la prova per queste 312 chiavi (compito che il computer svolge in maniera semplice).

Una variante dei cifrari appena visti è un cifrario a sostituzione polialfabetico, noto con il nome di cifrario di Vigènere (Blaise de Vigenère, 1532-1596); questo cifrario prevede innanzitutto di stabilire una chiave di lughezza scelta composta da interi compresi tra 0 e 25 (spesso alla sequenza di questi numeri è associata una parola semplicemente ponendo 0=a, 1=b ...); usando la chiave si farà scorrere ogni lettera del testo in chiaro di un numero di posizioni pari al numero corrispondente della chiave, e una volta arrivati alla fine della chiave si ricomincia da capo. Questo procedimento può essere visto semplicemente come il cifrario di Cesare che però cambia chiave ad ogni lettera; diamone un esempio:

Esempio:

testo in chiaro	p	r	o	n	t	i	p	a	r	t	e	n	z	a	v	i	a
chiave	c	a	m	p	a	n	a	c	a	m	p	a	n	a	c	a	m
testo cifrato	r	r	a	c	t	v	p	c	r	f	t	n	m	a	x	i	m

Tabella 3.2: Cifratura di Vigénere

Definizione 3.2 (cifrario di Vigènere)**.**
Sia m un intero positivo fissato; siano poi $P, C, K \in (\mathbb{Z}_{26})^m$ con la chiave $K=(k_1, k_2, ..., k_m)$; definiamo la funzione di cifratura f_k del cifrario di

Vigènere:
$f_k(x_1, x_2, ..., x_m)$=$(k_1 + x_1, k_2 + x_2, ..., k_m + x_m)$
e la funzione di decifrazione g_k del cifrario di Vigènere:
$g_k(y_1, y_2, ..., y_m)$=$(y_1 - k_1, y_2 - k_2, ..., y_m - k_m)$
il tutto (mod 26).

Un modo più veloce per effettuare questa cifratura è quello di sfruttare la tabella di Vigènere (o tabula recta) che consiste in un quadrato di 26 righe per 26 colonne contenente tutte le lettere dell'alfabeto ed in cui ogni riga è spostata rispetto alla precedente di un posto in avanti; in questo modo leggendo le lettere del testo in chiaro nella prima riga e quelle della chiave nella prima colonna (o viceversa, la tabella è simmetrica), il loro punto di incontro sarà la lettera del testo cifrato.

	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figura 3.3: Tabula recta

Ovviamente questo sistema è sicuro se non è nota nè la chiave nè la sua lun-

ghezza; riguardo alla decifrabilità di questo cifrario si possono fare le stesse considerazioni fatte in precedenza con alcune modifiche: ovviamente conoscendo il testo cifrato ed una parte del testo in chiaro basta sottrarre i due per ottenere la chiave, è necessario però avere un testo in chiaro abbastanza lungo perchè altrimenti si rischia di non riuscire ad ottenere tutta la chiave, per questo si punta ad avere chiavi piuttosto lunghe.
Si potrebbe anche sfruttare la frequenza delle lettere come già visto sopra ma si rischia di incorrere in notevoli errori, infatti ad ogni lettera in chiaro non è detto che corrisponda sempre la stessa lettera nel testo cifrato, ed è per questo motivo che questo studio di frequenza non si rivela granchè utile.
Il metodo migliore per decifrare il messaggio è quindi quello di trovare prima la lunghezza della chiave e poi la chiave stessa; vediamo come si procede.

3.1.1 Crittanalisi del cifrario di Vigènere

Studiamo innanzitutto come ricavare la lunghezza della chiave avendo a disposizione solo il testo cifrato: i due metodi principali sono il test delle frequenze di Kasiski e quello di Friedman che prendono il nome dai loro inventori ed hanno avuto successo la prima volta rispettivamente nel 1863 e nel 1925.

Il test di Kasiski

Supponiamo di trovare nel testo cifrato delle lettere ripetute; sappiamo che questo non può dirci nulla sul testo in chiaro poichè lettere uguali possono venire cifrate con lettere diverse; supponiamo ora di trovare non singole lettere, ma sequenze di 2, 3 o più lettere uguali sparse nel testo cifrato; è probabile che queste sequenze corrisponderanno a sequenze uguali anche nel testo in chiaro e che la distanza tra queste sequenze sia un multiplo della lunghezza della chiave.
Ovviamente più lunghe sono le sequenze, maggiore è la probabilità che la distanza sia effettivamente un multiplo della lunghezza della chiave; consideriamo ad esempio un testo cifrato abbastanza lungo ed individuiamo tutte le sequenze di 3 lettere che si ripetono nel testo e mettiamo in una tabella le distanze tra una sequenza e l'altra; se ne può dedurre che la lunghezza della chiave è il MCD tra tutte le distanze.
In realtà questo metodo non può dare certezza assoluta sulla lunghezza della chiave soprattutto per due motivi; innanzitutto ci possono essere sequenze uguali generate accidentalmente e quindi la loro distanza non dovrebbe essere tenuta in considerazione nel calcolo del MCD, e inoltre è possibile che

la lunghezza della chiave non sia in realtà il MCD trovato ma ne sia un suo sottomultiplo; per questo motivo si introduce il test di Friedman.

Il test di Friedman

Questo test si basa principalmente su alcuni semplici calcoli di probabilità e sul concetto di indice di coincidenza. Per ogni lingua esistono tabelle con la frequenza di ogni lettera dell'alfabeto, consideriamo ad esempio l'alfabeto inglese e denotiamo con $p_1, ..., p_{26}$ la frequenza caratteristica di ogni lettera. Consideriamo il solito testo cifrato abbastanza lungo, la probabilità che in due posizioni qualsiasi si trovi la lettera di posizione con indice i, è semplicemente $p = p_i^2$; quindi in generale la probabilità che in due posizioni qualsiasi si trovi la stessa lettera è data da

$$p = \sum_{i=1}^{26} p_i^2.$$

Se consideriamo un testo casuale in cui ogni lettera è equiprobabile cioè $p_i = \frac{1}{26}$ la probabilità di cui sopra sarà p=0,038, molto inferiore rispetto ad un testo con significato in una qualche lingua (ad esempio in italiano questa p=0,075, quasi il doppio).
Si denota con

$$I = indice\ di\ coincidenza = \sum_{i=1}^{26} p_i^2;$$

si osserva che questo indice di coincidenza cresce al crescere dell'irregolarità del testo e diminuisce fino a 0,038 quando tutte le lettere sono equiprobabili, inoltre l'indice è invariante per i cifrari monoalfabetici mentre tende a decrescere per i cifrari polialfabetici.
Ovviamente per un testo cifrato con Vigènere si avrà un indice "più piccolo" rispetto a quello di un cifrario monoalfabetico, che dipenderà dalla lunghezza della chiave e mi permetterà di calcolare quanto vale l=lunghezza chiave.
Un modo analogo per descrivere l'indice di coincidenza è il seguente: supponiamo di avere a disposizione n lettere, di cui n_i è il numero di lettere i-esime, e di volere sapere quale è il numero di coppie possibili formate da lettere uguali; allora questo sarà dato da: $\sum_{i=1}^{26} \frac{n_i(n_i-1)}{2}$.
Quindi considerando una delle prime definizioni di probabilità, e cioè il numero di casi possibili fratto il numero di casi favorevoli, ne verrà che la probabilità di scegliere a caso una coppia di lettere uguale è:

$$\frac{\sum_{i=1}^{26} \frac{n_i(n_i-1)}{2}}{\frac{n(n-1)}{2}} = \frac{\sum_{i=1}^{26} n_i(n_i-1)}{n(n-1)}.$$

E questo per definizione, coincide con I=indice di coincidenza.
Torniamo quindi al metodo per determinare la lunghezza l della chiave: consideriamo una tabella in cui nella colonna i-esima vengono scritte le lettere che occupano il posto $i,\ l+i,\ 2l+i$ ... (cioè tutte le lettere che sono cifrate con la stessa lettera della parola chiave), uno studio di questo permetterà il calcolo di I e conseguentemente di l.
Osserviamo che ogni colonna corrisponde ad un cifrario monoalfabetico e quindi la probabilità di trovare una coppia di lettere uguali nella stessa colonna è di 0,075 mentre per colonne diverse scende, supponiamo al minimo e cioè 0,038.
Sia poi n il numero di lettere del testo cifrato, allora ogni colonna ha $\frac{n}{l}$ lettere; scegliamo a caso una lettera tra n possibilità, questa mi identifica la colonna di appartenenza in cui avrò $\frac{n}{l}-1$ modi per scegliere una seconda lettera, cioè il numero di coppie di lettere nella stessa colonna è:

$$NU = n\frac{\frac{n}{l}-1}{2} = \frac{n(n-l)}{2l};$$

e rispettivamente il numero di coppie che sono in colonne diverse è

$$ND = n\frac{n-\frac{n}{l}}{2} = \frac{n^2(l-1)}{2l}.$$

Quindi il numero di coppie di lettere uguali è: $A = NU * 0,075 + ND * 0,038$ e di conseguenza la probabilità (intesa come in precedenza) che una coppia casuale contenga due lettere uguali è

$$P = \frac{A}{\frac{n(n-1)}{2}} = \frac{0,037n}{l(n-1)} + \frac{0,038n-0,075}{n-l}.$$

Ma allora poichè per definizione $P \approx I$ e per quanto visto sopra:

$$I = \frac{\sum_{i=1}^{26} n_i(n_i-1)}{n(n-1)},$$

ne viene che

$$l = \frac{0,037n}{(n-1)I - 0,038n + 0,075}.$$

Questo numero non sarà sicuramente un intero ma fornirà un ordine di grandezza che mi permetterà di stabilire quale, tra le possibili l determinate con metodo di Kasiski è quella esatta; così facendo avrò determinato l con una sicurezza piuttosto elevata.

Una volta trovata la lunghezza della chiave il più è fatto, infatti ora determinare il testo in chiaro è molto più facile; basta considerare la tabella costruita sopra e vedere in ogni colonna quale è la lettera più frequente (a meno di considerazioni se sono presenti più lettere ad alta frequenza) e questa corrisponderà alla lettera più frequente dell'alfabeto usato; la loro differenza darà il primo elemento della chiave; procedendo così per ogni colonna si otterrà l'intera chiave. Facciamo un piccolo esempio.

Esempio:
Supponiamo di avere un testo cifrato e di avere già calcolato la lunghezza della chiave $l = 5$. Consideriamo poi la prima colonna della tabella di cui sopra e cioè consideriamo tutte le lettere di posto 1,6,11 ... con il numero di volte in cui compaiono:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	0	7	1	1	2	9	0	1	8	8	0	0
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	0	4	5	2	0	3	6	5	1	0	1	0

Tabella 3.3: Trovare la chiave nel cifrario di Vigénere

Quindi la lettera più frequente è la G che corrisponderà alla lettera più frequente (nell'alfabeto inglese) e, allora la prima lettera della chiave sarà 2=c.

Ovviamente più l è piccolo più facile è decrittare questo codice; per questo è così importante l'intuizione di Vernam, cioè un crittosistema in cui la chiave è lunga quanto il testo (teoricamente infinita) e non è mai ripetuta (per questo spesso si parla di sistema OTP, one-time pad); si dovrà poi a Shannon, nel 1949, la dimostrazione che questo crittosistema è teoricamente inattaccabile.

3.2 Cifrario di Vernam

Nel 1917 Gilbert S. Vernam era un giovane ingegnere che lavorava alla American Telephone & Telegraph Company (AT&T) nella sezione dedicata alla telegrafia a stampa diretta; il problema di cui si stava occupando allora era quello della sicurezza di questo metodo.
L'idea di Vernam era quella di basare la protezione su un sistema crittografico la cui principale caratteristica era quella di "combinare" testo in chiaro e chiave.
Possiamo vedere questo metodo in due modi diversi ma tra loro equivalenti;

il primo e il più semplice è quello di vedere il metodo di Vernam come un procedimento che somma la frase da criptare alla chiave (associando come al solito ad ogni lettera il corrispondente numero secondo lo schema: a=0, b=1...).
Il secondo modo di vedere il metodo è quello di sfruttare l'operatore logico XOR; ogni carattere del testo in chiaro viene rappresentato mediante 5 unità (che sono tradizionalmente 0 o 1, cioè la presenza o l'assenza di un impulso elettrico), quindi in totale si hanno $2^5 = 32$ diverse combinazioni che corrispondono alle lettere dell'alfabeto e ad altri simboli di punteggiatura.
Una volta fatto questo e interpretata anche la chiave in questo modo, si sommano le due sequenze di 0, 1 ottenute secondo le regole del codice binario (senza riporti) ovvero:
-1+1=0
-0+0=0
-1+0=0+1=1
Facciamo un esempio in entrambi i modi:

Esempio:
(primo modo) supponiamo di voler criptare il messaggio "hello", allora procederemo come segue: (i calcoli sono fatti tutti mod 26)

testo in chiaro	h	e	l	l	o
testo in chiaro(numerico)	7	4	11	11	14
chiave	x	m	c	k	l
chiave(numerica)	23	12	2	10	11
testo cifrato(numerico)(somma)	30	16	13	21	25
testo cifrato	e	q	n	v	z

Tabella 3.4: Primo metodo di cifratura

(secondo modo) supponiamo di voler criptare la lettera a (a=11000), allora procederemo come segue:

testo in chiaro	1	1	0	0	0
chiave	1	0	0	1	1
testo cifrato(somma binaria)	0	1	0	1	1

Tabella 3.5: Secondo metodo di cifratura

La realizzazione ingegneristica di questo cifrario è basata sulla tecnica del nastro di carta perforato; una macchina, in grado di leggere due nastri perforati in entrata (chiave e testo in chiaro) combinarli nel modo scritto sopra e

dare in uscita il nastro perforato del corrispondente testo criptato; viceversa ma sempre con la stessa macchina, dando in input testo da decifrare e chiave, ne usciva in output il testo in chiaro.

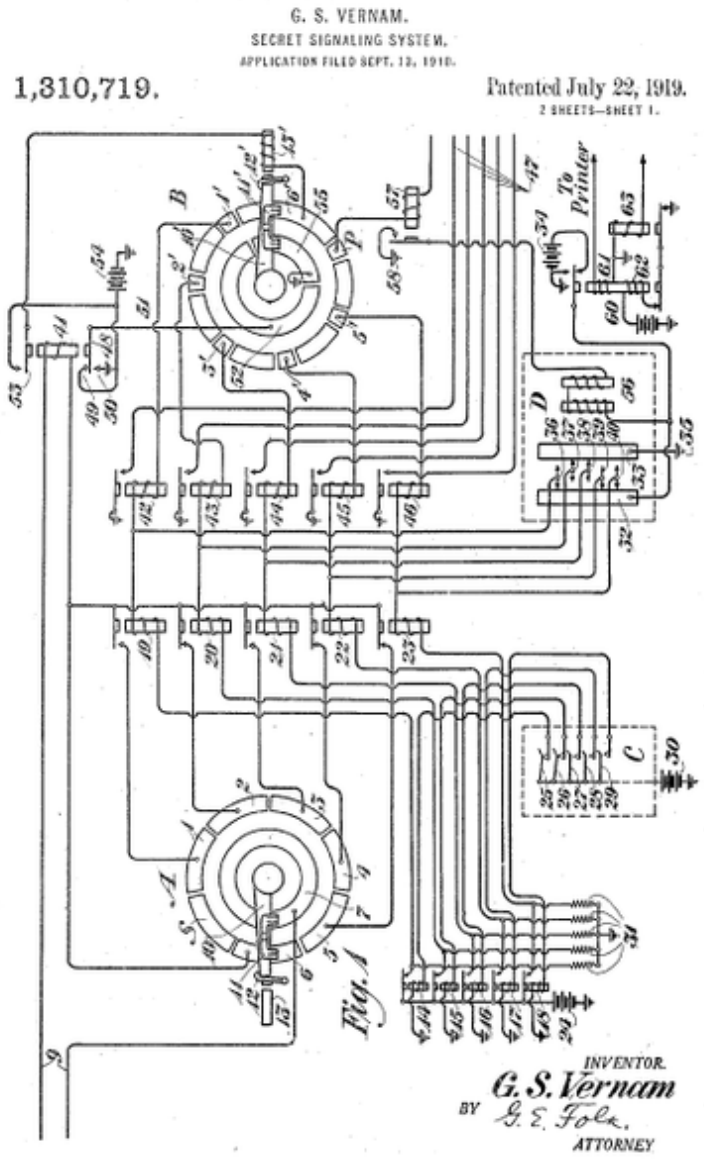

Figura 3.4: La macchina di Vernam

Si deve a Vernam anche l'aver completamente automatizzato, e quindi eliminato l'intervento umano, in questa catena di comunicazione; questo quindi

è un primo passo verso la moderna e completa tecnologizzazione di tutto il processo.
Invertendo il procedimento, per decriptare un codice basta sottrarre al testo cifrato la chiave, ragionando come sopra.
Nei primi tempi le chiavi avevano la forma di un ciclo di nastro di carta perforato con sequenze di 0,1 casuali; quindi ogni chiave passava attraverso la macchina ad intervalli regolari, permettendo facilmente a terze parti di trovare la chiave con l'analisi delle frequenze del metodo Kasiski.
Si provò a risolvere questo problema allungando di molto la chiave, ma ovviamente questa diventava allora molto difficile da maneggiare nelle macchine; si deve però a J. O. Mauborgne (un ufficiale dell'esercito) la risoluzione di questo problema.
Egli capì che per evitare questi problemi la chiave doveva essere infinita, senza senso e completamente casuale (random), e da qui viene il nome OTP.
Ecco che interviene finalmente l'infinito; il suo ruolo non solo è centrale per permettere alla macchina di essere completamente efficiente ma anche perchè, come dimostrerà Shannon, grazie alle ipotesi di cui sopra, questo sistema è completamente sicuro in teoria ed in pratica, ed è anche il solo ad esserlo.

3.2.1 La teoria di Shannon

Introduciamo alcune nozioni preliminari di probabilità e di teoria dell'informazione.

Definizione 3.3 (probablità condizionata)**.**
Si definisce la probabilità condizionata di y rispetto a x (cioè la probabilità di y sapendo che vale x)

$$p_Y(y|x) = \frac{p_{X,Y}(x,y)}{p_X(x)}.$$

Definizione 3.4 (variabili indipendenti)**.**
Date X, Y variabili aleatorie, si dice che queste sono indipendenti se
$p_Y(y|x) = p_Y(y)$ cioè se la probabilità di y non varia sapendo quanto vale x.

Teorema 3.2.1 (Teorema di Bayes)**.**
Siano X,Y variabili aleatorie, allora vale che

$$p_X(x|y) = \frac{p_X(x)p_Y(y)}{p_Y(y|x)}.$$

Un concetto molto importante per le sue applicazioni alla teoria dell'informazione è quello di Entropia; intuitivamente si può definire l'Entropia come

la misura dell'incertezza di un certo risultato, ma diamone una definizione rigorosa.
Consideriamo le seguenti condizioni che deve soddisfare la misura dell'incertezza di un risultato che denotiamo con H:
1) H deve essere continua e funzione della distribuzione delle probabilità;
2)

$$H(\frac{1}{n},...,\frac{1}{n}) \leqslant H(\frac{1}{n+1},...,\frac{1}{n+1}),$$

$\forall n > 0$, cioè la misura dell'incertezza deve crescere al crescere del numero dei possibili esiti equiprobabili;
3) $\forall\ q,\ 0 < q < 1$ vale che

$$H(p_1,...,qp_j,(1-q)p_j,...,p_n) = H(p_1,...,p_j,...,p_n) + p_j H(q,(1-q)),$$

cioè se un esito presenta due possibili casi allora la misura dell'incertezza aumenta ed è data dall'incertezza del valore p_j e da quella causata dalla presenza dei due casi.

Uno dei maggiori esponenti della crittografia classica, Claude Shannon, formulò il seguente teorema:

Teorema 3.2.2.
Sia $H(x)$ una funzione che soddisfi le proprietà di cui sopra, allora

$$H(p_1,...,p_n) = -\lambda \sum_k p_k log_2(p_k),$$

e $H(x) \geqslant 0$, con λ=costante positiva.

Quindi ne segue che possiamo assumere come misura dell'incertezza dell'esito di X:

$$H = -\sum_{x\in X} p(x) log_2(p(x)) \geqslant 0.$$

Un'altra interpretazione dell'entropia vede questa grandezza come il numero di domande vero/falso da porre per conoscere l'esito di un esperimento; di conseguenza in crittografia si può immaginare che l'entropia rappresenti la difficoltà di ricavare informazioni contenute in messaggi che occorre decifrare, si può pensare ad esempio a come ottenere una chiave.
Diamo ora alcune ulteriori definizioni e proprietà relative all'entropia.

Definizione 3.5 (entropia congiunta)**.**

$$H(X,Y) = -\sum_{x\in X}\sum_{y\in Y} p_{X,Y}(x,y) log_2(p_{X,Y}(x,y)),$$

cioè l'entropia relativa all'incertezza della variabile $Z = (X,Y)$.

Definizione 3.6 (entropia condizionata)**.**

$$H(Y|X) = -\sum_{x\in X}\sum_{y\in Y} p_{X,Y}(x,y) log_2(p_Y(y|x)),$$

cioè l'entropia relativa all'incertezza di Y una volta noto il valore assunto da X.

Questa definizione è di immediata deduzione infatti:

$$H(Y|X) = \sum_{x\in X} p_X(x) H(Y|X=x) = -\sum_x p_X(x)(\sum_y p_Y(y|x) log_2(p_Y(y|x)),$$

per la definizione di probabilità condizionata

$$H(Y|X) = -\sum_{x\in X}\sum_{y\in Y} p_{X,Y}(x,y) log_2(p_Y(y|x)).$$

Teorema 3.2.3 (regola della catena)**.**

$$H(X,Y) = H(X) + H(Y|X),$$

cioè l'incertezza dell'evento congiunto è data dall'incertezza su X sommata all'incertezza su Y noto il valore assunto da X.

Dimostrazione.

$$H(X,Y) = -\sum_{x\in X}\sum_{y\in Y} p_{X,Y}(x,y) log_2(p_{X,Y}(x,y)) =$$

$$= -\sum_{x\in X}\sum_{y\in Y} p_{X,Y}(x,y) log_2(p_X(x) p_Y(y|x)) =$$

$$= -\sum_{x\in X}\sum_{y\in Y} p_{X,Y}(x,y) log_2(p_X(x)) - \sum_{x\in X}\sum_{y\in Y} p_{X,Y}(x,y) log_2(p_Y(y|x)) =$$

$$= -(\sum_{x\in X} log_2(p_X(x)) \sum_{y\in Y} p_{X,Y}(x,y)) + \ H(Y|X) =$$

$$= -(\sum_{x\in X} (p_X(x)) log_2(p_X(x)) + \ H(Y|X) = H(X) \ + \ H(Y|X).$$

□

Proposizione 3.2.4. *Valgono le seguenti tre proprietà di H:*
1)

$$H(X) \leqslant log_2(n),$$

dove n è il numero dei possibili esiti di x; vale l'uguaglianza se tutti gli esiti possibili sono equiprobabili (questo significa che la massima entropia si ha per distribuzione di probabilità uniforme)
2)

$$H(X,Y) \leqslant H(X) + H(Y),$$

e vale l'uguaglianza solo nel caso in cui X, Y siano indipendenti
3)

$$H(Y|X) \leqslant H(Y),$$

e vale l'uguaglianza solo nel caso in cui X, Y siano indipendenti (questo significa che il condizionamento riduce l'entropia, cioè X può dare solo informazioni su Y, non accrescere la sua incertezza).

Il risultato 3), nonchè il più importante, discende dalla regola della catena e dal punto 2), infatti:

$$H(X) + H(Y|X) = H(X,Y) \leqslant H(X) + H(Y).$$

Mostriamo ora che OTP ha sicurezza perfetta (o assoluta); per fare questo ci poniamo alcune domande: dati come al solito P, C, K (con la scelta di K indipendente dalla scelta di P), ci chiediamo quanto vale $H(K|C)$ e soprattutto se $H(K|C) < H(K)$.

Definizione 3.7 (crittosistema a segretezza assoluta)**.** Un crittosistema si dice avere sicurezza perfetta se $H(P|C) = H(P)$.

Facciamo un esempio in cui questo non accade:

Esempio:
Siano $P = a, b, c$ $C = u, v, w$ $K = k_1, k_2$ con:

$$p(a) = 0,5,\ p(b) = 0,3,\ p(c) = 0,2;$$

$$p(k_1) = p(k_2) = 0,5 \text{ } e \text{ } P, K \text{ } indipendenti.$$

Sia poi e_k la funzione di cifratura rispetto alla chiave k t.c.:

$$e_{(k_1)}(a) = u,\ e_{(k_1)}(b) = v,\ e_{(k_1)}(c) = w;$$

$$e_{(k_2)}(a) = u,\ e_{(k_2)}(b) = w,\ e_{(k_2)}(c) = v.$$

Posta $p_C(u)$=probabilità che il testo cifrato sia u:

$$p_C(u) = p_K(k_1)p_P(a) + p_K(k_2)p_P(a) = (0,5)(0,5) + (0,5)(0,5) = 0,5.$$

Analogamente $p_C(v) = 0,25$, $p_C(w) = 0,25$.
Calcoliamo ora $p(b|v)$, ricordando la definizione:

$$p(b|v) = \frac{p_{P,C}(b,v)}{p_C(v)} = \frac{p_{P,K}(b,k_1)}{p_C(v)};$$

poichè abbiamo assunto che P e K fossero indipendenti

$$p(b|v) = \frac{p_P(b)p_K(k_1)}{p_C(v)} = \frac{(0,3)(0,5)}{0,25} = 0,6.$$

Analogamente

$$p(a|w) = p(a|v) = 0;\ p(c|v) = 0,4\ p(c|w) = p(c|w) = 0,4;\ p(b|w) = 0,6.$$

Possiamo quindi ora calcolare le entropie che ci interessano ricordando le definizioni.

$$H(P) = -(0,5log_2(0,5) + 0,3log_{0,3}(0,5) + 0,2log_2(0,2)) = 1,485.$$
$$H(P|C) = -\sum_{x\in P}\sum_{y\in C} p(x|y)log_2(p(x|y))) = 0,485.$$

Perciò in questo esempio, conoscere il testo cifrato riduce notevolmente l'incertezza del testo in chiaro. Proviamo che per OTP questo non succede.

Teorema 3.2.5 (Shannon 1949)**.**
OTP ha sicurezza assoluta.

Dimostrazione. Consideriamo quindi un cifrario OTP con alfabeto
$\mathbb{Z}_2 = \{0,1\}, P = C = K = \{0,1\}^l$ dove l è un intero che mi dà la lunghezza di P, C, K ed assumiamo che le chiavi siano casuali e quindi tutte con uguale probabilità cioè $p(k) = \frac{1}{2^l}\ \forall k \in K$.
Dato allora il testo cifrato $c \in C$ e ricordando che P, K sono indipendenti,

$$p_C(c) = \sum_{x\in P, k\in K, e_k(x)=c} p_P(x)p_K(k) = \frac{1}{2^l}\sum_{x\in P, k\in K, e_k(x)=c} p_P(x).$$

Poichè ad ogni messaggio in chiaro e messaggio cifrato corrisponde una sola chiave t.c. $e_k(x) = c$, ogni x compare nella sommatoria una sola volta e

quindi basta ridurre l'indice della sommatoria a $x \in P$ e ricordare che la somma delle probabilità di tutti i possibili testi in chiaro è 1, cioè:

$$p_C(c) = \frac{1}{2^l} \sum_{x \in P} p_P(x) = \frac{1}{2^l}.$$

Questo mi dice semplicemente che tutti i testi cifrati sono equiprobabili; passiamo ora al calcolo delle entropie.
Per quanto appena visto tutte le 2^l possibilità per K, C sono equiprobabili e quindi

$$H(K) = H(C) = log_2(2^l) = l.$$

Calcoliamo ora $H(P, K, C)$ in due modi differenti:
poichè C è univocamente determinato da P, K:

$$H(P, K, C) = H(P, K),$$

poichè P, K sono indipendenti

$$H(P, K, C) = H(P) + H(K),$$

e inoltre vale anche che

$$H(P, K, C) = H(P, C) = H(P|C) + H(C).$$

Uguagliando ora i due termini e ricordando che $H(K) = H(C)$ ne verrà che

$$H(P) = H(P|C),$$

e questo per definizione prova che il sistema ha sicurezza perfetta. □

Questo risultato permette in realtà di enunciare un teorema più generale

Teorema 3.2.6. *Dato un crittosistema con n chiavi equiprobabili con probabilità* $\frac{1}{n}$ *e t.c. per ogni* $x \in P$, $c \in C$ *c'è una ed una sola chiave k t.c.* $e_k(x) = c$*; allora questo sistema ha sicurezza perfetta.*

Ad esempio, uno dei cifrari più usati attualmente è RSA (algoritmo crittografico a chiave pubblica) non è un cifrario a sicurezza assoluta; infatti disponendo di tempo sufficiente posso decifrare tutti i testi cifrati possibili fino a trovare p.
L'entropia ovviamente non tiene in considerazione il tempo di calcolo, ma RSA proprio per la complessità computazionale della fattorizzazione è comunque ritenuto sicuro.

In conclusione abbiamo mostrato come grazie all'introduzione di una chiave teoricamente infinita e irripetibile, il cifrario di Vernam sia l'unico, anche a fronte di cirari più moderni come RSA, ad avere sicurezza assoluta; cioè anche in crittografia l'infinito ha un ruolo centrale e insostituibile.

Bibliografia

[1] Ermanno Lanconelli, *Lezioni di analisi matematica 1.* Pitagora editrice,Bologna 2° edizione, 1998.

[2] Ermanno Lanconelli, *Lezioni di analisi matematica 2, seconda parte.* Pitagora editrice,Bologna 1° edizione, 1997.

[3] Wade Tappe, Lawrence C. Washington, *Crittografia, con elementi di teoria dei codici.* Pearson Prentice Hall, 2° edizione, 2009.

[4] Douglas R. Stinson, *Cryptography, theory and practice.* CRC press, 1956.

[5] David Kahn, *The codebreakers, the story of secret writing.* Scribner, New York 2nd edition, 1996.

[6] Luigia Berardi, Albert Beutelspacher, *Crittologia. Come proteggere le informazioni riservate.* Franco Angeli, quaderni di informatica 1996.

Siti consultati

[7] http://quod.lib.umich.edu/cgi/t/text/pageviewer-idx?c=umhistmath;cc=umhistmath;sid=603f716ffce17415c213a8103432af51;rgn=full%20text;idno=ABW0362.0001.001;view=pdf;seq=00000283

[8] http://www.matematicahtml.altervista.org/pi.html

[9] http://ebookspdfs.org/read/

[10] http://www.vialattea.net/pagine/infinito/index.html#somm

[11] http://xoomer.virgilio.it/meno.uno_in.matematica/Infinito%20nella%20matematica.pdf

[12] http://progettomatematica.dm.unibo.it/

[13] http://en.wikipedia.org/wiki/Koch_snowflake

[14] http://www.miorelli.net/frattali/matematica.html

[15] http://www.frattali.it/index.html

[16] http://it.wikipedia.org/wiki/Frattale