In copertina sono rappresentati un cerchio di raggio 1 ed un quadrato di lato $\sqrt{\pi}$: le due figure hanno la stessa area.

Indice

Presentazione **xiii**

Introduzione **xvii**

1 Lo sviluppo decimale **1**
1.1 Sviluppi decimali 1
1.1.1 Esistenza degli sviluppi decimali 3
1.1.2 Sviluppi periodici 5
1.1.3 Unicità degli sviluppi decimali 9
1.2 Un quadrato è equipotente ad un intervallo 11

2 Frazioni continue **15**
2.1 Frazioni continue finite 15
2.2 Frazioni continue infinite 16
2.2.1 Le formule di Eulero 17
2.2.2 Frazioni continue e serie 22
2.3 Sviluppo in frazione continua dei razionali 26
2.3.1 Algoritmo euclideo della divisione 28
2.3.2 Doppia rappresentazione dei razionali 29
2.4 Sviluppo in frazione continua degli irrazionali 30
2.4.1 Esistenza degli sviluppi in frazione continua 30
2.4.2 Unicità degli sviluppi in frazione continua 36
2.5 Un quadrato è equipotente ad un intervallo 36
2.6 Esempi di applicazioni 37
2.6.1 Calcolo numerico 37
2.7 Le frazioni continue periodiche 38
2.8 La successione delle convergenti 45
2.9 Le frazioni intermedie ed il loro uso 47
2.9.1 Algoritmo per il calcolo delle convergenti 51

2.10 Sviluppi notevoli 55
2.10.1 Sperimentazioni con la DFT 59
2.11 Approssimazione diofantea 61
2.11.1 Migliori approssimazioni del II tipo 64
2.11.2 Migliori approssimazioni del I tipo 70
2.11.3 Approssimazione di $\sqrt{3}$ in Archimede 71
2.12 Calendari 75
2.12.1 La "misteriosa" frazione gregoriana 97/400 77
2.12.2 Il ciclo metonico ed il calendario ebraico 80
2.12.3 Il calendario islamico 80
2.13 Le convergenti come funzioni 82
2.13.1 Le convergenti di ordine 0 ed 1 82
2.13.2 La convergente di ordine 2 84
2.13.3 Le convergenti di ordine $k \geq 3$ 85

3 Approssimazione diofantea **89**
3.1 Teorema di Dirichlet 89
3.2 Teorema di Liouville 94
3.2.1 I numeri trascendenti di Liouville 96
3.3 Teorema di Hurwitz–Borel 98
3.4 Cenni al Teorema di Roth 102

4 Da Hermite a Lindemann **107**
4.1 Premesse 107
4.2 Se $r \neq 0$ è razionale, e^r è irrazionale 108
4.3 π^2 è irrazionale 111
4.4 Se $r \neq 0$ è razionale, $\cos(r)$ è irrazionale 115
4.5 Il numero di Nepero e è trascendente 119
4.6 π è trascendente 123
4.6.1 Calcolo con riga e compasso 123
4.6.2 Numeri costruibili 123
4.6.3 Trascendenza di π 124

A Complementi di Analisi matematica **141**
A.1 Il numero di Nepero 141
A.1.1 Sulla definizione di e, delle funzioni esponenziale e logaritmo 144
A.1.2 Introduzione del logaritmo tramite l'integrale 144
A.1.3 Introduzione dell'esponenziale tramite una serie 147

A.1.4 L'esponenziale come soluzione di un'equazione differenziale 149
A.1.5 L'approccio classico 150
A.2 Pi greco 155
A.2.1 Archimede e π 156
A.2.2 Il prodotto infinito di Viète 157
A.2.3 Il prodotto infinito di Wallis 160
A.2.4 Altri modi di definire π 161
A.2.5 L'esponenziale in campo complesso 164

B Compendio di Algebra **167**
B.1 La divisione euclidea. MCD di due interi 167
B.2 Strutture algebriche: definizioni 170
B.3 Estensione di un campo 178
B.3.1 Estensione semplice 182
B.3.2 Estensioni algebriche 185
B.3.3 Il caso dell'estensione quadratica 191
B.3.4 Campo di riducibilità completa di un polinomio 191
B.3.5 Campo di spezzamento del polinomio $x^n - 1 \in \mathbb{Q}[x]$ . . 194
B.4 L'algebra della riga e del compasso 195
B.4.1 Punti costruibili 196
B.4.2 Caratterizzazione algebrica dei punti costruibili 197
B.4.3 Problemi classici non costruibili con riga e compasso . . 201
B.4.4 Costruibilità dei poligoni regolari e numeri primi di Fermat 203

Elenco delle figure

2.1 La definizione delle frazioni continue in Lagrange (1798) 18
2.2 La dimostrazione di Eulero (1744a) delle formule di ricorrenza . 19
2.3 Le frazioni intermedie 48
2.4 Pseudo–codice dell'algoritmo del Corollario 2.9.1 53
2.5 Spettri delle trasformate discrete di Fourier 60
2.6 Miglior approssimazioni di π 71
2.7 Grafico di $c_1(x)$ su $[0,1]$ 83
2.8 Grafico di $c_2(x)$ su $[0,1]$. 85
2.9 Parti diverse del grafico di $c_2(x)$, su vari intervalli 86
2.10 Grafico di $c_3(x)$ su $[0,1]$ 86

3.1 La cubica $x^3 - 5y^3 = 2048$ e due suoi punti interi 105
3.2 Le cubiche $x^3 - 7y^3 = 32768$ e $x^3 - 19y^3 = 262144$ 106

4.1 Grafico di $f(x) = (1/10!)\, x^{10}(1-x)^{10}$ 110

Elenco delle tabelle

2.1 Frazione di Rogers–Ramanujan 27
2.2 Sviluppo in frazione continua di $\alpha = 43200/10463$ 29
2.3 Sviluppo in frazione continua di $\alpha = 314159265358/100000000000$ 34
2.4 I calcoli del bottaio. 63
2.5 Migliori approssimazioni del II tipo di $\alpha = \sqrt{5}$ 64
2.6 Migliori approssimazioni del II tipo di $a' = 5^h 49' 16''$ 79

4.1 Valori di $f^{(j)}(0)$ per $0 \leq j \leq 26$ 112

Presentazione

Anche il cosiddetto uomo della strada, per quanto "anumerato", ha sentito parlare nella sua vita del numero π, e magari pensa che valga esattamente 3,14. Probabilmente conosce anche l'espressione "quadratura del cerchio", per dire metaforicamente che qualcosa è impossibile. Infine può darsi che abbia sentito parlare della riforma gregoriana del calendario, che pose termine al calendario giuliano e vagamente ricorda che questa è legata a un computo complesso degli anni bisestili: per esempio potrebbe avere sentito dire alla TV alla fine del 1999 che il 2000 sarebbe stato un anno bisestile, a differenza degli anni "secolari", come il 1900 o il 1800. Alla scuola media avrà visto gli allineamenti decimali dei numeri, per cui ad esempio è $1/3 = 0,3333\ldots$ Se poi ha frequentato una scuola superiore avrà incontrato almeno un altro numero famoso: e. Tutto questo per dire che alcuni oggetti matematici o eventi storici legati a proprietà matematiche fanno parte del bagaglio minimo di conoscenze e ricordi di tutti quanti, un po' come i nomi di Garibaldi o di Verdi.

A fronte di questo, è curioso che anche persone dotate di cultura matematica, ad esempio laureati in matematica, mediamente abbiano una conoscenza abbastanza superficiale di alcuni teoremi e metodi matematici rilevanti che stanno dietro a tali oggetti o eventi. E questo non per colpa loro ma per alcune lacune che compaiono, sempre con le dovute eccezioni, nei programmi usuali della formazione di base dei nostri laureati in matematica. Ciò ha conseguenze anche per l'insegnamento nelle scuole secondarie superiori: alcuni argomenti matematici affascinanti e legati alle conoscenze di base prima ricordate, non entrano nelle nostre aule liceali, anche se vi potrebbero essere trattati con una certa facilità e con il sicuro interesse degli allievi. Il risultato è che moltissimi, anche con una cultura scientifica avanzata, su questi temi rimangono al livello primordiale dell'uomo della strada. Il fenomeno affonda le sue radici in una tradizione antica: come ricordano gli autori di questo volume, già J.L. Lagrange nel 1774 lamentava l'esistenza di queste lacune addirittura nei matematici, che conoscevano in pochi la teoria delle frazioni continue. Come sottolinea il sottotitolo di questo libro, c' è una matematica elementare "dimenticata" da molti, frutto di ricerche sviluppatesi a partire dal Sei-Settecento e che ha

prodotto alcuni importanti teoremi di matematica avanzata, dimostrati alcuni nella seconda metà del secolo XIX da Hermite e Lindemann, altri nella prima metà del secolo successivo da Thue, Siegel e Roth, che per questo vinse la medaglia Fields nel 1958.

Il libro di G. Caristi, C. Fiori e S. Invernizzi vuole colmare proprio queste lacune culturali e lo fa presentando sia la parte teorica più elementare, ma non perciò meno importante, che è alla base di queste conoscenze mancanti, sia la parte più avanzata di tali argomenti. Pertanto presenta dapprima le frazioni continue (cap. 2), tema che potrebbe entrare benissimo nei curricoli della scuola secondaria e poi, capitalizzando quanto percorso nel capitolo, introduce vari teoremi classici sulle approssimazioni diofantee, dovuti a Dirichlet, Liouville e altri (cap. 3), nonché le dimostrazioni dapprima dell'irrazionalità, poi della trascendenza di e e π, dovute a Hermite e Lindemann (cap. 4).Sono questi risultati a legare gli argomenti che anche l'uomo della strada ricorda a profondi risultati e metodi matematici. Come ci ricorda la citazione di Bombieri posta all'inizio dell'Introduzione al volume, sono risultati moderni che hanno un eccezionale valore storico e importanti conseguenze filosofiche: il risultato di Lindemann (1882), ad esempio, prova che con gli strumenti della geometria euclidea è impossibile quadrare il cerchio.

Molti sono i pregi di quest'opera: soprattutto il felice equilibrio tra un'esposizione rigorosa e precisa e la ricchezza di esempi numerici, che rendono comprensibili i passaggi più ardui delle dimostrazioni formali. Si può dire che tali esempi costituiscono un viaggio culturalmente ricchissimo attraverso i numeri più famosi e comuni che si incontrano a scuola (da $\sqrt{3}$ a $\sqrt{5}$, da π a e, e così via). Ma nella tradizione scolastica questi numeri emergono spesso come strane e a volte misteriose icone di un panorama "matematico" arido e povero, tra la razionalizzazione di un'espressione e la risoluzione routinaria di un'equazione di secondo grado (quante volte ho chiesto ai miei studenti di matematica perché si sceglie π come misura dell'angolo piatto e mi sono trovato di fronte a una sconsolante scena muta). In questo volume, al contrario, essi sono l'illustrazione di contenuti teorici, algoritmici e numerici di un'estrema ampiezza e profondità. Il lettore è accompagnato per mano lungo un itinerario dove ritroverà tutti i numeri che aveva incontrato nella sua vita matematica di liceale, ma immersi in questo nuovo entusiasmante panorama. Acquisterà così il senso matematico che questi numeri hanno e ripercorrerà con un nuovo spirito vecchi itinerari. Ad esempio, il tema degli allineamenti periodici, nel contesto delle frazioni continue, diventa l'oggetto degli interessanti teoremi di Lagrange sugli irrazionali quadratici. Analogamente le tecniche di approssimazione dei numeri irrazionali sono spiegate con tutto lo spessore numerico e teorico che

le approssimazioni diofantee danno loro, introducendo ad esempio la nozione di buona o cattiva approssimazione. Un altro aspetto molto interessante del volume è lo sforzo di inquadrare storicamente i contenuti matematici che si incontrano, mettendo in luce da un lato il progredire delle idee e delle tecniche da un ricercatore all'altro (per es. da Liouville a Roth in un secolo di scoperte e miglioramenti); dall'altro l'intreccio con eventi storici esterni alla matematica. Per esempio un certo numero di pagine è dedicato ai vari calendari presenti e passati: molti sanno che il calendario gregoriano ha sostituito quello giuliano, come pure che islamici e israeliti hanno un calendario diverso dal nostro, ma quasi nessuno (ricordo come eccezione il volume di G. Peano, Giochi di aritmetica e problemi interessanti. Paravia, Torino, 1925) ha affrontato questi argomenti inquadrando il problema da un punto di vista matematico. Due ricche ed utilissime appendici riassumono i concetti analitici e algebrici che eventualmente il lettore non ricordi e che sono usati nei vari capitoli. Inoltre il primo capitolo è un'utilissima introduzione agli allineamenti decimali dei numeri reali, altro argomento tipicamente poco noto o malamente digerito dai più.

Per tutti questi motivi il volume sarà di utilissima lettura agli insegnanti di matematica (compresi i colleghi dell'università: magari si sentiranno invogliati a parlare di frazioni continue nei loro corsi, posto che già non lo facciano) e agli studenti di questa disciplina: ne usciranno arricchiti culturalmente e professionalmente.

Ferdinando Arzarello

Introduzione

... la Théorie des fractions continues manque dans les livres ordinaires d'Arithmétique et d'Algèbre, et ... par cette raison, elle doit être peu connue des géomètres ...

Joseph–Louis Lagrange, 1774

... Lindemann nel 1882 dimostrò rigorosamente che è impossibile effettuare la quadratura del cerchio con costruzioni puramente geometriche e in particolare per mezzo della geometria euclidea. Un trionfo della matematica moderna, dato il suo significato storico e le sue conseguenze filosofiche.

Enrico Bombieri, 2006

I centocinquant'anni cui si allude nel titolo sono quelli che vanno dal *De fractionibus continuis* di Eulero del 1744 all'*Über die Zahl* π, pubblicato nel 1882 sui *Mathematische Annalen* da Ferdinand von Lindemann. In questo secolo e mezzo, nella matematica sono stati fatti enormi progressi, che certamente non sono stati "dimenticati" nella didattica: basti citare, per fare un solo esempio, le costruzioni formali e rigorose dei numeri reali sulla base della conoscenza dei numeri razionali, realizzate ad opera principalmente di Georg Cantor e di Richard Dedekind, e pubblicate nello stesso anno, il 1872. Il primo compito di quest'introduzione sarà quindi quello di giustificare la scelta, per certi versi ardita, di quell'aggettivo: dimenticata.

Inizieremo dal teorema di Lindemann. Come noto, questo afferma che π è trascendente sul campo $\mathbb{Q}$ dei numeri razionali, cioè che non esistono numeri

interi $b_0, b_1, b_2, \ldots, b_n$ $(\neq 0)$ tali che la somma $b_0 + b_1\pi + b_2\pi^2 + \ldots + b_n\pi^n$ sia uguale a zero, per quanto grande si prenda n. Questo risultato, definito da Enrico Bombieri "un trionfo della matematica moderna", implica in particolare che uno dei problemi classici della matematica greca, la quadratura del cerchio, non ha soluzione: è impossibile costruire con riga e compasso, seguendo le regole euclidee, il lato di un quadrato che abbia la stessa area di un cerchio di raggio uguale ad 1. Gli altri problemi classici presi quasi sempre ad esempio sono la duplicazione del cubo e la trisezione dell'angolo. Ma la matematica soggiacente alle soluzioni (positive o negative) di tali problemi è profondamente diversa. Lo studio della duplicazione del cubo e della trisezione dell'angolo, per esempio, si può svolgere senza uscire dall'ambito della teoria delle estensioni algebriche del campo razionale, mentre per la quadratura del cerchio la soluzione attualmente proposta passa per la trascendenza di π. Tipicamente, i testi di algebra dedicati alla teoria dei campi ed alla teoria di Galois riescono a dimostrare completamente l'irrisolubilità della duplicazione del cubo ed ad identificare quali siano i casi risolubili e quali no della trisezione dell'angolo, ma per la quadratura del cerchio di norma si limitano a sfruttare, senza dimostrarla, la trascendenza di π. È quindi così che nasce spontanea una domanda: ma quanto è difficile la dimostrazione di Lindemann? Veramente è "improponibile", anche a livello delle nostre lauree in matematica, incluse quelle dedicate all'insegnamento? Non sarebbe opportuno che chi studia matematica, o un futuro docente, vedesse o leggesse almeno una volta nella vita questa dimostrazione, se non altro per rendersi conto del livello della sua difficoltà e dell'itinerario storico che portò Lindemann ad essa?

Gli autori di questo volume sono convinti che la risposta all'ultima domanda debba essere affermativa. Il Capitolo 4 del volume offre così un percorso, completo nei dettagli, che porta dalle più semplici dimostrazioni dell'irrazionalità di e e di π, all'irrazionalità di π^2, alle dimostrazioni meno banali dell'irrazionalità di e^x, di $\cos(x)$ e di $\sin(x)$, se x è razionale $\neq 0$, conducendo così gradualmente al teorema di Hermite del 1873 che dimostra la trascendenza del numero e di Nepero, utilizzando strumenti di analisi matematica, in particolare le formula di integrazione per parti. Il teorema di Lindemann, di nove anni successivo, si basa completamente, *mutatis mutandis*, sulla tecnica usata da Hermite per e, ma con due differenze fondamentali che ne creano forse le maggiori difficoltà. La prima è che la trascendenza di π viene da Lindemann dimostrata nel campo $\mathbb{C}$ dei numeri complessi (in effetti Lindemann prova che $i\pi \in \mathbb{C}$ è trascendente su $\mathbb{Q}$) e quindi il "familiare" integrale $\int_a^b f(x)dx$ delle scuole superiori o del primo anno dell'università non basta e deve essere sostituito da un "integrale di linea" in $\mathbb{C}$. La seconda difficoltà è che è necessaria

una manipolazione algebrica di polinomi piuttosto pesante, che non serve nel caso di e. In particolare, per esemplificare questa seconda difficoltà, abbiamo inserito nella dimostrazione alcuni esempi–pilota con polinomi di grado "basso", esempi che possono essere gestiti, ricreati ed eventualmente estesi, da chi legge questo libro, con un qualunque sistema di computer algebra.

Proprio perché il Capitolo 4 è dedicato essenzialmente alla trascendenza di e e di π, alla fine del volume si trovano due appendici. Nella prima, l'Appendice A, si presentano in modo comparato i principali modi di introdurre le funzioni logaritmo, esponenziale e trigonometriche, nella convinzione che chi studia (o insegna) matematica deve essere conscio della possibilità di molteplici approcci a queste funzioni e delle loro origini storiche. L'Appendice B è un compendio di algebra inserito con un duplice obiettivo: da un lato fornire le definizioni e nozioni di algebra utili alla comprensione del testo, dall'altro dare una caratterizzazione algebrica dei punti costruibili con riga e compasso (anche per il loro legame con l'essere un numero reale algebrico o trascendente).

L'argomento sviluppato nel Capitolo 2 del testo è la teoria delle frazioni continue. Questo è forse davvero un argomento "dimenticato". Nell'ormai lontano 1993, al XV Convegno UMI–CIIM sull'insegnamento della matematica, Benedetto Scimemi si chiese: *perché le frazioni continue sono trattate con tanta negligenza nella nostra scuola superiore (e inferiore)?*, ed aggiunse: *perché le frazioni continue sono ignorate nell'Università?*[1] In effetti è strano che quasi tutti i testi sulle frazioni continue contengano od inizino con l'osservazione che questa bellissima ed utile teoria è del tutto trascurata nell'insegnamento. L'anno precedente, il 1992, Andrew M. Rockett e Peter Szüsz, autori di un testo fondamentale sull'argomento (1992, p. viii), avevano lamentato che la teoria delle frazioni continue non riceve l'attenzione che merita.[2] In precedenza, il matematico sovietico Aleksandr Khinchin, nella prefazione alla prima edizione del suo classico trattato sulla teoria delle frazioni continue (1964) aveva motivato la necessità di una monografia di base sull'argomento con il fatto che questa teoria, a suo tempo parte dei programmi di matematica delle scuole superiori, era stata cancellata da quei programmi e non faceva neppure parte dei curricula standard delle lauree universitarie in matematica.[3] In tempi

[1] Lo stesso Scimemi propose una possibile risposta: la matematica nelle nostre scuole ed università è troppo *dialettica* (ossia concentrata sulle dimostrazioni, sulla dualità vero/falso, sui risultati di esistenza ed unicità, "un raffinato esercizio intellettuale in cui il vero progresso è affidato alla mente superiore di pochi eletti") e poco *costruttiva*, o algoritmica ("quella che inventa e perfeziona procedure di calcolo, spesso suggerite da problemi pratici").

[2] The theory of continued fractions does not receive the attention it deserves.

[3] I feel that an elementary monograph on the theory of continued fractions is necessary because this theory, which formerly was a part of the mathematical program at the inter-

molto più recenti, Manfred Schroeder (2009, p. 73), nella più recente edizione del suo trattato sulla teoria dei numeri e delle sue applicazioni, può ancora confermare che le frazioni continue, pur essendo uno dei temi più affascinanti ed utili dell'aritmetica, sono ancora del tutto trascurate dalle nostre strutture scolastiche.[4] Hans Ivar Riesel (2012, Appendice 8) afferma che la teoria delle frazioni continue è un argomento affascinante ed estremamente utile, sia dal punto di vista teorico che da quello computazionale, ma che è alquanto trascurato nei corsi di matematica, e sul quale esistono solo pochissimi libri di base.[5]

Straordinario però è certamente il fatto che ad iniziare la lista delle "lamentele" fu addirittura Joseph–Louis Lagrange, che nelle *Additions aux éléments d'algèbre d'Euler* (Eulero, 1774, pp. 6–7) osservò che la teoria delle frazioni continue è poco conosciuta e merita maggiore diffusione.[6]

Come autori di questo volume, non possiamo esimerci da questa *doléance*. Per la situazione italiana concordiamo completamente con l'analisi di Benedetto Scimemi (1993): la matematica, sia nelle scuole secondarie che nelle università è diventata prevalentemente "strutturale": tuttavia questo innegabile progresso è purtroppo avvenuto a discapito dello studio di "casi singoli" o di teorie non facilmente classificabili nella lista delle "strutture".[7]

Ma in fondo non è questa la ragione che ci ha convinto a inserire in questo volume una trattazione di base della teoria delle frazioni continue, peraltro abbastanza ampia da includere i legami con l'approssimazione diofantea, la periodicità degli sviluppi, ed una trattazione, per certi versi poco nota, dell' origine dell'approssimazione di $\sqrt{3}$ in Archimede e delle scelte delle "misterio-

mediate level, has now been dropped from that program, and hence is no longer included in the new textbooks on elementary algebra. On the other hand, the curricula at the more advanced levels (even in the mathematics divisions of universities) also omit this theory. (Khinchin si riferisce naturalmente alla situazione delle scuole e dell'università nell'Unione Sovietica dei primi anni '50).

[4] Continued fractions are one of the most delightful and useful subjects of arithmetic, yet they have been continually neglected by our educational factions.

[5] In this Appendix we shall provide the reader with a glimpse at the theory of continued fractions. This is a fascinating and very useful theory, both theoretically and computationally. It is, however, a little neglected in mathematics courses, and there are only a few elementary books ... on the subject.

[6] ... la Théorie des fractions continues manque dans les livres ordinaires d'Arithmétique et d'Algèbre, et ... par cette raison, elle doit être peu connue des géomètres ....

[7] In un certo senso i grandi risultati della matematica non sono quelli che si appoggiano a potenti teorie preesistenti, ma quelli la cui dimostrazione richiede idee geniali e di norma un enorme numero di "passaggi" ben collegati, ciascuno dei quali, preso singolarmente, è tipicamente banale, come in un meraviglioso mosaico, nel quale ogni singola tessera è in fondo solo una banale pietruzza colorata.

se" frazioni 97/400 nella riforma del calendario di Gregorio XIII e 11/30 nel calendario islamico dell'Egira. La vera motivazione è che abbiamo ritenuto, in pieno accordo con i matematici succitati, che questa teoria sia davvero bellissima, e quindi, se la matematica è anche estetica, è qualcosa che non possa e non debba essere "dimenticata".

Il testo inizia con il Capitolo 1 dedicato agli sviluppi decimali. Si tratta ovviamente di un argomento notissimo. Tuttavia lo abbiamo incluso all'inizio sia per una comparazione fra lo sviluppo decimale e quello in frazione continua, che include una ricostruzione storica del carteggio Cantor–Dedekind che portò al famoso teorema di Cantor sull'esistenza di un'applicazione biiettiva fra un intervallo I ed il quadrato $I \times I$, sia perchè in questo tema esiste un argomento poco discusso, quello dell'unicità degli sviluppi decimali: in linea di principio *potrebbe* essere $\pi = 3.14159265358979323846264\ldots = 3.14158376999989567988895\ldots$. È solo l'abitudine, o l'idea che un numero reale *sia* il suo sviluppo decimale, che ci fa respingere come evidentemente assurda questa possibilità: in effetti c'è bisogno di una dimostrazione.[8]

Infine, il Capitolo 3 rappresenta virtualmente il *trait d'union* fra le frazioni continue ed i teoremi di trascendenza. Infatti, tramite i fatti di base della teoria dell'approssimazione diofantea, come il teorema di Liouville del 1844, è possibile dimostrare esplicitamente l'esistenza dei numeri trascendenti, senza ricorrere a dimostrazioni non costruttive basate sulle differenti cardinalità dei reali algebrici e di tutti i reali. Il Capitolo 3 include anche una dimostrazione completa del teorema di Hurwitz–Borel ed alcuni cenni al teorema di Roth, con qualche esempio numerico sul computo dei punti di coordinate intere su particolari curve cubiche piane.

Talvolta, all'interno di una dimostrazione particolarmente complessa dal punto di vista tecnico, vengono sviluppati degli esempi numerici illustrativi dei passaggi o dei ragionamenti eseguiti. Per distinguere tali esempi, utili dal punto di vista didattico ma formalmente estranei dalla dimostrazione vera e propria, essi verranno racchiusi fra il simbolo ▼ (che indica l'inizio dell'esempio) ed il simbolo ▲ (che ne indica la fine). Come di consueto, il "quadratino pieno" ■ indica la fine di una dimostrazione o di un'unità logica.

[8] E sinceramente sarebbe un fatto poco comprensibile se nelle lauree universitarie si discutesse di unicità degli sviluppi in serie di Taylor o di Fourier delle funzioni senza parlare precedentemente del problema dell'unicità degli sviluppi decimali dei numeri.

Ringraziamenti

Gli autori desiderano innanzitutto ringraziare Bruno D'Amore, per il suo fondamentale supporto ed incoraggiamento nella preparazione di questo testo, e Ferdinando Arzarello, per aver accettato di redigere la presentazione del lavoro. Ringraziamo anche, per il loro entusiasmo, per le loro osservazioni e soprattutto per la loro pazienza, gli studenti e le studentesse della laurea triennale in matematica dell'Università di Trieste, dove la versione "beta" di questo libro è stata sperimentata come testo per l'insegnamento di *Matematiche Complementari* negli aa.aa. 2010–2011 e 2011–2012. Infine, o come si usa dire, intraducibilmente, *last but not least*, vogliamo ringraziare la Pitagora Editrice–Tecnoprint, e specialmente, per la loro grande professionalità, disponibilità e gentilezza, Maura Sughi ed Antonella Valzania, senza il cui supporto tecnico quest'edizione probabilmente non sarebbe mai stata realizzata. A tutti auguriamo una buona lettura.

Gabriella Caristi
Carla Fiori
Sergio Invernizzi

Modena–Trieste, maggio 2012

Capitolo 1

Lo sviluppo decimale

1.1 Sviluppi decimali

Lo sviluppo decimale (o più in generale lo sviluppo in base $b > 1$) di un numero reale è uno di quegli argomenti ritenuti "ben noti" della matematica di base. Uno sviluppo decimale è una scrittura formale del tipo

$$a_0 \,.\, a_1 a_2 a_3 a_4 a_5 a_6 a_7 \ldots \tag{1.1}$$

dove $a_0 \geq 0$ è un intero e $(a_i)_{i\geq 1}$ è una successione di elementi dell'insieme $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, le *cifre decimali*.[1] Volendo essere più precisi, uno sviluppo decimale come (1.1) può essere definito come una coppia $(a_0, (a_i)_{i\geq 1})$ costituita da un numero intero $a_0 \geq 0$ e da una successione $(a_i)_{i\geq 1}$ di numeri interi tali che per ogni $i \geq 1$ sia $0 \leq a_i \leq 9$. Il problema didattico è quindi quello di determinare il legame fra le scritture formali (1.1) ed i numeri reali α positivi.[2]

La risposta a questa domanda dipende strettamente da cosa si ritiene sia un numero reale α, dipende cioè dalla definizione adottata per il sistema dei numeri reali. Ad esempio, se si adotta per i reali il modello classico delle sezioni di Dedekind del campo razionale $\mathbb{Q}$, la (1.1) è nient'altro che una "codifica" di una sezione (A', A'') di $\mathbb{Q}$ (Fiori e Invernizzi 2009, p. 93 segg.). In ogni caso però, qualunque sia il modello (o, *a fortiori*, se si assume direttamente una definizione assiomatica), alla fine il sistema $\mathbb{R}$ dei numeri reali è un *campo*

[1] In questo testo per separare la parte intera a_0 dalla parte frazionaria $a_1 a_2 a_3 a_4 a_5 a_6 a_7 \ldots$ usiamo un *punto*, seguendo la convenzione anglosassone; la convenzione italiana prevede l'uso di una virgola.

[2] Ci limitiamo ai numeri non negativi, visto che per i numeri negativi si aggiunge banalmente il segno meno allo sviluppo del loro valore assoluto.

ordinato completo (Fiori e Invernizzi 2009, p. 20). Ciò in conclusione consente in ogni caso di interpretare (1.1) come un numero reale. Infatti, data la (1.1), la struttura di campo consente di calcolare per ogni $n \geq 0$ i razionali:

$$\alpha_n = a_0 + \sum_{i=1}^{n} \frac{a_i}{10^i}$$

L'insieme di tali α_n è superiormente limitato dall'intero $a_0 + 1$: infatti,

$$\sum_{i=1}^{n} \frac{a_i}{10^i} \leq \sum_{i=1}^{n} \frac{9}{10^i} = \frac{\overbrace{99\ldots9}^{n}}{1\underbrace{00\ldots0}_{n}} \leq 1$$

e quindi, per la completezza, esiste l'estremo superiore $\alpha = \sup_{n\geq 0} \alpha_n$. Ma per il teorema sul limite delle successioni monotone prima, e per la simbologia delle serie numeriche poi, si può alla fine scrivere:

$$\alpha = \sup_{n\geq 0} \left\{ a_0 + \sum_{i=1}^{n} \frac{a_i}{10^i} \right\} = \lim_{n\to\infty} \left\{ a_0 + \sum_{i=1}^{n} \frac{a_i}{10^i} \right\} = a_0 + \sum_{i=1}^{\infty} \frac{a_i}{10^i} \qquad (1.2)$$

In conclusione, conviene d'ora in poi chiamare *sviluppo decimale* un numero reale del tipo (1.2). Le domande che nascono spontaneamente sono allora due:

Esistenza: l'insieme degli sviluppi decimali (1.2), ottenuti al variare dell'intero $a_0 \geq 0$ e della successione di cifre decimali $(a_i)_{i\geq 1}$, coincide con l'insieme di tutti i numeri reali $\alpha \geq 0$, o di questi ne resta fuori qualcuno? In altri termini: *ogni* numero reale $\alpha \geq 0$ può essere rappresentato nella forma (1.2)?

Unicità: due diversi sviluppi decimali possono coincidere con lo stesso numero reale? Se sì, in quali casi questo accade?

Iniziamo con dare risposta affermativa alla questione dell'esistenza.[3]

[3] Questa discussione può sembrare inutilmente accademica. Tuttavia ci sembra rilevante che il problema dell'esistenza e dell'unicità dello sviluppo decimale dei numeri *preceda* altri problemi analoghi, come quelli relativi agli sviluppi in serie (di potenze o di Fourier) delle funzioni.

1.1.1 Esistenza degli sviluppi decimali

Teorema 1.1.1 *Per ogni numero reale $\alpha \geq 0$ esistono un intero $a_0 \geq 0$ ed una successione di cifre decimali $(a_i)_{i\geq 1}$ tali che $\alpha = a_0 + \sum_{i=1}^{\infty} a_i/10^i$.*

Dimostrazione. Sia dato $\alpha \geq 0$. Utilizziamo la funzione *parte intera* $x \mapsto [x]$ che associa ad x il massimo intero $\leq x$. Poniamo per definizione:

$$\begin{aligned} a_0 &:= [\alpha] && (1.3)\\ a_1 &:= [10 \cdot (\alpha - a_0)] && (1.4)\\ a_2 &:= [100 \cdot (\alpha - \{a_0 + a_1/10\})] \\ &\dots \\ a_i &:= [10^i \cdot (\alpha - \{a_0 + \sum_{k=1}^{i-1} a_k/10^k\})] && (1.5)\\ &\dots \end{aligned}$$

In (1.3), a_0 è per costruzione un intero ≥ 0. Resta da provare che la successione $(a_i)_{i\geq 1}$ definita dalle (1.4)–(1.5) verifica per ogni $i \geq 1$ le disuguaglianze $0 \leq a_i \leq 9$. Procediamo per induzione. Dalla definizione di a_0 abbiamo $0 \leq \alpha - a_0 < 1$, per cui $0 \leq a_1 < 10$. Poi dalla definizione di a_1 abbiamo $0 \leq 10 \cdot (\alpha - a_0) - a_1 < 1$, cioè (dividendo per 10)

$$0 \leq \alpha - \{a_0 + a_1/10\} < 1/10$$

per cui $0 \leq a_2 < 10$. Supponiamo che $0 \leq a_{i-1} < 10$: ne viene che

$$0 \leq 10^{i-1} \cdot (\alpha - \{a_0 + \sum_{k=1}^{i-2} a_k/10^k\}) - a_{i-1} < 1$$

da cui, moltiplicando per 10

$$\begin{aligned} 0 &\leq 10^i \cdot (\alpha - \{a_0 + \sum_{k=1}^{i-2} a_k/10^k\}) - 10 \cdot a_{i-1} && (1.6)\\ &= 10^i \cdot (\alpha - \{a_0 + \sum_{k=1}^{i-1} a_k/10^k\}) < 10 && (1.7) \end{aligned}$$

e quindi

$$0 \leq [10^i \cdot (\alpha - \{a_0 + \sum_{k=1}^{i-1} a_k/10^k\})] < 10$$

il che implica che $0 \leq a_i < 10$.

Infine, dividendo la (1.7) per 10^i, e ponendo ivi $n = i - 1$, si ottiene

$$0 \leq \alpha - \{a_0 + \sum_{k=1}^{n} a_k/10^k\} < 10^{-n}$$

e quindi $\alpha = a_0 + \sum_{i=1}^{\infty} a_i/10^i$. ■

Osservazione 1.1.2 Nella rappresentazione di un numero reale non–negativo $\alpha = a_0 + \sum_{i=1}^{\infty} a_i/10^i$ (con $a_0 \geq 0$ intero e $(a_i)_{i\geq 1}$ una successione di cifre decimali) l'intero $a_0 = [\alpha]$ è, come si è visto, la *parte intera* di α, mentre $\sum_{i=1}^{\infty} a_i/10^i$ è la *mantissa* di α.[4]

È utile osservare subito che la procedura della dimostrazione del precedente Teorema 1.1.1 non può produrre tutte le possibili successioni di cifre. Si ha infatti:

Proposizione 1.1.3 *La successione* $(a_i)_{i\geq 1}$ *definita dalle* (1.4)–(1.5) *non può essere* 9*–periodica, cioè non può essere* $a_i = 9$ *da un certo indice* n *in poi.*

Dimostrazione. Supponiamo per assurdo che esista un indice $n \geq 1$ tale che per $i \geq n$ sia $a_i = 9$. Allora[5]

$$\begin{aligned}
\alpha &= a_0 + \sum_{i=1}^{\infty} a_i/10^i = \{a_0 + \sum_{i=1}^{n-1} a_i/10^i\} + \sum_{i=n}^{\infty} 9/10^i \\
&= \{a_0 + \sum_{i=1}^{n-1} a_i/10^i\} + (9/10^n) \underbrace{\sum_{i=0}^{\infty} 1/10^i}_{\|} \\
&= \{a_0 + \sum_{i=1}^{n-1} a_i/10^i\} + (9/10^n) \cdot (10/9) \\
&= \{a_0 + \sum_{i=1}^{n-2} a_i/10^i\} + a_{n-1}/10^{n-1} + 1/10^{n-1}
\end{aligned}$$

[4] Seguendo Peano (1906, p. 103, 159), il termine latino *mantissa* è di probabile origine etrusca e significa *aggiunta*; la sua introduzione in matematica è dovuta a Wallis (1693): "Ejusque partes decimales abscissas, *appendicem* voco, sive *mantissam*".

[5] Ricordiamo la formula della somma della serie geometrica di ragione r $(0 < |r| < 1)$: $\sum_{i=1}^{\infty} r^i = 1/(1-r)$. Per $r = 1/10$ si ha $\sum_{i=1}^{\infty} 1/10^i = 1/(1-1/10) = 10/9$ (Cecconi e Stampacchia 1974, p. 259).

Usando la definizione di a_{n-1} abbiamo:

$$\begin{aligned} a_{n-1} &:= [10^{n-1} \cdot (\alpha - \{a_0 + \sum_{i=1}^{n-2} a_i/10^i\})] \\ &= [10^{n-1} \cdot (a_{n-1}/10^{n-1} + 1/10^{n-1})] \\ &= [a_{n-1} + 1] = a_{n-1} + 1, \end{aligned}$$

un assurdo. ■

Osservazione 1.1.4 È utile osservare subito che se la successione $(a_i)_{i\geq 1}$ delle cifre è 9–periodica, ma non dalla prima cifra, cioè se si ha $a_i = 9$ per $i \geq n \geq 2$ opportuno, e se $a_{n-1} \leq 8$, allora, con le ovvie consuete notazioni:[6]

$$a_0.\, a_1 a_2 \ldots a_{n-1}\overline{9} = a_0.\, a_1 a_2 \ldots (a_{n-1} + 1)\overline{0}$$

mentre se la $(a_i)_{i\geq 1}$ è 9–periodica sin dalla prima cifra si ha:

$$a_0.\, \overline{9} = (a_0 + 1).\overline{0}$$

Infatti, nel primo caso si ha

$$\begin{aligned} a_0.\, \ldots a_{n-1} + \sum_{k=1}^{\infty} 9/10^{n-1+k} &= a_0.\, \ldots a_{n-1} + (9/10^n) \cdot \sum_{k=0}^{\infty} 1/10^k \\ &= a_0.\, a_1 \ldots a_{n-1} + (9/10^n) \cdot 10/9 \\ &= a_0.\, a_1 \ldots a_{n-1} + (1/10^{n-1}) \\ &= a_0.\, a_1 \ldots (a_{n-1} + 1)\overline{0} \end{aligned}$$

Nel secondo caso si procede allo stesso modo. ■

Questo giustifica ad esempio le uguaglianze $0.4\overline{9} = 0.5\overline{0} = 0.5$ e $0.\overline{9} = 1.\overline{0} = 1$.

1.1.2 Sviluppi periodici

Gli sviluppi decimali possono essere classificati in due categorie a seconda che la successione delle cifre $(a_i)_{i\geq 1}$ sia periodica oppure no. Più precisamente diremo:

[6] Cf. la successiva Sezione 1.1.2.

- **sviluppi periodici** quelli in cui la successione $(a_i)_{i\geq 1}$ è definitivamente periodica, cioè esistono un indice $n \geq 0$ ed un intero $p \geq 1$ tali che per $j > n$ sia $a_j = a_{j+p}$. In altri termini

$$\alpha = a_0.\ \underbrace{a_1 a_2 \dots a_n}_{\text{antiperiodo}} \underbrace{a_{n+1} \dots a_{n+p}}_{\text{periodo}} \underbrace{a_{n+1} \dots a_{n+p}}_{\text{periodo}} a_{n+1} \dots a_{n+p} \dots$$

  ed in questi casi si usa spesso la classica notazione con sopralinea:

$$\alpha = a_0.\ \underbrace{a_1 a_2 \dots a_n}_{\text{antiperiodo}} \underbrace{\overline{a_{n+1} a_{n+2} \dots a_{n+p}}}_{\text{periodo}}$$

  Se $p = 1$, sono rilevanti i casi in cui per ogni $j > n$ si ha $a_j = 9$ (sviluppi $9-$periodici) oppure per ogni $j > n$ si ha $a_j = 0$ (sviluppi $0-$periodici, scolasticamente detti *numeri decimali limitati*). Per convenzione secolare, il periodo "zero" dei numeri decimali $0-$periodici può essere omesso. Come esempi di queste notazioni:

$$\begin{aligned} 3/7 &= 0.428571428571428571\ldots = 1.\overline{428571} \\ 353/19980 &= 0.017667667667667667\ldots = 0.017\overline{667} \\ 1/2 &= 0.4\overline{9} = 0.5\overline{0} = 0.5 \end{aligned}$$

- **non periodici**, gli altri.

Dimostriamo ora che la classificazione degli sviluppi in periodici e non periodici corrisponde esattamente alla suddivisione dei reali in numeri razionali e irrazionali. Iniziamo con un esempio introduttivo.

Esempio 1.1.5 Si consideri il numero $x = 0.\,\overline{12}$ con sviluppo decimale periodico e periodo di due cifre decimali. Moltiplicando x per $10^2 = 100$ otteniamo allora $100\,x = 12.\,\overline{12} = 12 + x$. Risolvendo l'equazione $100\,x = 12 + x$, abbiamo $x = 12/99$.

Se fosse presente un antiperiodo, cioè se ad esempio fosse $x = 0.\,345\overline{12}$, potremmo scrivere ovviamente

$$x = 0.\,345 + 0.\,000\overline{12} = \frac{345}{1000} + \frac{12}{99 \times 1000} = \frac{345 \times 99 + 12}{99000}$$

Vediamo ora il teorema generale.

Teorema 1.1.6 *Un numero reale $\alpha \geq 0$ ha sviluppo decimale periodico (incluso il periodo 0) se e solo se è razionale.*

DIMOSTRAZIONE. Supponiamo $0 \le \alpha < 1$ (dato che la parte intera di α qui non conta). Supponiamo che lo sviluppo decimale sia periodico:

$$\alpha = 0.a_1a_2\dots a_n\overline{b_1b_2\dots b_s} = 0.a_1a_2\dots a_n\, b_1b_2\dots b_s\, b_1b_2\dots b_s\, b_1b_2\dots b_s\ \dots$$

Allora $10^n\alpha$ e $10^{n+s}\alpha$ hanno la stessa parte frazionaria (con sviluppo uguale a $0.\overline{b_1b_2\dots b_s}$) e quindi la loro differenza è uguale a un intero N:

$$10^{n+s}\alpha - 10^n\alpha = N$$

Quindi

$$\alpha = \frac{N}{10^{n+s} - 10^n}$$

▼ Ad esempio, sia $\alpha = 0.17\overline{123}$. Abbiamo $n = 2, s = 3$. Calcoliamo

$$N = 10^{n+s}\alpha - 10^n\alpha = 10^5\alpha - 10^2\alpha = 17123.\overline{123} - 17.\overline{123} = 17123 - 17 = 17106$$

quindi [7]

$$0.17\overline{123} = \frac{17106}{10^5 - 10^2} = \frac{17106}{99900}$$

▲

Viceversa, sia $\alpha = h/k \in [0, 1)$ razionale (con $k > 0$). Le parti frazionarie di

$$\alpha,\ 10\alpha,\ 10^2\alpha,\ 10^3\alpha,\ 10^4\alpha,\ \dots$$

che sono tutte numeri razionali con denominatore $= k$, hanno valori nell'insieme finito

$$0,\ \frac{1}{k},\ \frac{2}{k},\ \dots,\ \frac{k-1}{k}$$

[7] Ricordiamo la regola scolastica: *La frazione generatrice di un numero periodico misto ha per numeratore la differenza tra l'intero formato da parte intera, antiperiodo e periodo, e l'intero formato da parte intera e antiperiodo; per denominatore, tanti 9 quante sono le cifre del periodo, seguiti da tanti 0 quante sono le cifre dell'antiperiodo.*
Questa regola ha comunque una semplice spiegazione, proponibile anche a livelli scolastici. Consideriamo per primo i numeri periodici come $x = 0.\overline{159}$: evidentemente $1000\,x = 159.\overline{159} = 159 + x$ cioè $999\,x = 159$ e quindi $x = 159/999$. Consideriamo ora un numero misto come $\alpha = 3.14\overline{159}$. Si ha subito:

$$\begin{aligned}\alpha = 3.14\overline{159} = 3.14 + 0.00\overline{159} &= 3.14 + \frac{x}{100} = 3.14 + \frac{159}{999\,00} \\ &= \frac{3.14 \times 999\,00 + 159}{999\,00} = \frac{314 \times (1000 - 1) + 159}{999\,00} \\ &= \frac{314159 - 314}{999\,00}.\end{aligned}$$

quindi ci sono due razionali come $10^n\alpha$ e $10^{n+s}\alpha$ con la stessa parte frazionaria, e quindi come in precedenza la loro differenza è uguale a un intero N:

$$10^{n+s}\alpha - 10^n\alpha = N$$

da cui si ricava che

$$10^n\alpha = \frac{N}{10^s - 1}$$

Sia ora N_1 la parte intera di $N/(10^s - 1)$ per modo che risulti

$$10^n\alpha = \frac{N}{10^s - 1} = N_1 + \frac{N_2}{10^s - 1}$$

con $0 \leq N_2 < 10^s - 1$, ovvero

$$10^n\alpha - N_1 = \frac{N_2}{10^s - 1}$$

Considerata la serie armonica di ragione $1/10^s$ si ha:

$$1 + \frac{1}{10^s} + \frac{1}{10^{2s}} + \frac{1}{10^{3s}} + \ldots = \frac{1}{1 - \frac{1}{10^s}} = \frac{10^s}{10^s - 1}$$

da cui:

$$\frac{1}{10^s} + \frac{1}{10^{2s}} + \frac{1}{10^{3s}} + \ldots = \frac{1}{10^s - 1}$$

e quindi:

$$10^n\alpha - N_1 = \frac{N_2}{10^s - 1} = \frac{N_2}{10^s} + \frac{N_2}{10^{2s}} + \frac{N_2}{10^{3s}} + \ldots$$

Concludiamo che o $N_2 = 0$ e allora α ha uno sviluppo 0–periodico, oppure $N_2 \neq 0$ e α ha per antiperiodo le cifre di N_1 e per periodo le s cifre dell'intero N_2.

▼ Ad esempio, sia $\alpha = h/k = 3/7$. Tabulando le parti frazionarie di $3 \cdot 10^j/7$ per $j = 0, \ldots$ si vede che $3/7$ e $3 \cdot 10^6/7 = 3000000/7$ hanno la stessa parte frazionaria (uguale a $3/7$), in quanto $3000000/7 = 428571 + 3/7$. Abbiamo $n = 0$, $s = 6$, $N = 428571$, $N_1 = 0$, $N_2 = N = 428571$. Infine

$$10^n\alpha - N_1 = \frac{3}{7} = \frac{428571}{1000000} + \ldots = 0.\overline{428571}$$

▲

La dimostrazione è conclusa. ■

Esercizio 1.1.7 Dimostrare che il Teorema 1.1.6 vale indipendentemente dalla base dello sviluppo. Dimostrare cioè che, fissato un numero intero $B > 1$, un numero reale $\alpha \geq 0$ ha sviluppo B–nario periodico (incluso il periodo 0) se e solo se è razionale.

1.1.3 Unicità degli sviluppi decimali

Abbiamo visto nella sezione precedente che i numeri razionali che moltiplicati per una potenza di 10 danno un intero (cioè i decimali "limitati") ammettono *due* sviluppi decimali, uno 0–periodico ed uno 9–periodico. Mostreremo ora che questo è l'unico caso in cui un numero reale ha due sviluppi formalmente differenti.[8]

Teorema 1.1.8 *Dati due interi non negativi a_0 e b_0 e date due successioni di cifre $(a_i)_{i\geq 1}$ e $(b_i)_{i\geq 1}$ $(0 \leq a_i, b_i < 10)$, consideriamo i numeri reali:*

$$\alpha = a_0 + \sum_{i=1}^{\infty} a_i/10^i, \qquad \beta = b_0 + \sum_{i=1}^{\infty} b_i/10^i$$

Se $\alpha = \beta$, vale una ed una sola delle seguenti proposizioni (i) *e* (ii)*:*

(i) *$a_0 = b_0$ e per ogni $i \geq 1$ si ha $a_i = b_i$;*

(ii) *una ed una sola delle successioni $(a_i)_{i\geq 1}$ e $(b_i)_{i\geq 1}$ è $9-$periodica. Inoltre, se è $9-$periodica, ad esempio, la $(a_i)_{i\geq 1}$:*

(ii.1) *se $(a_i)_{i\geq 1} = (9, 9, 9, 9, 9, 9, \ldots)$, allora $(b_i)_{i\geq 1} = (0, 0, 0, 0, 0, 0, \ldots)$, e si ha $b_0 = a_0 + 1$,*

(ii.2) *se $(a_i)_{i\geq 1} = (a_1, a_2, \ldots, a_k, 9, 9, 9, 9, 9, 9, \ldots)$, con $a_k \leq 8$, allora $(b_i)_{i\geq 1} = (b_1, b_2, \ldots, b_k, 0, 0, 0, 0, 0, 0, \ldots)$, con $b_0 = a_0$, $b_i = a_i$ per $1 \leq i \leq k-1$, e si ha $b_k = a_k + 1$.*

Dimostrazione. È evidente che non possono essere vere entrambe le (i) e (ii). Supponiamo ora falsa la (i). Proviamo la (ii). Se (i) è falsa può essere $a_0 \neq b_0$. In questo caso si ha subito che le due successioni non possono essere entrambe $9-$periodiche: sottraendo la parte $9-$periodica in comune, avremmo

$$a_0 + \sum_{i=1}^{n} a_i/10^i = b_0 + \sum_{i=1}^{n} b_i/10^i$$

[8] Abbiamo già visto che, ad esempio, $0.5\overline{0} = 0.4\overline{9}$. Questo potrebbe far sospettare che, analogamente, nello sviluppo $\pi = 3.14159\ldots$ si possa mettere 8 al posto della quinta cifra 9, pur di "compensare" questa diminuizione aumentando corposamente qualcuna delle cifre successive. In altri termini, in linea di principio *potrebbe* essere $\pi = 3.14159265358979323846264\ldots = 3.14158376999989567988895\ldots$. È solo l'abitudine che ci fa respingere come *evidentemente* assurda questa possibilità: in effetti c'è bisogno di una dimostrazione.

e questo è impossibile se gli interi a_0, b_0 sono diversi, dato che le due sommatorie (finite) sono entrambe < 1. Ora, quale delle due è $9-$periodica dipende da quale fra a_0 e b_0 è il minore dei due. Supponiamo per esempio che sia $a_0 < b_0$. Per ipotesi $a_0+\alpha_1 = b_0+\beta_1$ con $\alpha_1 = \sum_{i=1}^{\infty} a_i/10^i$, $\beta_1 = \sum_{i=1}^{\infty} b_i/10^i$, $0 \leq \alpha_1, \beta_1 \leq 1$. Quindi $0 < b_0 - a_0 = \alpha_1 - \beta_1$ con $0 < \alpha_1 - \beta_1 \leq 1$ ed essendo a_0, b_0 interi non può essere altro che $\alpha_1 - \beta_1 = 1$, e da questo non può essere altro che $\alpha_1 = 1$ e $\beta_1 = 0$, e quindi non può essere altro che $a_i = 9$ e $b_i = 0$ per $i \geq 1$.

Sempre se la (i) è falsa, ma è $a_0 = b_0$, esiste il minimo k tale che $a_k \neq b_k$. Quindi intanto si ha $b_0 = a_0$ e $b_i = a_i$ per $1 \leq i \leq k-1$. Riscriviamo $\alpha = \beta$ come

$$a_0 + \sum_{i=1}^{k-1} a_i/10^i + \sum_{i=k}^{\infty} a_i/10^i = b_0 + \sum_{i=1}^{k-1} b_i/10^i + \sum_{i=k}^{\infty} b_i/10^i$$

Semplificando gli addendi uguali e moltiplicando per 10^k:

$$\sum_{i=k}^{\infty} a_i/10^{i-k} = \sum_{i=k}^{\infty} b_i/10^{i-k}$$

cioè

$$a_k + \underbrace{a_{k+1}/10 + a_{k+2}/10^2 + \ldots}_{\alpha_2} = b_k + \underbrace{b_{k+1}/10 + b_{k+2}/10^2 + \ldots}_{\beta_2}$$

con $0 \leq \alpha_2, \beta_2 \leq 1$. Basta allora ripetere l'argomento precedente. ■

Abbiamo in conclusione che:

Teorema 1.1.9 *La rappresentazione di un numero reale $\alpha \geq 0$ come serie del tipo*

$$\alpha = a_0 + \sum_{i=1}^{\infty} a_i/10^i$$

dove $a_0 \geq 0$ è un intero e dove, per $i \geq 1$, le cifre a_i sono interi tali che $0 \leq a_i \leq 9$, è unica (nel senso che α identifica univocamente sia l'intero $a_0 \geq 0$ che la successione $(a_i)_{i\geq 1}$ di cifre fra 0 e 9), ad eccezione del caso in cui esista un intero $N \geq 1$ tale che $10^N\alpha$ sia intero, nel qual caso la successione delle cifre può essere $0-$periodica oppure $9-$periodica.

Osservazione 1.1.10 Lo sviluppo decimale dei numeri reali è evidentemente molto semplice da descrivere, utilissimo nelle applicazioni ed è anche ben collegato alla definizione formale dei numeri reali come sezioni di Dedekind

del campo razionale (Fiori e Invernizzi 2009, p. 93 segg.), tanto che scolasticamente si tende a confondere la nozione di numero reale con quella di sviluppo decimale. Esso presenta un inestetismo evidente, la doppia rappresentazione di taluni razionali, ma il suo "difetto" più serio è la "cattiva" approssimazione di $\alpha = \sum_{i=0}^{\infty} a_i/10^i$ con le somme parziali $\sum_{i=0}^{n} a_i/10^i$. Infatti, ad esempio, è prassi approssimare π con $3.14 = 314/100$ oppure il numero di Nepero e con $2.71 = 271/100$, ma, come si vedrà, $314/100$ non è una "buona" approssimazione razionale di π, né $271/100$ è una "buona" approssimazione di e. Infatti, se si ammettono denominatori comparabili a 100, le approssimazioni $\pi \approx 355/113 = 3.14159\ldots$ ed $e = 193/71 = 2.71830\ldots$ sono di gran lunga migliori rispettivamente di 3.14 e di 2.71. Lo stesso "difetto" si manifesta evidente con i razionali: ad esempio si ha $3/7 = 0.\overline{428571}$, ma nessuna delle ridotte $4/10$, $42/100$, $428/1000$, $4285/10000$, ... è una approssimazione razionale di $3/7$ "migliore" di quanto lo sia lo stesso $3/7$.

Esercizio 1.1.11 Siano

$$\begin{aligned} x &= 0.26364656667686961061161 26 \\ y &= 0.27374757677787971071171 27 \end{aligned}$$

Scrivere lo sviluppo decimale di un numero razionale r tale che $x < r < y$.

Esercizio 1.1.12 Siano

$$\begin{aligned} x &= 0.\overline{44332} \\ y &= 0.44332443324\overline{433} \end{aligned}$$

Scrivere lo sviluppo decimale di un numero irrazionale α tale che $x < \alpha < y$.

1.2 Un quadrato è equipotente ad un intervallo

Oggi, risultati come

$$\aleph_0 \cdot \aleph_0 = \aleph_0, \quad 2^{\aleph_0} = \mathfrak{C}, \quad \mathfrak{C} \cdot \mathfrak{C} = \mathfrak{C}$$

non destano alcuna meraviglia o incredulità in chi studia matematica ed incontra (anche a livello *naïf*) le basi della teoria degli insiemi infiniti e della cardinalità. Ricordiamo che $\aleph_0$ è la cardinalità degli insiemi numerabili, cioè equipotenti ad $\mathbb{N}$, mentre $\mathfrak{C}$ è la cardinalità *del continuo*, cioè la cardinalità di $\mathbb{R}$. In particolare, la uguaglianza $\mathfrak{C} \cdot \mathfrak{C} = \mathfrak{C}$ equivale ad affermare che un quadrato è equipotente ad un intervallo, cioè che vale il seguente:

Teorema 1.2.1 *Sia $I = [0, 1]$. Esiste un'applicazione biiettiva $I^2 \to I$.*

In questa forma, questo risultato è dovuto a Georg Cantor, che lo dimostrò nel giugno del 1877. Riporteremo questa dimostrazione più avanti, nella Sezione 2.5. È interessante ricordare, a conclusione di questo Capitolo dedicato agli sviluppi decimali, che essa ebbe una genesi travagliata, legata proprio alla doppia rappresentazione decimale dei razionali 0– e 9–periodici

La storia della dimostrazione di Cantor del Teorema 1.2.1 iniziò il 5 gennaio 1874, quando Cantor scrisse una breve lettera a Richard Dedekind, nella quale pose al collega il problema dell'esistenza o meno di un'applicazione biiettiva $I^2 \to I$. Precisò che la questione gli appariva molto difficile, e aggiunse che la sua idea era che tale biiezione *non* potesse esistere. Va infatti ricordato che all'epoca il concetto di "dimensione" era ancora molto vago, e legato al "numero delle coordinate indipendenti". In termini meccanici, si riteneva che un sistema fisico a 2 (o più) "gradi di libertà" non potesse essere descritto da una sola variabile 1–dimensionale. Dopo un lungo silenzio, Cantor riprese la questione nel giugno del 1877, e ottenne una "dimostrazione" proprio di ciò in cui non credeva: in una lettera a Dedekind di mercoledì 20 giugno 1877 presentò infatti al collega la costruzione esplicita di un'applicazione $I^2 \to I$ che affermò essere biiettiva.

L'idea originalissima di Cantor è basata sulla "alternanza delle cifre decimali", e su un lemma preliminare, che afferma l'esistenza di una applicazione biiettiva $\phi : [0, 1] \to (0, 1]$ che consente di sostituire I con $I' = (0, 1]$. Per ogni punto $(x, y) \in I'^2$ si considerano gli sviluppi decimali

$$x = 0.\, a_1 a_2 a_3 \ldots, \quad y = 0.\, b_1 b_2 b_3 \ldots$$

scegliendo sempre quelli 9–periodici quando possibile (l'esclusione dello 0 è servita a questo scopo). Si costruisce poi un numero reale $t \in I$ da associare a (x, y) con la tecnica della "alternanza delle cifre decimali":

$$t = 0.\, a_1 b_1 a_2 b_2 a_3 b_3 \ldots$$

Ma solo due giorni dopo, il venerdì 22 giugno 1877, Dedekind rispose a Cantor segnalandogli un difetto nella dimostrazione. Infatti l'argomento di Cantor riesce a dimostrare solo che:

Teorema 1.2.2 *Sia $I = [0, 1]$. Esiste un'applicazione iniettiva $I^2 \to I$.*

Infatti l'applicazione $(x, y) \to t$ definita dalla tecnica della "alternanza delle cifre decimali" non è suriettiva in quanto sono esclusi dall'immagine tutti i

$t \in I$ nel cui sviluppo decimale si hanno da un certo punto in poi tutte le cifre di ordine dispari (oppure tutte quelle di ordine pari) uguali a 0. Ad esempio, $t = 0.3420202020202\ldots$ dovrebbe provenire da $x = 0.322222\ldots$, $y = 0.4000000\ldots$, ma per tale y va scelto lo sviluppo $y = 0.39999999\ldots$, e quindi il procedimento dell'alternanza delle cifre decimali produce $t' = 0.332929292929\ldots \neq t$. Si può in particolare vedere subito che la immagine del quadrato tramite l'applicazione definita da Cantor con l'alternanza delle cifre è totalmente disconnessa.[9]

Preso atto della svista, il giorno dopo, sabato 23, Cantor inviò a Dedekind una cartolina postale nella quale lo ringraziò per l'osservazione, e si ripromise di "sistemare" la dimostrazione del teorema, della cui verità era ormai convinto. Gli basterà in effetti la domenica 24 per ottenere la dimostrazione "pulita" (quella che presenteremo nella Sezione 2.5), e lunedì 25 giugno 1877 fu in grado di comunicare a Dedekind di aver conseguito finalmente il successo pieno.[10]

Osservazione 1.2.3 Con il senno di poi si può affermare che la tecnica dell'alternanza delle cifre decimali come presentata da Cantor porta comunque all'equipotenza di un quadrato ed un intervallo. Lo stesso Cantor enfatizzò nella famosa cartolina postale che la cosa importante era di aver costruito un'applicazione *iniettiva* dal quadrato nell'intervallo: per cui l'intervallo è equipotente al quadrato o addirittura ha cardinalità maggiore! Infatti il Teorema 1.2.2 stabilisce che $\mathfrak{C} \cdot \mathfrak{C} \leq \mathfrak{C}$, e dato che la banale iniezione $t \mapsto (t, 0)$ mostra che $\mathfrak{C} \cdot \mathfrak{C} \geq \mathfrak{C}$, per il teorema cosiddetto di Cantor–Schröder–Bernstein (Barozzi e Matarasso, 1986, p. 43) si ottiene l'uguaglianza $\mathfrak{C} \cdot \mathfrak{C} = \mathfrak{C}$. Quanto e come Cantor fosse disponibile ad utilizzare il teorema di Cantor–Schröder–Bernstein (in pratica la proprietà antisimmetrica della relazione d'ordine fra cardinali transfiniti) è ancora oggetto di studi storici.[11]

[9] Un sottoinsieme E di $\mathbb{R}$ è *totalmente disconnesso* se fra due qualunque punti di E esiste un punto che non appartiene ad E. Ad esempio, l'insieme degli irrazionali è totalmente disconnesso in quanto fra due qualunque reali, e in particolare fra due irrazionali, esiste un razionale. Nel caso in esame, dati due qualunque numeri $t, s \in I$ tali che $t < s$ esiste un razionale r tale che $t < r < s$. Esiste quindi n tale che $10^{-n} < \min\{s-r, r-t\}$. Modificando lo sviluppo decimale di r *dopo* l'$(n+1)$–esima cifra ponendo uguali a 0 (ad esempio) le cifre di ordine pari, si ottiene un numero r', ancora strettamente compreso fra t ed s, che non può essere generato con il procedimento dell'alternanza delle cifre decimali.

[10] Va sottolineato in questo importante progresso della matematica anche il ruolo ricoperto dalle Poste prussiane, che erano evidentemente in grado di far recapitare la corrispondenza coprendo in un solo giorno i 182 km che dividono la città di Halle, la sede di Cantor, da Brunswick (oggi Braunschweig), la sede di Dedekind, e per di più in pieno *weekend*.

[11] Il teorema nasce nel decennio 1887–1897, con svariati contributi successivi di Dedekind, Cantor, Schröder e infine Bernstein.

Ci si può infine chiedere come mai a Cantor siano serviti tre anni per pensare ad un procedimento tanto banale come l'alternanza delle cifre decimali. Uno studio di Arrigo e D'Amore (1999) mostra che si è portati a pensare alle cifre dello sviluppo decimale di un reale α come ad un *unicum* non modificabile, tanto che la sperimentazione in classe ha provato che taluni studenti di scuola superiore ritengono *illegittimo* un procedimento che "toglie" ad α le cifre di ordine pari (o dispari) per "creare" altri numeri che di fatto sarebbero quindi "nascosti" in α stesso.

Capitolo 2

Frazioni continue

2.1 Frazioni continue finite

Iniziamo con il definire formalmente, per induzione, le *frazioni continue finite*, ovvero le "espressioni" che si possono scrivere nella forma "intuitiva"

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \; a_{n-1} + \cfrac{1}{a_n}}}} \tag{2.1}$$

che usa la notazione dei tre puntini di sospensione. Nella (2.1) l'indice n è un intero ≥ 1, a_0 è un intero ≥ 0, gli a_k per $1 \leq k \leq n-1$ sono interi positivi, mentre a_n è un numero reale positivo arbitrario.

Definizione 2.1.1 (frazioni continue finite) *Sia $n \geq 1$ un intero, sia a_0 un numero intero ≥ 0, siano a_1, a_2, $\ldots$, a_{n-1} numeri interi ≥ 1, e sia $a_n \in \mathbb{R}$, $a_n > 0$. Indichiamo con*

$$\alpha = [a_0;\, a_1, a_2, \ldots, a_{n-1}, a_n] \tag{2.2}$$

il numero reale definito per induzione (sul numero di termini dopo il punto e virgola) da:

$$\begin{aligned} &[a_0;\, a_1] = a_0 + 1/a_1 \quad \text{(un solo termine dopo il punto e virgola)} \\ &[a_0;\, \underbrace{a_1, a_2, \ldots, a_{n-1}, a_n}_{n \text{ termini}}] = [a_0;\, \underbrace{a_1, a_2, \ldots, a_{n-2}, a_{n-1} + 1/a_n}_{(n-1) \text{ termini}}] \end{aligned} \tag{2.3}$$

Ad esempio:

$$\alpha = [3; 4, 5, 6] = 3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{6}}} = \frac{421}{130} \approx 3.23846$$

Un altro esempio numerico:

$$\alpha = [3; 4, 5, \sqrt{3}] = 3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{\sqrt{3}}}} = \frac{13 + 68\sqrt{3}}{4 + 21\sqrt{3}} \approx 3.23927$$

Un esempio simbolico:

$$\alpha = [3; 4, 5, \xi] = 3 + \cfrac{1}{4 + \cfrac{1}{5 + \cfrac{1}{\xi}}} = \frac{13 + 68\,\xi}{4 + 21\,\xi}$$

2.2 Frazioni continue infinite

Introdurremo ora le *frazioni continue infinite*, brevemente dette *frazioni continue* (sottointendendo "infinite").

Definizione 2.2.1 *Sia a_0 un numero intero ≥ 0 e sia $(a_k)_{k\geq 1}$ una successione di numeri interi ≥ 1. Consideriamo la successione $(c_k)_{k\geq 0}$ di frazioni continue finite*

$$\begin{aligned} c_0 &= a_0 \\ c_k &= [a_0;\, a_1, a_2, \ldots, a_k] \end{aligned} \tag{2.4}$$

Se la successione $(c_k)_{k\geq 0}$ converge ad un numero $\alpha \in \mathbb{R}$, diremo che la ***frazione continua (infinita)***

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} \tag{2.5}$$

converge *ad α, e scriveremo simbolicamente*

$$\alpha = \lim_{k\to\infty} [a_0;\, a_1, a_2, \ldots, a_k] = [a_0;\, a_1, a_2, a_3, \ldots] \tag{2.6}$$

ed anche

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}} \tag{2.7}$$

Quando la successione $(c_k)_{k\geq 0}$ definita nella (2.4) è convergente, la frazione (numero razionale) c_k è chiamata la k–esima ***convergente*** della frazione continua (2.6) o (2.5).[1]

Osservazione 2.2.2 Le frazioni continue che abbiamo definito in precedenza sono più propriamente dette frazioni continue (finite o infinite) *semplici*, in quanto tutti i "numeratori" sono uguali a 1. Più in generale si possono considerare frazioni continue *generalizzate*, del tipo:

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_3}{a_3 + \cfrac{b_4}{\ddots}}}} \tag{2.8}$$

dove le a_k e le b_k possono essere numeri arbitrari o addirittura funzioni reali di una variabile reale. Nella Figura 2.1 si può leggere l'introduzione del concetto di frazione continua (generalizzata) come presentata da Lagrange (1798). Queste frazioni "generalizzate" non sono proprio solo una "pura curiosità", come scrive Lagrange, ma comunque escono dai limiti della nostra trattazione.

2.2.1 Le formule di Eulero

Gran parte della teoria che svilupperemo dipende da alcune semplici formule, che, dati che siano gli interi a_k, consentono di calcolare le c_k della (2.4) con semplici formule di ricorrenza. Queste formule sono dovute a Wallis (1656, pp. 191–192) e ad Eulero (1744a, pp. 103–104); entrambi gli autori trattano il caso delle frazioni continue generalizzate del tipo (2.8).[2] Eulero (1744a) calcola

[1] Si osservi la analogia con il concetto di serie numerica convergente: la successione delle convergenti di una frazione continua corrisponde alla successione delle somme parziali della serie.

[2] Va però notato che il contributo di Wallis in questo campo è sporadico, limitandosi sostanzialmente alle due pagine sopracitate, mentre è Eulero con la sua *De fractionibus continuis dissertatio* (1744a) a fare del tema delle frazioni continue un nuovo autonomo capitolo della matematica. È per questi motivi che chiamiamo le formule dimostrate in questa sezione *formule di Eulero* (e non *formule di Wallis–Eulero*).

§ I.—- *Sur les fractions continues considérées par rapport à l'Arithmétique.*

1. Comme la Théorie des fractions continues manque dans les livres ordinaires d'Arithmétique et d'Algèbre, et que, par cette raison, elle doit être peu connue des géomètres, nous croyons devoir commencer ces Additions par une exposition abrégée de cette Théorie, dont nous aurons souvent lieu de faire l'application dans la suite.

On appelle, en général, *fraction continue* toute expression de cette forme

$$a+\cfrac{\alpha}{b+\cfrac{\beta}{c+\cfrac{\gamma}{d+\cfrac{\delta}{e+\ddots}}}}$$

où les quantités $a, b, c, \ldots$ et $\alpha, \beta, \gamma, \ldots$ sont des nombres entiers poitifs ou négatifs; mais nous ne considérerons ici quel les fractions continues où les numérateurs $b, c, d, \ldots$ sont égaux à l'unité, c'est–à–dire, celles qui sont de la forme

$$a+\cfrac{1}{b+\cfrac{1}{c+\cfrac{1}{d+\cfrac{1}{e+\ddots}}}}$$

$a, b, c, \ldots$ étant d'ailleurs des nombres quelconques entiers positifs ou négatifs: car celles–ci sont, 'a proprement parler, les seules qui soient d'un grand usage dans l'Analyse, les autres n'étant presque que de pure curiosité.

Figura 2.1: La definizione delle frazioni continue (generalizzate) in Lagrange (1798). Rispetto all'originale, in questa riproduzione abbiamo invertito le lettere latine con le greche, per coerenza con la successiva Figura 2.2. Si noti come Lagrange mette subito in rilievo che la teoria delle frazioni continue manca nei trattati tipici di aritmetica ed algebra.

esplicitamente, con l'aiuto di uno "schema", i primi valori delle frazioni finite che si ottengono troncando la (2.8), includendo all'inizio la frazione formale $1/0$ corrispondente a $k = -1$ (si veda la successiva Osservazione 2.2.4), e conclude esponendo la legge di ricorrenza a parole: si veda la Figura 2.2.[3]

> Lex autem progressionis harum fractionum ex sequente schemate clare percipietur:
>
> $$\begin{array}{cccccc} a & b & c & d & e \\ \frac{1}{0}; & \frac{a}{1}; & \frac{ab+\alpha}{b}; & \frac{abc+\alpha c+\beta a}{bc+\beta}; & \frac{abcd+\alpha dc+\beta ad+\gamma ab+\alpha\gamma}{bcd+\beta d+\gamma b} \\ \alpha & \beta & \gamma & \delta & \varepsilon \end{array}$$
>
> ... Lex jam progressionis in hoc consistit ut cuiusque fractionis numerator per indicem supra scriptum multiplicatus una cum numeratore præcedentis fractionis per suum infra scriptum indicem multiplicato præbeat numeratorem sequentis fractionis: Atque eodem modo cuiusque fractionis denominator per indicem suum supra positum multiplicatus una cum denominatore præcedentis fractionis per indicem suum infra scriptum indicem multiplicato præbeat denominatorem fractionis sequentis.

Figura 2.2: La dimostrazione di Eulero (1744a) delle formule di ricorrenza che esprimono le convergenti di una frazione continua generalizzata.

Teorema 2.2.3 *Sia $(a_k)_{k\geq 0}$ una successione di interi, con $a_0 \geq 0$ e $a_k \geq 1$ per $k \geq 1$. Definiamo induttivamente due successioni di interi $(A_k)_{k\geq 0}$, e $(B_k)_{k\geq 0}$ con le* ***formule di Eulero****:*

$$\begin{cases} A_0 = a_0, & A_1 = a_0 a_1 + 1, \\ B_0 = 1, & B_1 = a_1, \end{cases} \quad \text{e per } k \geq 2 : \begin{cases} A_k = a_k\, A_{k-1} + A_{k-2} \\ B_k = a_k\, B_{k-1} + B_{k-2} \end{cases} \tag{2.9}$$

[3] La lettura di questo brano di Eulero mostra immediatamente quale progresso per lo studio della matematica sia stata la formalizzazione del principio di induzione dovuta a Giuseppe Peano. Eulero usa spesso l'"induzione" come metodo dimostrativo, Ad esempio, nel calcolo della somma di alcune serie che rappresentano valori particolari della funzione zeta di Riemann $\zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$, $(s \in \mathbb{C}, \Re(s) > 1)$, Eulero (1768, p. 84) scrive: *Cette remarque me paroit d'autant plus importance, qu'elle n'est encore fondée sur une induction, mais que je porterai à un tel degré de certitude, qu'on la pourra regarder comme très rigoureusement démontrée.* Tuttavia, Eulero con il termine *induction* si riferisce alla "logica induttiva", contrapposta alla solita "logica deduttiva" comunemente usata in matematica. In linguaggio moderno diremmo che Eulero dimostra la verità di alcuni suoi teoremi generali, provando che sono validi in taluni casi speciali che gli conferiscono una consapevole certezza.

Allora, per ogni $k \geq 0$, si ha che

$$\frac{A_k}{B_k} = [a_0;\, a_1, a_2, \ldots, a_k] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\ a_{k-1} + \cfrac{1}{a_k}}} \tag{2.10}$$

$$A_{k+1}B_k - A_kB_{k+1} = (-1)^k \tag{2.11}$$

Dimostrazione. Si noti che per ogni $k \geq 0$ si ha $B_k > 0$, in base alla stessa definizione. Come base di induzione verifichiamo la (2.10) e la (2.11) per $k = 0$ e per $k = 1$. Si ha

$$\begin{aligned} \frac{A_0}{B_0} &= \frac{a_0}{1} = a_0 = [a_0;] \\ \frac{A_1}{B_1} &= \frac{a_0a_1 + 1}{a_1} = a_0 + \frac{1}{a_1} = [a_0;\, a_1] \end{aligned} \tag{2.12}$$

Converrà calcolare anche

$$\frac{A_2}{B_2} = \frac{a_2A_1 + A_0}{a_2B_1 + B_0} = \frac{a_0a_1a_2 + a_2 + a_0}{a_1a_2 + 1} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2}} = [a_0;\, a_1, a_2]$$

Inoltre

$$A_1B_0 - A_0B_1 = (a_0a_1 + 1) \times 1 - a_0 \times a_1 = 1 = (-1)^0$$
$$A_2B_1 - A_1B_2 = (a_0a_1a_2 + a_2 + a_0)a_1 - (a_0a_1 + 1)(a_1a_2 + 1) = -1 = (-1)^1$$

Supponiamo quindi che la (2.10) e la (2.11) siano vere per l'indice $k - 1 \geq 1$ e proviamole per l'indice k. Usiamo la ovvia uguaglianza

$$[a_0;\, \underbrace{a_1, a_2, \ldots, a_k}_{k \text{ termini}}] = a_0 + \frac{1}{[a_1;\, \underbrace{a_2, a_3, \ldots, a_k}_{(k-1) \text{ termini}}]}$$

Per l'ipotesi induttiva, possiamo esprimere $[a_1;\, a_2, a_3, \ldots, a_k]$ come frazione

$$\frac{A'_{k-1}}{B'_{k-1}} = [a_1;\, a_2, a_3, \ldots, a_k]$$

dove le A' e le B' verificano le formule di Eulero. Ponendo allora per definizione:

$$\frac{p_k}{q_k} = [a_0;\, a_1, a_2, \ldots, a_k]$$

abbiamo

$$\frac{p_k}{q_k} = a_0 + \frac{1}{A'_{k-1}/B'_{k-1}} = \frac{a_0\, A'_{k-1} + B'_{k-1}}{A'_{k-1}}$$

Per la (2.11), A'_{k-1} e B'_{k-1} sono primi fra loro (non possono avere un fattore comune ≥ 2), quindi anche p_k e q_k sono primi fra loro, e pertanto:

$$\begin{cases} p_k = a_0\, A'_{k-1} + B'_{k-1} \\ q_k = A'_{k-1} \end{cases}$$

Esplicitiamo il fatto che, per l'ipotesi induttiva, le A' e le B' verificano le formule di Eulero:

$$\begin{cases} A'_{k-1} = a_k\, A'_{k-2} + A'_{k-3} \\ B'_{k-1} = a_k\, B'_{k-2} + B'_{k-3} \end{cases}$$

Le a hanno indice k invece di $k-1$ in quanto la frazione $[a_1;\, a_2, \ldots, a_k]$ "inizia" con a_1 e non con a_0. Infine:

$$\begin{aligned} p_k &= a_0(a_k A'_{k-2} + A'_{k-3}) + (a_k B'_{k-2} + B'_{k-3}) \\ &= a_k(a_0 A'_{k-2} + B'_{k-2}) + (a_0 A'_{k-3} + B'_{k-3}) \\ &= a_k p_{k-1} + p_{k-2} \\ q_k &= a_k A'_{k-2} + A'_{k-3} \\ &= a_k q_{k-1} + q_{k-2} \end{aligned}$$

Ne viene che le p_k e le q_k verificano le formule di ricorrenza (2.9) e pertanto necessariamente si ha $p_k = A_k$ e $q_k = B_k$ per ogni $k \geq 0$. Dunque la (2.10) è verificata per l'indice k.

Proviamo ora la (2.11) per l'indice k. Per l'ipotesi induttiva

$$A_k B_{k-1} - A_{k-1} B_k = (-1)^{k-1}$$

e le formule di Eulero già dimostrate, si ha:

$$\begin{aligned} A_{k+1}B_k - A_k B_{k+1} &= (a_{k+1}A_k + A_{k-1})B_k - A_k(a_{k+1}B_k + B_{k-1}) \\ &= -(A_k B_{k-1} - A_{k-1}B_k) \\ &= -(-1)^{k-1} = (-1)^k \end{aligned} \tag{2.13}$$

il che prova che la (2.11) è vera per ogni $k \geq 0$. ■

Osservazione 2.2.4 Si possono assumere nelle formule di Eulero condizioni iniziali per un indice artificioso $k = -1$:

$$\begin{cases} A_{-1} = 1, & A_0 = a_0 \\ B_{-1} = 0, & B_0 = 1 \end{cases} \tag{2.14}$$

Infatti ritroviamo esattamente i valori:

$$\begin{cases} A_1 = a_1\, A_0 + p_1\, A_{-1} & = a_0 a_1 + 1 \\ B_1 = a_1\, B_0 + p_1\, B_{-1} & = a_1 \end{cases} \tag{2.15}$$

Osservazione 2.2.5 È immediato osservare che la successione $(B_k)_{k\geq 0}$ "dei denominatori" è positiva, crescente, e strettamente crescente per $n \geq 1$:

$$1 = B_0 \leq B_1 < B_2 < B_3 < B_4 < \dots$$

La positività è ovvia. Per definizione, $B_0 = 1$ e $B_1 = a_1 \geq 1$. Se $k \geq 2$, per le formule di Eulero si ha $B_k = a_k B_{k-1} + B_{k-2} > a_k B_{k-1} \geq B_{k-1}$ ■

Esercizio 2.2.6 Dimostrare che nel caso di una frazione continua generalizzata (2.8) le formule Eulero diventano:

$$\begin{cases} A_0 = a_0, & A_1 = a_0 a_1 + b_1 \\ B_0 = 1, & B_1 = a_1 \end{cases} \quad \text{e per } k \geq 2 : \begin{cases} A_k = a_k\, A_{k-1} + b_k\, A_{k-2} \\ B_k = a_k\, B_{k-1} + b_k\, B_{k-2} \end{cases}$$

2.2.2 Frazioni continue e serie

Le formule di Eulero consentono di dimostrare un importante legame fra le frazioni continue e le serie.

Teorema 2.2.7 (Frazione continua come serie) *Sia a_0 un numero intero ≥ 0 e sia $(a_k)_{k\geq 1}$ una successione di numeri interi ≥ 1. La successione $(c_k)_{k\geq 0}$ di frazioni continue finite $c_k = [a_0;\, a_1, a_2, \dots, a_k]$ definita nella (2.4) coincide con la successione $(s_k)_{k\geq 0}$ delle somme parziali della serie numerica:*

$$\underbrace{\frac{a_0}{B_0}}_{r_0} + \underbrace{\frac{1}{B_1}}_{r_1} - \underbrace{\frac{1}{B_1 B_2}}_{r_2} + \underbrace{\frac{1}{B_2 B_3}}_{r_3} - \underbrace{\frac{1}{B_3 B_4}}_{r_4} + \underbrace{\frac{1}{B_4 B_5}}_{r_5} - \dots \tag{2.16}$$

dove i B_k ai denominatori sono quelli definiti nelle formule di Eulero (2.9).

DIMOSTRAZIONE. Si osservi subito che la serie (2.16) è a segni alterni dal termine r_1 in poi. Poniamo

$$s_k = r_0 + r_1 - r_2 + \ldots + (-1)^{k+1} r_k = r_0 + \sum_{i=1}^{k} (-1)^{i+1} r_i$$

e dimostriamo per induzione su k che per ogni $k \geq 0$ si ha $s_k = c_k$.

Per le (2.12) e per le formule di Eulero (2.9) abbiamo:

$$\begin{aligned} s_0 = r_0 \qquad & = a_0 = c_0 \\ s_1 = r_0 + r_1 \quad & = a_0 + \frac{1}{B_1} = a_0 + \frac{1}{a_1} = c_1 \end{aligned}$$

Supponiamo ora $k \geq 2$ e che sia $s_k = c_k$, ossia che:

$$s_k = a_0 + \frac{1}{B_1} - \frac{1}{B_1 B_2} + \frac{1}{B_2 B_3} - \ldots + (-1)^{k-1} \frac{1}{B_{k-1} B_k} = \frac{A_k}{B_k} = c_k \quad (2.17)$$

Usando la (2.11) abbiamo allora:

$$\begin{aligned} s_{k+1} &= s_k + (-1)^k \cdot \frac{1}{B_k B_{k+1}} \\ &= \frac{A_k}{B_k} + (-1)^k \cdot \frac{1}{B_k B_{k+1}} \\ &= \frac{A_k}{B_k} + \frac{A_{k+1} B_k - A_k B_{k+1}}{B_k B_{k+1}} \\ &= \frac{A_k}{B_k} + \left(\frac{A_{k+1}}{B_{k+1}} - \frac{A_k}{B_k} \right) \\ &= \frac{A_{k+1}}{B_{k+1}} = c_{k+1} \end{aligned}$$

Il teorema è dimostrato. ■

Esempio numerico 2.2.8 Il Teorema 2.2.7 vale ovviamente anche se la frazione continua (2.5) è finita. Si verifichi che $541/189 = [2; 1, 6, 3, 1, 2, 2]$; si calcolino le frazioni A_k/B_k $(k = 0, \ldots, 6)$ e si scriva espressamente la somma (finita) (2.16) verificando che è uguale a $541/189$.

SOLUZIONE. Le frazioni A_k/B_k $(k = 0, \ldots, 6)$ sono $2, 3, \frac{20}{7}, \frac{63}{22}, \frac{83}{29}, \frac{229}{80}, \frac{541}{189}$. La corrispondente somma (finita) a segni alterni (2.16) è:

$$2 + \frac{1}{1} - \frac{1}{7} + \frac{1}{154} - \frac{1}{638} + \frac{1}{2320} - \frac{1}{15120} = \frac{541}{189}$$

Il prossimo risultato è, per la teoria degli sviluppi in frazione continua, l'analogo della convergenza delle serie del tipo $a_0 + \sum_{k=1}^{\infty} a_k/10^k$ (dove a_0 è un intero e per $k \geq 1$ gli a_k sono cifre decimali). Per la convergenza di tali serie si usa il criterio del confronto con la serie geometrica di ragione $1/10$, mentre per le frazioni continue si usa il criterio di Leibniz di convergenza delle serie a segni alterni (Cecconi e Stampacchia 1974, Teorema 64.1, p. 274).

Corollario 2.2.9 *Ogni frazione continua infinita* $[a_0;\, a_1, a_2, a_3, \ldots]$ *converge ad un numero reale* α ***irrazionale****.*

Dimostrazione. Proviamo che la serie (2.16) soddisfa le ipotesi del criterio di convergenza di Leibniz per le serie a segni alterni. È già stato notato che la serie (2.16) è a segni alterni almeno dal secondo termine in poi. Assumiamo quindi $k \geq 2$. Per l'Osservazione 2.2.5 si ha $B_{k+2} > B_k$, ossia $B_{k+2}/B_k > 1$, e quindi:

$$\frac{1}{B_k B_{k+1}} = \frac{B_{k+2}}{B_k} \cdot \frac{1}{B_{k+1} B_{k+2}} > \frac{1}{B_{k+1} B_{k+2}}$$

cioè la successione dei moduli dei termini della serie (2.16) è monotona decrescente. Ancora, dalle definizioni $B_1 = a_1$ e $B_2 = a_1 a_2 + 1$ abbiamo $B_1 B_2 \geq 2$. Dalla disuguaglianza:

$$B_{k-1} B_k = B_{k-1} \cdot (a_k B_{k-1} + B_{k-2}) = a_k B_{k-1}^2 + B_{k-1} B_{k-2} > 2\, B_{k-2} B_{k-1}$$

ottenuta utilizzando l'ipotesi $a_k \geq 1$ e la disuguaglianza stretta $B_{k-1} > B_{k-2}$ dell'Osservazione 2.2.5, si deduce che

$$B_{k-1} B_k > 2^{k-1}$$

e quindi il termine generale della serie (2.16) è infinitesimo (e la convergenza della serie è di tipo geometrico).

Resta da provare che $\alpha = \lim_{k\to\infty} [a_0;\, a_1, a_2, \ldots, a_k] = [a_0;\, a_1, a_2, a_3, \ldots]$ è irrazionale.[4] Basterà provare che è irrazionale la mantissa di α, ossia si può assumere $a_0 = 0$. Abbiamo quindi:

$$\alpha = \frac{1}{a_1 + \beta} \qquad \text{dove } \beta = \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots}}}$$

[4] Seguiremo qui l'idea utilizzata da Legendre (1794) per provare che π^2 è irrazionale; una tecnica analoga venne utilizzata da Lambert (1761) per dimostrare che π è irrazionale.

Supponiamo per assurdo che esistano due interi p, q primi fra loro tali che $0 < p < q$, $\alpha = p/q$. Quindi (dalla precedente uguaglianza)

$$\beta = \frac{1}{\alpha} - a_1 = \frac{1 - a_1\alpha}{\alpha} = \frac{1 - a_1(p/q)}{p/q} = \frac{q - a_1 p}{p}$$

da cui β è uguale a una frazione positiva irriducibile che ha un denominatore *minore* del denominatore della frazione che definisce α. Si ripete la stessa procedura con

$$\beta = \frac{1}{a_2 + \gamma}$$

ottenendo ad ogni passaggio un denominatore intero positivo minore del precedente. Ciò è assurdo, dato che si può procedere per una infinità numerabile di passaggi. ■

Osservazione 2.2.10 Se in luogo delle frazioni continue infinite *semplici* (con i "numeratori parziali" tutti uguali ad 1) si considerano quelle *generalizzate* del tipo (2.8), ci si può chiedere se e quando la relativa successione delle "frazioni parziali"

$$c_0 = a_0, \quad c_1 = a_0 + \frac{b_1}{a_1}, \quad c_2 = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2}}, \quad \dots$$

sia convergente oppure no. In generale non è facilissimo costruire esplicitamente una frazione continua generalizzata non convergente.[5]

Esempio numerico 2.2.11 Si consideri la frazione continua generalizzata

$$\cfrac{2}{1 + \cfrac{3}{1 + \cfrac{32}{1 + \cfrac{135}{1 + \cfrac{384}{1 + \cfrac{875}{1 + \ddots}}}}}} \tag{2.18}$$

definita, con i simboli di (2.8), da $a_0 = 0$, $a_k = 1$ per $k \geq 1$, $b_1 = 2$, $b_k = (k-1)^3(k+1)$ per $k \geq 2$. Utilizzando le formule (2.16) ed una calcolatrice

[5] A differenza dal caso delle serie numeriche, in cui esibire una serie non convergente è in complesso abbastanza banale.

simbolica (o un sistema di computer algebra) si verifichi che i valori A_k/B_k per $0 \leq k \leq 11$ sono:

$$0,\ 2,\ \frac{1}{2},\ \frac{11}{6},\ \frac{7}{12},\ \frac{107}{60},\ \frac{37}{60},\ \frac{739}{420},\ \frac{533}{840},\ \frac{4399}{2520},\ \frac{1627}{2520},\ \frac{48137}{27720}$$

e che le differenze $r_k = A_{k+1}/B_{k+1} - A_k/B_k$ per $0 \leq k \leq 10$ sono:

$$2,\ -\frac{3}{2},\ \frac{4}{3},\ -\frac{5}{4},\ \frac{6}{5},\ -\frac{7}{6},\ \frac{8}{7},\ -\frac{9}{8},\ \frac{10}{9},\ -\frac{11}{10},\ \frac{12}{11}$$

Questo porta a congetturare che la successione $(r_k)_{k\geq 0}$ *sia* la successione $r_k = (-1)^k \frac{k+1}{k}$, che ha due distinti punti limite $+1$ e -1 (Cecconi e Stampacchia 1974, p. 108, Esempio 1); questa congettura, o "induzione logica", può essere dimostrata formalmente. Si conclude che la successione A_k/B_k è indeterminata e conseguentemente, per definizione, la frazione (2.18) ***non*** è convergente.

Un altro esempio di frazione continua generalizzata ***non*** convergente è la frazione del tipo di Rogers–Ramanujan (Chrystal 1900, Part II, Ex. 2, p. 509).

$$\cfrac{2}{1+\cfrac{4}{1+\cfrac{8}{1+\cfrac{16}{1+\cfrac{32}{1+\cfrac{64}{1+\ddots}}}}}} \tag{2.19}$$

dove si ha $a_0 = 0$, e per $k \geq 1$ si ha $a_k = 1$ e $b_k = 2^k$. Qui ci limitiamo a calcolare nella Tabella 2.1 le "frazioni parziali" A_k/B_k per $1 \leq k \leq 16$, ordinate in modo crescente. La non–convergenza dipende dal fatto che la distanza fra due successivi valori della successione c_k decresce, ma non tende a zero.

2.3 Sviluppo in frazione continua dei razionali

Vedremo ora che ogni numero razionale positivo può essere "sviluppato" in frazione continua finita e che questo sviluppo finito è unico sotto la condizione che l'ultimo termine dello sviluppo sia $\neq 1$.

$c_2 = \frac{2}{5}$	$= 0.4$
$c_4 = \frac{50}{93}$	$= 0.537634$
$c_6 = \frac{3826}{6461}$	$= 0.592168$
$c_8 = \frac{1063410}{1725629}$	$= 0.616245$
$c_{10} = \frac{1132979698}{1805435581}$	$= 0.627538$
$c_{12} = \frac{4732027835890}{7475495336637}$	$= 0.633005$
$c_{14} = \frac{78282557888746994}{123144883455482557}$	$= 0.635695$
$c_{16} = \frac{5155078753389622613490}{8092381769059159562941}$	$= 0.637029$
$\ldots$	$\ldots$
$c_{15} = \frac{24753039592699614706}{21958686920654707389}$	$= 1.12725$
$c_{13} = \frac{753013825525234}{666367860021949}$	$= 1.13003$
$c_{11} = \frac{91342992882}{80431196861}$	$= 1.13567$
$c_9 = \frac{44047858}{38391485}$	$= 1.14733$
$c_7 = \frac{83954}{71613}$	$= 1.17233$
$c_5 = \frac{626}{509}$	$= 1.22986$
$c_3 = \frac{18}{13}$	$= 1.38462$
$c_1 = 2$	$= 2.$

Tabella 2.1: Tabulazione in ordine crescente delle "frazioni parziali" c_k per $1 \leq k \leq 16$ di una frazione del tipo di Rogers–Ramanujan.

2.3.1 Algoritmo euclideo della divisione

La dimostrazione dell'esistenza dello sviluppo in frazione continua finita di un razionale α si basa sostanzialmente sull'algoritmo euclideo per il calcolo del MCD di due interi positivi (Teoremi B.1.1 e B.1.3).

Teorema 2.3.1 *Sia $\alpha = u_0/u_1$ un numero razionale positivo, con u_0, u_1 interi positivi primi fra loro. Esistono un intero $n \geq 0$ ed una $(n+1)$–pla $(a_0, a_1, a_2, \ldots, a_n)$ di numeri interi, con $a_0 \geq 0$, $a_k \geq 1$ per $1 \leq k < n$, ed $a_n \geq 2$, tali che*

$$\alpha = \frac{u_0}{u_1} = [a_0;\, a_1, a_2, \ldots, a_n]$$

DIMOSTRAZIONE. Sia dato il numero razionale $\alpha = u_0/u_1$, con u_0, u_1 interi positivi primi fra loro, ossia $\text{MCD}(u_0, u_1) = 1$. Per non appesantire la dimostrazione, ci riferiamo ad un esempio specifico: $u_0 = 43200$ ed $u_1 = 10463$. L'algoritmo delle divisioni successive per il calcolo del $\text{MCD}(u_0, u_1)$ conduce ad una tabella come la seguente:[6]

$$\begin{array}{rcrcrll}
43200 & = & 4 \times 10463 & + & 1348 & u_0 = a_0 \cdot u_1 + u_2 & \text{(passo 0)} \\
10463 & = & 7 \times 1348 & + & 1027 & u_1 = a_1 \cdot u_2 + u_3 & \text{(passo 1)} \\
1348 & = & 1 \times 1027 & + & 321 & u_2 = a_2 \cdot u_3 + u_4 & \text{(passo 2)} \\
1027 & = & 3 \times 321 & + & 64 & u_3 = a_3 \cdot u_4 + u_5 & \text{(passo 3)} \\
321 & = & 5 \times 64 & + & 1 & u_4 = a_4 \cdot u_5 + u_6 & \text{(passo 4)} \\
64 & = & 64 \times 1 & + & 0 & u_5 = a_5 \cdot u_6 & \text{(passo 5)}
\end{array}$$

Qui l'algoritmo si è arrestato al passo $n = 5$, quando ha dato resto nullo. Supponiamo che, in generale, l'algoritmo si arresti al passo $n \geq 1$ (non può arrestarsi al passo $n = 0$ in quanto per ipotesi u_0, u_1 sono primi fra loro). Si ha sempre ovviamente $a_0 \geq 0$ (risulta $a_0 = 0$ quando $u_0 < u_1$). Si ha $a_n \geq 2$, in quanto, essendo u_{n+1} il resto di un divisione intera per u_n, si ha $u_{n+1} < u_n$, e quindi $a_n = u_n/u_{n+1} > 1$; gli a_k con $1 \leq k \leq n-1$ (se ne esistono) sono tutti ≥ 1 in quanto sono quozienti di divisioni intere di numeri positivi. Nel caso concreto in esame abbiamo:

$$\frac{43200}{10463} = [4;\, 7, 1, 3, 5, 64] = [a_0;\, a_1, a_2, a_3, a_4, a_5]$$

[6] Ricordiamo che in questo algoritmo la sequenza dei resti delle divisioni successive è strettamente decrescente, e quindi ad un certo passo si deve necessariamente ottenere un resto nullo; il $\text{MCD}(u_0, u_1)$ è allora il resto della divisione precedente.

$$
\begin{aligned}
\frac{43200}{10463} &= 4 + \frac{1348}{10463} \\
&= 4 + \frac{1}{\frac{10463}{1348}} = 4 + \frac{1}{7 + \frac{1027}{1348}} \\
&= 4 + \frac{1}{7 + \frac{1}{\frac{1348}{1027}}} = 4 + \frac{1}{7 + \frac{1}{1 + \frac{321}{1027}}} \\
&= 4 + \frac{1}{7 + \frac{1}{1 + \frac{1}{\frac{1027}{321}}}} = 4 + \frac{1}{7 + \frac{1}{1 + \frac{1}{3 + \frac{64}{321}}}} \\
&= 4 + \frac{1}{7 + \frac{1}{1 + \frac{1}{3 + \frac{1}{\frac{321}{64}}}}} = \mathbf{4} + \frac{1}{\mathbf{7} + \frac{1}{\mathbf{1} + \frac{1}{\mathbf{3} + \frac{1}{\mathbf{5} + \frac{1}{\mathbf{64}}}}}}
\end{aligned}
$$

Tabella 2.2: Sviluppo in frazione continua finita di $\alpha = 43200/10463$ con le successive frazioni "a più piani".

La genesi di questa rappresentazione è forse più chiara se si rappresentano i passi successivi dello sviluppo di $\alpha = 43200/10463$ con le frazioni "a più piani": si veda la Tabella 2.2. ■

2.3.2 Doppia rappresentazione dei razionali

Proseguendo l'esempio precedente, è evidente che la rappresentazione trovata non è "unica". Si ha infatti $[4;\, 7, 1, 3, 5, 64] = [4;\, 7, 1, 3, 5, 63, 1]$, dato che

$$5 + \frac{1}{64} = 5 + \frac{1}{63 + \frac{1}{1}}$$

In generale abbiamo sempre un doppio sviluppo dei numeri razionali come frazione continua finita, in quanto evidentememte:

$$[a_0;\, a_1, a_2, \ldots, a_{n-1}, a_n] = [a_0;\, a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1]$$

Comunque, queste due rappresentazioni dei razionali come frazioni continue sono le uniche possibili. Si ha infatti:

Teorema 2.3.2 *Se* $[a_0;\, a_1, a_2, \ldots, a_n] = [b_0;\, b_1, b_2, \ldots, b_m]$ *con* a_0, b_0 *interi* ≥ 0, *e con* a_k, b_k *interi positivi per* $k \geq 1$ *e* $a_n \geq 2$, $b_m \geq 2$, *allora si ha* $n = m$ *e per ogni* $0 \leq k \leq n$ *si ha* $a_k = b_k$.

DIMOSTRAZIONE. Lasciamo la dimostrazione (per induzione) alla cura del lettore. ■

Vi è quindi in conclusione un'analogia parziale fra lo sviluppo decimale di un numero razionale positivo ed il suo sviluppo in frazione continua finita. Nel caso dello sviluppo decimale di un numero razionale positivo abbiamo sviluppi "illimitati" e periodici, ed inoltre la eventuale doppia rappresentazione (0−periodica e 9−periodica) riguarda i *soli* razionali che moltiplicati per una potenza di 10 danno un intero. Nel caso dello sviluppo di un numero razionale positivo in frazione continua finita, abbiamo sviluppi finiti, e la doppia rappresentazione riguarda *tutti* i razionali, ma in questo caso è semplice privilegiarne una da scegliere come *canonica*: viene prescelta quella "più corta", con l'ultimo quoziente $a_k \geq 2$, come viene prodotto automaticamente dall'algoritmo euclideo del MCD.

2.4 Sviluppo in frazione continua degli irrazionali

Nel Capitolo 1 abbiamo dimostrato l'esistenza dello sviluppo decimale di un numero reale $\alpha \geq 0$. In questo capitolo abbiamo già visto che, ovviamente, ogni frazione continua finita è un numero razionale ed anche che ogni numero razionale (positivo) ha uno sviluppo in frazione continua finita (unico sotto la condizione che l'ultimo termine sia ≥ 2). Nella sezione precedente abbiamo visto che ogni frazione continua infinita converge a (o se si preferisce è) un numero irrazionale. Per continuare nel confronto fra i due tipi di sviluppo proveremo ora che ogni numero irrazionale positivo ha uno sviluppo in frazione continua infinita, e che questo sviluppo è unico (enfatizzando che si tratta di frazione continua semplice).

2.4.1 Esistenza degli sviluppi in frazione continua

Teorema 2.4.1 *Per ogni numero reale* ***irrazionale*** $\alpha > 0$ *esistono un intero* $a_0 \geq 0$ *ed una successione* $(a_k)_{k\geq 1}$ *di interi positivi tali che*

$$\alpha = \lim_{k\to\infty} [a_0;\, a_1, a_2, \ldots, a_k] = [a_0;\, a_1, a_2, a_3, \ldots]$$

DIMOSTRAZIONE. Sia dato un numero irrazionale $\alpha > 0$. Utilizziamo la funzione *parte intera* $x \mapsto [x]$ che associa ad x il massimo intero $\leq x$. Definiamo induttivamente una successione $(\xi_k)_{k\geq 0}$ di numeri reali

$$\begin{cases} \xi_0 = \alpha \\ \xi_k = \dfrac{1}{\xi_{k-1} - [\xi_{k-1}]} \quad \text{per } k \geq 1 \end{cases} \tag{2.20}$$

ed una successione di interi $(a_k)_{k\geq 0}$ ponendo $a_k = [\xi_k]$. Evidentemente $a_0 = [\alpha] \geq 0$. Se per un indice $k \geq 1$ fosse $\xi_{k-1} - [\xi_{k-1}] = 0$, allora $\xi_{k-1} = 1/(\xi_{k-2} - [\xi_{k-2}])$ sarebbe intero, e quindi ξ_{k-2} sarebbe razionale; proseguendo a ritroso, avremmo l'assurdo che ξ sarebbe razionale. Quindi le due successioni sono ben definite e si ha $a_k \geq 1$ per $k \geq 1$. La frazione continua $[a_0;\, a_1, a_2, a_3, \ldots]$ è quindi infinita e converge ad un irrazionale: mostriamo che converge proprio ad α. Con la simbologia delle frazioni continue finite possiamo scrivere:

$$\alpha = [a_0;\, a_1, a_2, \ldots, a_{k-1}, \xi_k]$$

Come visto in precedenza, la frazione continua finita $[a_0;\, a_1, \ldots, a_{k-1}, \xi_k]$ può essere riscritta come una frazione formale con un unico denominatore:[7]

$$\alpha = \frac{\xi_k A_{k-1} + A_{k-2}}{\xi_k B_{k-1} + B_{k-2}} \tag{2.21}$$

dove gli A ed i B sono gli interi calcolati dalle formule di Eulero a partire dalla frazione $[a_0;\, a_1, a_2, \ldots]$ (senza far intervenire l'irrazionale ξ_k ma solo gli interi $a_0, a_1, a_2, \ldots, a_{k-1}$). Possiamo quindi calcolare la differenza fra α e la $(k-1)$–esima convergente della frazione $[a_0;\, a_1, a_2, \ldots]$:

$$\begin{aligned} \frac{A_{k-1}}{B_{k-1}} - \alpha &= \frac{A_{k-1}}{B_{k-1}} - \frac{\xi_k A_{k-1} + A_{k-2}}{\xi_k B_{k-1} + B_{k-2}} \\ &= \frac{A_{k-1}\xi_k B_{k-1} + A_{k-1}B_{k-2} - B_{k-1}\xi_k A_{k-1} - B_{k-1}A_{k-2}}{B_{k-1}\,(\xi_k B_{k-1} + B_{k-2})} \\ &= \frac{A_{k-1}B_{k-2} - B_{k-1}A_{k-2}}{B_{k-1}\,(\xi_k B_{k-1} + B_{k-2})} \\ &= \frac{(-1)^{k-2}}{B_{k-1}\,(\xi_k B_{k-1} + B_{k-2})} \end{aligned} \tag{2.22}$$

dove la identità $A_{k-1}B_{k-2} - B_{k-1}A_{k-2} = (-1)^{k-2}$ viene dalla (2.11). Dato che $\xi_k > 0$ e $B_k \to \infty$, si ha $[a_0;\, a_1, \ldots, a_{k-1}] \to \alpha$. ■

[7] Come nell'esempio fornito in precedenza: $\alpha = [3; 4, 5, \xi] = \dfrac{13 + 68\,\xi}{4 + 21\,\xi}$.

Esempio numerico 2.4.2 Consideriamo $\alpha = \sqrt{3}$, che è un irrazionale algebrico di grado 2, cioè un irrazionale quadratico (Definizione B.3.21). Il polinomio minimo di α è $p_0(x) = x^2 - 3$, ed è questo che consente di *definire* $\sqrt{3}$ come numero reale, in quanto consente di definire la sezione di Dedekind (A', A''), che **è** il numero $\sqrt{3}$. Ad esempio, per ottenere $a_0 = [\sqrt{3}] = 1$ basta osservare che $p_0(1) = 1^2 - 3 < 0 < 2^2 - 3 = p_0(2)$. Per calcolare $a_1 = [1/(\sqrt{3} - 1)]$ basta considerare il polinomio minimo di $1/(\sqrt{3} - 1) = \frac{1}{2}(1 + \sqrt{3})$, che è $p_1(x) = x^2 - x - \frac{1}{2}$, e verificare che $p_1(1) < 0 < p_1(2)$: quindi $a_1 = 1$. Questo processo prosegue con il calcolo di $a_2 = [1/(\frac{1}{2}(1 + \sqrt{3}) - 1)] = [1 + \sqrt{3}] = 2$.

In generale, vogliamo enfatizzare che lo sviluppo in frazione continua di un numero algebrico si può effettuare in linea di principio nell'ambito dell'aritmetica intera usando i polinomi minimi, quindi senza ricorrere (artificiosamente) al calcolo dello sviluppo decimale.

È chiaro che se si ammette di sapere che $\sqrt{3} = 1.73205\ldots$, si ottiene immediatamente che $a_0 = [\sqrt{3}] = 1$, $a_1 = [1/0.73205\ldots] = [1.366025\ldots] = 1$, $a_2 = [1/0.366025\ldots] = [2.73205\ldots] = 2$, ecc., ma si deve ricorrere all'aritmetica (in virgola fissa o in virgola mobile) dei numeri reali.

Esempio numerico 2.4.3 Consideriamo $\alpha = \pi$. A differenza del caso $\alpha = \sqrt{3}$, non abbiamo qui a disposizione alcun metodo *elementare* che ci consenta di effettuare calcoli "esatti" con π. Ci dobbiamo quindi "fidare" di uno sviluppo decimale, ad esempio, del tipo $\pi \approx 3.14159265359$, che ha 11 cifre decimali dopo la virgola. Come scelta immediata possiamo riprodurre l'algoritmo (2.20) con una calcolatrice (con la divisione) che memorizzi i numeri con 12 cifre. I primi termini dello sviluppo di π risultano allora:

$$
\begin{aligned}
\xi_0 &= 3.14159265359 && a_0 = 3\\
\xi_1 &= 1/0.14159265359 = 7.06251330592 && a_1 = 7\\
\xi_2 &= 1/0.06251330592 = 15.9965944095 && a_2 = 15\\
\xi_3 &= 1/0.99659440950 = 1.00341722818 && a_3 = 1\\
\xi_4 &= 1/0.00341722818 = 292.634833650 && a_4 = 292\\
\xi_5 &= 1/0.63483365000 = 1.57521580653 && a_5 = 1\\
\xi_6 &= 1/0.57521580653 = 1.73847795670 && a_6 = 1\\
\xi_7 &= 1/1.73847795670 = 1.35413656011 && a_7 = 1\\
\xi_8 &= 1/0.35413656011 = 2.82376945122 && a_8 = 2\\
&\ldots
\end{aligned}
$$

Lo sviluppo di π calcolato è quindi:

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{\ddots}}}}} \tag{2.23}$$

oppure, in forma compatta:

$$\pi = [3;\, 7, 15, 1, 292, 1, 1, 1, 2 \ldots]$$

e questo è effettivamente lo sviluppo corretto fino al termine a_8. Se invece la nostra calcolatrice avesse soltanto 10 cifre, avremmo l'approssimazione 3.141592654 per π e lo sviluppo verrebbe:

$$\begin{aligned}
\xi_0 &= 3.141592654 && a_0 = 3 \\
\xi_1 &= 1/0.141592654 = 7.062513285 && a_1 = 7 \\
\xi_2 &= 1/0.062513285 = 15.99659976 && a_2 = 15 \\
\xi_3 &= 1/0.996599760 = 1.003461968 && a_3 = 1 \\
\xi_4 &= 1/0.003461968 = 288.8530454 && a_4 = 288 \\
&\ldots
\end{aligned}$$

con un errore nel termine a_4. Alternativamente, si può calcolare lo sviluppo in frazione continua finita del razionale 314159265359/100000000000 con l'algoritmo euclideo, come nella Tabella 2.3.

Lagrange, nelle *Additions* all'*Algèbre* di Eulero (1774), utilizza l'approssimazione L di π a 35 cifre decimali calcolata da Ludolph van Ceulen (1540–1610) ed incisa sulla sua pietra tombale nella chiesa di St. Pieterskerk a Leida (Olanda):[8]

$$L = 3.14159265358979323846264338327950288 < \pi < L + 10^{-35}$$

e ottiene[9] che

$$\pi \approx [3; 7{,}15{,}1{,}292{,}1{,}1{,}1{,}2{,}1{,}3{,}1{,}14{,}2{,}1{,}1{,}2{,}2{,}2{,}2{,}1{,}84{,}2{,}1{,}1{,}15{,}3{,}13{,}1{,}4{,}2{,}6{,}6{,}1]$$

[8] Per la curiosa storia di questo epitaffio si veda Oomes *et al.* (2000).

[9] Lagrange non specifica il metodo di calcolo; tuttavia le ultime cifre dello sviluppo che propone non sono coerenti con il valore di Ludolph.

$$
\begin{aligned}
314159265359 &= 100000000000 \times 3 + 14159265359 \\
100000000000 &= 14159265359 \times 7 + 885142487 \\
14159265359 &= 885142487 \times 15 + 882128054 \\
885142487 &= 882128054 \times 1 + 3014433 \\
882128054 &= 3014433 \times 292 + 1913618 \\
3014433 &= 1913618 \times 1 + 1100815 \\
1913618 &= 1100815 \times 1 + 812803 \\
1100815 &= 812803 \times 1 + 288012 \\
812803 &= 288012 \times 2 + 236779 \\
288012 &= 236779 \times 1 + 51233 \\
236779 &= 51233 \times 4 + 31847 \\
51233 &= 31847 \times 1 + 19386 \\
31847 &= 19386 \times 1 + 12461 \\
19386 &= 12461 \times 1 + 6925 \\
12461 &= 6925 \times 1 + 5536 \\
6925 &= 5536 \times 1 + 1389 \\
5536 &= 1389 \times 3 + 1369 \\
1389 &= 1369 \times 1 + 20 \\
1369 &= 20 \times 68 + 9 \\
20 &= 9 \times 2 + 2 \\
9 &= 2 \times 4 + 1 \\
2 &= 1 \times 2 + 0
\end{aligned}
$$

Tabella 2.3: Sviluppo in frazione continua del numero razionale $\alpha = 3.14159265359$ basato sull'algoritmo euclideo della divisione o del MCD.

Questo esempio evidenzia in generale un problema di continuità: è possibile definire una metrica nelle sequenze di interi positivi $(a_k)_{k\geq 1}$ in modo che, posta la metrica euclidea nell'intervallo $[0,1)$, l'applicazione che ad $x \in [0,1)$ fa corrispondere il suo sviluppo (finito o infinito) in frazione continua $[0;\, a_1, a_2, a_3, \ldots]$ sia continua ad eccezione di un insieme numerabile? E se sì, quale è questo insieme di punti di discontinuità? Questo è un problema che si incontra già nel caso dello sviluppo decimale (Fiori e Invernizzi 2009, pp. 98–99): ad esempio $\frac{1}{2}$ e $\frac{1}{2} - 10^{-12}$ sono numeri reali "vicini" ma hanno sviluppi decimali "distanti", precisamente $0.5000000000000000\ldots$ e $0.499999999999000\ldots$. In sostanza, data una "buona" approssimazione razionale r di π, non abbiamo per ora motivi per ritenere che un "segmento iniziale" dello sviluppo in frazione continua (infinita) di π coincida con lo sviluppo in frazione continua (finita) di r. Ritorneremo su questo problema nella Sezione 2.13.

Esercizio 2.4.4 Si calcolino i primi termini dello sviluppo di $\log 2$ in frazione continua assumendo l'approssimazione $\log 2 = 0.693147$. Si verifichi ancora, numericamente, che la serie (2.16) relativa allo sviluppo ottenuto è del tipo:

$$\log 2 = 1 - \frac{1}{3} + \frac{1}{30} - \frac{1}{130} + \frac{1}{1144} - \frac{1}{24376} + \ldots \tag{2.24}$$

Soluzione.

$$\log 2 = \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{6 + \cfrac{1}{\ddots}}}}}} \tag{2.25}$$

■

Si osservi, intuitivamente, che la serie (2.24) ha una convergenza a $\log(2)$ "molto più veloce" della convergenza della serie armonica a segni alterni che rappresenta $\log(2)$ nei trattati di analisi matematica (Cecconi e Stampacchia, 1974. p. 403):

$$\log 2 = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \ldots$$

Quest'osservazione è formalizzata nel prossimo esercizio.

Esercizio 2.4.5 Si dimostri che, per una frazione continua $[a_0;\, a_1, a_2, \ldots]$, le convergenti A_k/B_k come definite dalle formule di Eulero, verificano per ogni $k \geq 2$ la disuguaglianza

$$B_k \geq 2^{\frac{k-1}{2}} \tag{2.26}$$

SOLUZIONE. Per $k \geq 2$,

$$B_k = a_k B_{k-1} + B_{k-2} \geq B_{k-1} + B_{k-2} \geq 2\, B_{k-2}$$

Successive applicazioni di questa disuguaglianza danno:

$$B_{2k} \geq 2^k B_0 = 2^k > 2^{k-\frac{1}{2}}, \quad B_{2k+1} \geq 2^k B_1 \geq 2^k$$

■

2.4.2 Unicità degli sviluppi in frazione continua

Come per lo sviluppo decimale, vale un teorema di unicità per lo sviluppo in frazione continua dei numeri irrazionali.

Teorema 2.4.6 *Per ogni numero irrazionale α esiste una ed una sola frazione continua* ***infinita, semplice*** $[a_0;\, a_1, a_2, \ldots]$ *che converge ad α.*

DIMOSTRAZIONE. C'è solo da provare l'unicità. Supponiamo che

$$\alpha = [a_0;\, a_1, a_2, \ldots] = [a'_0;\, a'_1, a'_2, \ldots]$$

Per prima cosa, visto che nella rappresentazione $\alpha = a_0 + 1/(a_1 + \ldots)$ si ha necessariamente che $1/(a_1 + \ldots) < 1$ (la frazione $[a_0;\, a_1, a_2, \ldots]$ non è finita, altrimenti α sarebbe razionale) è ovvio che $a_0 = [\alpha]$ e che anche $a'_0 = [\alpha]$, per cui $a_0 = a'_0$. Supponiamo di aver provato che $a_k = a'_k$ per i $k \leq n-1$. Allora, con notazioni analoghe, abbiamo $A_k = A'_k$ e $B_k = B'_k$ per i $k \leq n-1$. Riprendendo la (2.21) e con analoghe notazioni abbiamo allora

$$\alpha = \frac{A_n}{B_n} = \frac{\xi_n A_{n-1} + A_{n-2}}{\xi_n B_{n-1} + B_{n-2}} = \frac{\xi'_n A'_{n-1} + A'_{n-2}}{\xi'_n B'_{n-1} + B'_{n-2}} = \frac{\xi'_n A_{n-1} + A_{n-2}}{\xi'_n B_{n-1} + B_{n-2}}$$

per cui deve essere $\xi_n = \xi'_n$, e visto che $a_n = [\xi_n]$ e $a'_n = [\xi'_n]$ si conclude che $a_n = a'_n$, per cui le due frazioni coincidono in ogni termine. ■

2.5 Un quadrato è equipotente ad un intervallo

Possiamo ora dimostrare il famoso teorema sull'uguaglianza delle cardinalità di $[0,1)$ e di $[0,1) \times [0,1)$ introdotto nella precedente Sezione 1.2. Esporremo la dimostrazione comunicata da Cantor a Dedekind nella lettera del 25 giugno 1877 e pubblicata l'anno seguente (Cantor, 1878).

Teorema 2.5.1 (Cantor, 1878) *Esiste un'applicazione biiettiva*

$$f : [0,1) \to [0,1) \times [0,1)$$

DIMOSTRAZIONE. Indichiamo con $J = [0,1) \setminus \mathbb{Q}$ l'insieme costituito dai numeri irrazionali di $[0,1)$, e con $\mathcal{F}$ l'insieme delle successioni di numeri interi $(a_n)_{n\geq 0}$, tali che, per ogni $n \geq 0$, sia $a_n \geq 1$. Per quanto visto in questo capitolo, esiste una funzione biiettiva $\varphi : J \to \mathcal{F}$ che associa ad $\alpha \in J$ la successione $(a_n)_{n\geq 1}$ degli interi ≥ 1 nello sviluppo in frazione continua $\alpha = [0;\, a_1, a_2, \ldots]$. Ora si considerino le frazioni continue $[0;\, a_1, a_3, a_5 \ldots]$ e $[0;\, a_2, a_4, a_6, \ldots]$ formate rispettivamente con i termini di indice dispari e di indice pari nella $(a_n)_{n\geq 1}$, e poniamo $u = [0;\, a_1, a_3, a_5 \ldots]$ e $v = [0;\, a_2, a_4, a_6, \ldots]$. Evidentemente $u \in J$, $v \in J$, e l'applicazione $\alpha \in J \mapsto (u, v) \in J \times J$ è biiettiva. Per concludere la dimostrazione basta osservare che esiste un'applicazione biiettiva ovvia fra J e $[0,1)$, ottenibile selezionando in J una successione di irrazionali (ad esempio $x_k = \sqrt{2}/2^k$, per $k \geq 1$) ed utilizzandone i termini di posto dispari per rappresentare la successione stessa e quelli di posto dispari per rappresentare i razionali di $[0,1)$, che sono numerabili.[10] ■

2.6 Esempi di applicazioni

2.6.1 Calcolo numerico

È ancora dovuto ad Eulero (Khovanskii, 1963) uno sviluppo in frazione continua generalizzata della funzione esponenziale:

$$e^x = 1 + \cfrac{2x}{2 - x + \cfrac{x^2}{6 + \cfrac{x^2}{10 + \cfrac{x^2}{14 + \cfrac{x^2}{18 + \ddots}}}}}$$

[10] L'argomento è quello che nel successivo *folklore* matematico verrà chiamato "l'albergo di Hilbert" (Gamow, 1947, pp. 17–18). L'albergo di Hilbert è un albergo ideale che ha una quantità numerabile di stanze, la 1, la 2, la 3, ecc., ed è tutto completo; durante la notte arriva un pullman che trasporta una quantità numerabile di persone, ciascuna delle quali chiede una stanza per sè. Il portiere riesce a sistemarle tutte, spostando l'ospite della 1 nella 2, quello della 2 nella 4, quello della 3 nella 6, ..., in generale quello della n nella $2n$, ..., liberando così tutte le stanze di numero dispari, che può assegnare ai clienti del pullman. In termini attuali, l'albergo di Hilbert è una metafora del fatto che se E è un insieme infinito si ha $|E| + \aleph_0 = |E|$; per provare questa uguaglianza in generale, serve l'assioma della scelta, ma, se $E = J$, per estrarre da E un insieme numerabile non serve la scelta.

che si riduce (troncando ai termini indicati) alla funzione razionale fratta di grado 5 seguente:

$$e^x \approx \frac{30240 + 15120\,x + 3360\,x^2 + 420\,x^3 + 30\,x^4 + x^5}{30240 - 15120\,x + 3360\,x^2 - 420\,x^3 + 30\,x^4 - x^5}$$

Il massimo modulo dell'errore in questa approssimazione per $0 \le x \le 1$ si ha in $x = 1$ ed è 2.76651×10^{-10}. Usando invece l'approssimazione della formula di Taylor, per ottenere un errore comparabile con quello della frazione continua bisogna spingere la formula di Taylor fino al grado 12:

$$e^x \approx 1 + x + \frac{x^2}{2} + \frac{x^3}{6} + \frac{x^4}{24} + \frac{x^5}{120} + \frac{x^6}{720} + \ldots + \frac{x^{10}}{3628800} + \frac{x^{11}}{39916800} + \frac{x^{12}}{479001600}$$

in modo da ottenere un errore in modulo $\le 1.72876 \times 10^{-10}$. Si noti che l'approssimazione con la frazione continua richiede il calcolo delle potenze intere di x fino al grado 5 (e non 12) e soprattutto *una sola divisione*, in più *fra numeri dello stesso ordine di grandezza.*

In altri termini, se cerchiamo delle frazioni che approssimino e con un errore dell'ordine di grandezza di 10^{-10} tramite la teoria delle frazioni continue, tramite la formula di Taylor e tramite lo sviluppo decimale, otteniamo rispettivamente le tre approssimazioni seguenti (già ridotte ai minimi termini):

$$e \approx \frac{49\,171}{18\,089}, \quad e \approx \frac{260\,412\,269}{95\,800\,320}, \quad e \approx \frac{679\,570\,457}{250\,000\,000}$$

dove si vede che la peggiore (in termini di dispendio di cifre) è la decimale, con ben 9 cifre al denominatore, preceduta dalla formula di Taylor con 8 cifre al denominatore, e soprattutto preceduta dalla convergente $A_{13}/B_{13} = 49171/18089$ dello sviluppo in frazione continua di e, che ha un denominatore di sole 5 cifre.

2.7 Le frazioni continue periodiche

Sappiamo che lo sviluppo decimale può essere pensato come un'applicazione che ad ogni numero *reale* $\alpha > 0$ associa un'unica successione di interi $(a_k)_{k\ge 0}$ dove $a_0 \ge 0$, $0 \le a_k \le 9$ per $k \ge 1$, e che non sia 0–periodica[11] in modo che risulti

$$\alpha = a_0.\, a_1 a_2 a_3 a_4 \ldots$$

Questa "codifica" distingue i numeri *reali* fra razionali e irrazionali, nel senso che α è *razionale* se e solo se la successione di interi $(a_k)_{k\ge 0}$ associatagli come

[11] Equivalentemente: che non sia 9–periodica.

sopra specificato dallo sviluppo decimale è una successione definitivamente *periodica* (cioè periodica da un certo indice in poi).

Anche lo sviluppo in frazione continua (infinita, semplice) può essere pensato come un'applicazione che ad ogni numero *reale irrazionale* $\alpha > 0$ associa un'unica successione di interi $(a_k)_{k\geq 0}$ dove $a_0 \geq 0$, $a_k \geq 1$ per $k \geq 1$, in modo che risulti

$$\alpha = [a_0;\, a_1, a_2, a_3, a_4, \ldots]$$

Vedremo in questa sezione che questa seconda "codifica" distingue i numeri *irrazionali* fra algebrici di grado 2 e gli altri irrazionali, nel senso che α è un *irrazionale quadratrico* se e solo se la successione di interi $(a_k)_{k\geq 0}$ associatagli come sopra specificato dallo sviluppo in frazione continua è una successione definitivamente *periodica* (periodica da un certo indice in poi). Questi risultati sono ancora dovuti ad Eulero per il "se" ed a Lagrange per il "solo se".

Teorema 2.7.1 (di Eulero–Lagrange sulle frazioni periodiche) *Un numero irrazionale con sviluppo in frazione continua* $\alpha = [a_0;\, a_1, a_2, a_3 \ldots]$ *è un irrazionale quadratico (un numero algebrico di grado* 2*) se e solo se la successione* $(a_k)_{k\geq 0}$ *è definitivamente periodica.*

Ricordiamo che una successione $(a_k)_{k\geq 0}$ è *definitivamente periodica* esistono interi n ed s tali che per $r > s$ sia $a_r = a_{n+r}$.

Dimostrazione. Supponiamo che lo sviluppo di α sia periodico e che quindi si possa scrivere, cambiando i simboli, nella forma:

$$\alpha = [\underbrace{b_0;\, b_1, \ldots, b_s}_{\text{antiperiodo}},\ \underbrace{a_0, a_1, \ldots, a_{n-1}}_{\text{periodo}},\ \underbrace{a_0, a_1, \ldots, a_{n-1}}_{\text{periodo}},\ \underbrace{a_0, a_1, \ldots, a_{n-1}}_{\text{periodo}},\ \ldots\,] \tag{2.27}$$

Poniamo

$$\begin{aligned} \theta &= [\,\underbrace{a_0; a_1, \ldots, a_{n-1}}_{\text{periodo}},\ \underbrace{a_0, a_1, \ldots, a_{n-1}}_{\text{periodo}},\ \underbrace{a_0, a_1, \ldots, a_{n-1}}_{\text{periodo}},\ \ldots\ldots\,] \\ &= [\,\underbrace{a_0; a_1, \ldots, a_{n-1}}_{\text{periodo}},\ \theta\,] \end{aligned}$$

▼ Ad esempio:

$$\begin{aligned}\alpha &= [\ \underbrace{2;\ 3}_{\text{antiperiodo}}\ ,\ \underbrace{4,\ 5}_{\text{periodo}}\ ,\ \ 4,\ \ 5,\ \dots\ ] \\ &= 2+\cfrac{1}{3+\cfrac{1}{\boxed{(\theta=)\ 4+\cfrac{1}{5+\cfrac{1}{\boxed{(\theta=)\ 4+\cfrac{1}{5+\ddots}}}}}}}\end{aligned}$$

e pertanto $\theta = [4;\ 5, \theta]$; le convergenti di questa frazione continua finita sono:

$$[4;] = \frac{A_0}{B_0} = \frac{4}{1}, \quad [4;5] = \frac{A_1}{B_1} = 4 + \frac{1}{5} = \frac{21}{5}, \quad \theta = [4;\ 5, \theta] = \frac{A_2}{B_2} = \frac{\theta \cdot 21 + 4}{\theta \cdot 5 + 1}$$

▲

In generale, per la (2.21) con $\theta = \xi_k$ abbiamo un'uguaglianza del tipo

$$\theta = [a_0;\ a_1, a_2, \dots, a_{n-1}, \theta] = \frac{\theta A' + A''}{\theta B' + B''} \tag{2.28}$$

con A', A'', B', B'' interi. Quindi θ è la soluzione positiva dell'equazione algebrica di grado 2 a coefficienti interi:

$$B'\theta^2 + (B'' - A')\theta - A'' = 0$$

(questa equazione, quale che sia il segno di $(B'' - A')$ ha sempre una permanenza ed una variazione, e quindi per la regola di Cartesio ha certamente una radice positiva) e quindi θ è un razionale o un irrazionale quadratico. Ma per ipotesi la frazione continua è infinita e quindi θ è un irrazionale, e quindi in particolare un irrazionale quadratico.

▼ Nel caso dell'esempio $\theta = [4;\ 5, \theta]$ la corrispondente equazione di secondo grado è

$$5\theta^2 + (1 - 21)\theta - 4 = 0$$

che ha soluzione positiva $\theta = \frac{2}{5}(5 + \sqrt{30})$. ▲

Ora si ha

$$\alpha = [b_0;\ b_1, \dots, b_s,\ \theta] = \frac{\theta A' + A''}{\theta B' + B''} \tag{2.29}$$

ovviamente con altri valori interi A', A'', B', B'' rispetto ai precedenti. Ragionando come sopra α è razionale o un irrazionale quadratico.[12] Ma per ipotesi la frazione continua è infinita, quindi α è irrazionale, e quindi un irrazionale quadratico. La prima parte del teorema è provata.

▼ Nel caso dell'esempio: $\alpha = [2;\, 3, \theta]$; le convergenti formali sono:

$$\frac{A_0}{B_0} = \frac{2}{1}, \quad \frac{A_1}{B_1} = 2 + \frac{1}{3} = \frac{7}{3}$$

per cui si ottiene

$$\alpha = \frac{A_2}{B_2} = \frac{\theta \cdot 7 + 2}{\theta \cdot 3 + 1} = \frac{\frac{2}{5}(5 + \sqrt{30}) \cdot 7 + 2}{\frac{2}{5}(5 + \sqrt{30}) \cdot 3 + 1} = \frac{1}{29}\left(56 + 2\sqrt{30}\right)$$

▲

Proviamo ora il viceversa. Sia α un irrazionale quadratico e quindi del tipo $\alpha = (a + \sqrt{b})/c$ con a, b, c interi, $c \neq 0$, $b > 0$ non quadrato. Abbiamo ora:

$$\alpha = \begin{cases} \dfrac{ac + \sqrt{bc^2}}{c^2} & \text{se } c > 0 \\ \dfrac{-ac + \sqrt{bc^2}}{-c^2} & \text{se } c < 0 \end{cases}$$

Non è quindi restrittivo supporre α della forma:

$$\alpha = \frac{P_0 + \sqrt{D}}{Q_0}$$

con P_0, D, Q_0 interi, $Q_0 \neq 0$, $D > 0$ non quadrato, e, inoltre, $Q_0 \,|\, (D - P_0^2)$, ovvero Q_0 è un divisore di $D - P_0^2$. Poniamo anche $\xi_0 = \alpha$. A partire dai valori iniziali (P_0, Q_0, ξ_0) definiamo induttivamente $(P_{i+1}, Q_{i+1}, \xi_{i+1})$ ponendo:

$$\begin{cases} P_{i+1} &= [\xi_i]\, Q_i - P_i \\ Q_{i+1} &= (D - P_{i+1}^2)/Q_i \\ \xi_{i+1} &= (P_{i+1} + \sqrt{D})/Q_{i+1} \end{cases} \tag{2.30}$$

Procediamo ora per passi. Dimostriamo per induzione che:

• *Per ogni $i \geq 0$, P_i e Q_i sono interi tali che $Q_i \,|\, (D - P_i^2)$*

[12] Più algebricamente, sapendo che θ è un irrazionale del tipo $(a + \sqrt{b})/c$ con a, b, c interi, $c \neq 0$, $b > 0$ non quadrato, si ha che $\theta \in \mathbb{Q}(\sqrt{b})$ e quindi anche $\alpha \in \mathbb{Q}(\sqrt{b})$; qui $\mathbb{Q}(\sqrt{b})$ è l'estensione algebrica di $\mathbb{Q}$ con $\sqrt{b}$.

L'affermazione è vera per $i = 0$. Supponiamola vera per i. Evidentemente, per la prima delle (2.30), P_{i+1} è intero. Inoltre, sviluppando la seconda delle (2.30), si ha

$$Q_{i+1} = (D - P_{i+1}^2)/Q_i = (D - P_i^2 + 2[\xi_i]\, Q_i P_i - [\xi_i]^2\, Q_i^2)/Q_i$$

ed avendo assunto che $Q_i \,|\, (D - P_i^2)$ si ha che Q_{i+1} è intero. Infine, si ha $Q_i = (D - P_{i+1}^2)/Q_{i+1}$, ovvero $Q_{i+1} \,|\, (D - P_{i+1}^2)$ (il quoziente è Q_i che è intero).

• *Con passaggi algebrici elementari, dalla terza delle* (2.30) *si ha:*

$$\xi_i = [\xi_i] + \frac{1}{\xi_{i+1}}$$

ovvero

$$\begin{cases} \xi_0 := \alpha \\ \xi_i := \dfrac{1}{\xi_{i-1} - [\xi_{i-1}]} \end{cases}$$

Quindi, se definiamo la successione di interi $a_i := [\xi_i]$, concludiamo che

$$\alpha = \xi_0 = [a_0;\, a_1, a_2, \ldots] = [a_0;\, a_1, a_2, \ldots, a_{n-1}, \xi_n] \tag{2.31}$$

Resta da mostrare che la frazione continua $[a_0;\, a_1, a_2, \ldots]$ è periodica. La strategia di Lagrange è astuta e si basa su una limitazione di crescita delle successioni P_n e Q_n. Si dimostra che:

• *Esiste un indice N tale che per $n \geq N$ riesce $0 < Q_n \leq D$ e $|P_{n+1}| < \sqrt{D}$*

Infatti, se ciò accade, le successioni P_n e Q_n possono assumere solo un numero finito di valori. Esistono quindi indici $i \neq j$ tali che $P_i = P_j$ e $Q_i = Q_j$, quindi $\xi_i = \xi_j$ e la frazione continua $[a_0;\, a_1, a_2, \ldots]$ è periodica.[13] Proviamo quindi l'esistenza dell'indice N detto. Dalla (2.31) deduciamo la (2.21):

$$\alpha = \frac{\xi_n A_{n-1} + A_{n-2}}{\xi_n B_{n-1} + B_{n-2}}$$

e da questa la

$$\alpha^* = \frac{\xi_n^* A_{n-1} + A_{n-2}}{\xi_n^* B_{n-1} + B_{n-2}} \tag{2.32}$$

dove * è il *coniugio*, ossia:

$$\alpha^* = \frac{P_0 - \sqrt{D}}{Q_0}, \quad \xi_n^* = \frac{P_n - \sqrt{D}}{Q_n}$$

[13] Si veda per maggior chiarezza il successivo esempio numerico.

Risolvendo la (2.32) rispetto a ξ_n^* si ottiene:

$$\xi_n^* = -\frac{B_{n-2}}{B_{n-1}}\left(\frac{\alpha^* - A_{n-2}/B_{n-2}}{\alpha^* - A_{n-1}/B_{n-1}}\right)$$

Il termine in parentesi tonde nella precedente uguaglianza ha limite 1 per $n \to \infty$, dato che $A_n/B_n \to \alpha$. Per la permanenza del segno, esiste N tale che per $n \geq N$ il termine in parentesi tonde è positivo, e per gli stessi indici, $\xi_n^* < 0$ e quindi (essendo $\xi_n > 0$ per $n > 0$) abbiamo $0 < \xi_n - \xi_n^* = 2\sqrt{D}/Q_n$ ed infine $0 < Q_n$. Dalla seconda delle (2.30) abbiamo $Q_nQ_{n+1} + P_{n+1}^2 = D$, e quindi per $n \geq N$ si ha $0 < Q_n \leq D$ e $|P_{n+1}| < \sqrt{D}$.

Il teorema è completamente dimostrato. ■

Esempio numerico 2.7.2 Consideriamo il caso di $\alpha = \frac{1}{29}\left(56 + 2\sqrt{30}\right)$

La forma $\alpha = (P_0 + \sqrt{D})/Q_0$ è $\alpha = (1624 + \sqrt{100920})/841$. Calcoliamo i valori delle successioni P_n, Q_n definite per ricorrenza, e le a_n da $n = 0$ fino a $n = 12$:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
P_n	1624	58	290	290	290	290	290	290	290	290	290	290	290
Q_n	841	116	145	116	145	116	145	116	145	116	145	116	145
a_n	2	3	4	5	4	5	4	5	4	5	4	5	4

Come si vede, se $0 \leq n \leq 12$, si ha $P_n \in \{1624, 58, 290\}$, $Q_n \in \{841, 116, 145\}$. Quindi le coppie (P_n, Q_n) possono assumere al massimo *nove* valori distinti. Se prendiamo come nella tabella *tredici* indici n (da 0 a 12), per lo *Schubfach-prinzip* di Dirichlet, o *Principio dei cassetti*,[14] per almeno due indici distinti $i \neq j$ (da 0 a 12) si avrà $(P_i, Q_i) = (P_j, Q_j)$, ossia $P_i = P_j$ e $Q_i = Q_j$. Nella tabella si vede che si possono prendere $i = 2$ e $j = 4$, con $P_2 = P_4 = 290$ e $Q_2 = Q_4 = 145$. Abbiamo quindi $\xi_2 = \xi_4 = (290 + \sqrt{100920})/145$. Questo implica che

$$\alpha = \xi_0 = [a_0;\, a_1, a_2, a_3, a_4, a_5, \ldots] = [a_0;\, a_1, \xi_2] = [a_0;\, a_1, a_2, a_3, \xi_4]$$

[14] Se A, B sono insiemi finiti, ed il numero di elementi di A è *maggiore* del numero degli elementi di B, allora nessuna applicazione $A \to B$ può essere iniettiva. La denominazione "principio dei cassetti" viene dal fatto che se si ripongono N oggetti in M cassetti, ed è $N > M$, almeno uno dei cassetti contiene (almeno) due oggetti. Nel caso in esame i "cassetti" sono $M = 9$ coppie distinte di numeri interi e gli "oggetti" sono gli $N = 13$ indici distinti (gli interi da 0 a 12) che si associano alle coppie. Lo *Schubfachprinzip* implica che esiste una coppia che ha avuti associati (almeno) due indici diversi.

ossia, posto $\beta := \xi_2 = \xi_4$ si ha

$$\beta = \xi_2 = [a_2;\, a_3, \xi_4] = [a_2;\, a_3, \beta] = [a_2;\, a_3, a_2, a_3, \beta] = \dots$$

■

Una frazione continua semplice *periodica* del tipo (2.27) si rappresenta sinteticamente come

$$\alpha = [b_0;\, b_1, \dots, b_s,\ \{a_0;\, a_1, \dots, a_{n-1}\}]$$

Una rappresentazione più classica, mutuata dalla rappresentazione decimale, usa la sopralineatura:

$$\alpha = [b_0;\, b_1, \dots, b_s,\ \overline{a_0, a_1, \dots, a_{n-1}}]$$

La prima, che racchiude il periodo in parentesi graffe, è preferibile se si deve scrivere di matematica con una tastiera.

Esercizio 2.7.3 Verificare che $\sqrt{3} = [1;\, \{1, 2\}]$. Calcolare $[\{1\}]$, $[2;\, \{1, 1, 1, 4\}]$, $[2;\, 3,\, \{4, 5\}\,]$.

SOLUZIONE. $\frac{1}{2}\left(1 + \sqrt{5}\right)$, $\sqrt{7}$, $\frac{1}{29}\left(56 + 2\sqrt{30}\right)$. ■

Osservazione 2.7.4 La periodicità degli sviluppi decimali dei razionali (i numeri algebrici di grado 1), e la periodicità degli sviluppi in frazione continua degli irrazionali quadratici (i numeri algebrici di grado 2) ispirò a Charles Hermite un problema che porta il suo nome: è possibile trovare una regola per associare ad ogni reale α una successione di interi in modo che tale successione sia periodica (o abbia altri tipi di regolarità) se e solo se α è un irrazionale cubico (un numero algebrico di grado 3) o più in generale un numero algebrico di grado $n \geq 3$? Questo *problema di Hermite* venne posto dal matematico francese a Carl Jacobi in una lettera poi pubblicata sul *Journal de Crelle* (Hermite, 1850, p. 286). Scrive Hermite:

> Mais permettez–moi, Monsieur, de revenir un instant sur les circostances remarcables, aux quelles donne lieu la réduction des formes dont les coefficients dépendent de racines d'équation algébriques à coefficients entiers. Peut–être parviendra–t–on à déduire de là, un système complet de caractères pour chaque espèce de ce genre de quantités, analogue par example à ceux que donne la théorie des fractions continues pour les racines des équations du second degré.

Il problema di Hermite è tuttora (marzo 2012) irrisolto.[15]

[15] Alcuni tentativi di soluzione si basano sulla introduzione delle *frazioni continue multidimensionali* (Garrity, 2001).

2.8 La successione delle convergenti

In questa sezione proviamo un teorema che stabilisce alcune importanti proprietà della successione A_k/B_k $(k \geq 0)$ delle convergenti di una frazione continua (eventualmente finita) convergente ad α.

Teorema 2.8.1 *Sia A_k/B_k $(k \geq 0)$ la successione delle convergenti di una frazione continua (eventualmente finita) convergente ad α. Allora:*

(i) *La sottosuccessione delle convergenti di indice pari è a sinistra di α, ed è crescente; la sottosuccessione delle convergenti di indice dispari è a destra di α, ed è decrescente; ossia:*

$$\frac{A_0}{B_0} < \frac{A_2}{B_2} < \frac{A_4}{B_4} < \frac{A_6}{B_6} < \ldots < \alpha < \ldots < \frac{A_7}{B_7} < \frac{A_5}{B_5} < \frac{A_3}{B_3} < \frac{A_1}{B_1} \quad (2.33)$$

(con la ovvia eccezione dell'ultima convergente, uguale ad α, nel caso di una frazione finita, cioè quando α è razionale).

(ii) *La successione degli scarti*

$$|B_k\alpha - A_k| \quad (k \geq 0)$$

e la successione delle distanze euclidee

$$\left|\alpha - \frac{A_k}{B_k}\right| \quad (k \geq 0)$$

sono strettamente decrescenti.

Dimostrazione. Saranno utili due uguaglianze che derivano direttamente dalle formule di Eulero:

$$A_kB_{k-1} - A_{k-1}B_k = (-1)^{k-1} \quad (k \geq 1) \quad (2.34)$$

$$A_kB_{k-2} - A_{k-2}B_k = (-1)^k\, a_k \quad (k \geq 2) \quad (2.35)$$

La (2.34) è esattamente la (2.11) con l'indice diminuito di 1. Per provare la (2.35) riscriviamo le formule di Eulero di una frazione continua semplice:

$$\begin{cases} A_k = a_k\, A_{k-1} + A_{k-2} \\ B_k = a_k\, B_{k-1} + B_{k-2} \end{cases} \quad (2.36)$$

nella forma equivalente:

$$\begin{cases} A_{k-2} = A_k - a_k\, A_{k-1} \\ B_{k-2} = B_k - a_k\, B_{k-1} \end{cases} \tag{2.37}$$

che porta al prodotto di matrici:

$$\begin{bmatrix} A_k & A_{k-1} \\ B_k & B_{k-1} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ -a_k & 0 \end{bmatrix} = \begin{bmatrix} A_{k-2} & A_k \\ B_{k-2} & B_k \end{bmatrix}$$

Calcolando i determinanti si ha (utilizzando la (2.34) per la prima matrice) che

$$(-1)^{k-1}\, a_k \;=\; (A_{k-2}B_k - A_k B_{k-2})$$

ossia, moltiplicando per -1, la (2.35).

Passiamo alla dimostrazione del teorema. La (i) segue direttamente dall'esame del Teorema 2.2.7 (con la solita ovvia eccezione nel caso finito). Se esaminiamo ora le posizioni reciproche di α e di tre convergenti successive come indicate nella (2.33), otteniamo per k pari:

$$\frac{A_k}{B_k} \;<\; \frac{A_{k+2}}{B_{k+2}} \;<\; \alpha \;<\; \frac{A_{k+1}}{B_{k+1}}$$

e per k dispari:

$$\frac{A_{k+1}}{B_{k+1}} \;<\; \alpha \;<\; \frac{A_{k+2}}{B_{k+2}} \;<\; \frac{A_k}{B_k}$$

In ogni caso abbiamo che:

$$\left|\frac{A_{k+2}}{B_{k+2}} - \frac{A_k}{B_k}\right| \;<\; \left|\alpha - \frac{A_k}{B_k}\right| \;<\; \left|\frac{A_{k+1}}{B_{k+1}} - \frac{A_k}{B_k}\right|$$

da cui:

$$\left|\frac{A_{k+2}B_k - A_k B_{k+2}}{B_{k+2}B_k}\right| \;<\; \left|\alpha - \frac{A_k}{B_k}\right| \;<\; \left|\frac{A_{k+1}B_k - A_k B_{k+1}}{B_{k+1}B_k}\right|$$

e per le (2.34–2.35):

$$\left|\frac{a_{k+2}}{B_{k+2}B_k}\right| \;<\; \left|\alpha - \frac{A_k}{B_k}\right| \;<\; \left|\frac{1}{B_{k+1}B_k}\right| \tag{2.38}$$

Infine, eliminando B_k e tenendo conto che $a_{k+2} \geq 1$:

$$\frac{1}{B_{k+2}} \;<\; |B_k\alpha - A_k| \;<\; \frac{1}{B_{k+1}} \quad (k \geq 0) \tag{2.39}$$

Questo prova che per $k \geq 0$ lo scarto $|B_k\alpha - A_k|$ è "intrappolato" fra due successivi valori di una successione strettamente decrescente (dato che $B_1 < B_2 < B_3 < \ldots$) e quindi la successione degli scarti è anch'essa strettamente decrescente. Per quanto riguarda la sucessione delle distanze euclideee, dal fatto già provato che per $k \geq 0$ si ha $|B_k\alpha - A_k| > |B_{k+1}\alpha - A_{k+1}|$, moltiplicando membro a membro questa disuguaglianza per la disuguaglianza $1/B_k > 1/B_{k+1}$ quando $k \geq 1$ oppure per la $1/B_0 \leq 1/B_1$ quando $k = 0$, si ottiene che

$$\left|\alpha - \frac{A_k}{B_k}\right| > \left|\alpha - \frac{A_{k+1}}{B_{k+1}}\right|$$

per ogni indice $k \geq 0$. ■

Esercizio 2.8.2 Si considerino due successioni $s_k = \sqrt{2} - \frac{1}{(2k)^2}$ e $d_k = \sqrt{2} + \frac{1}{2k+1}$, definite per $k \geq 1$. Si verifichi che la s_k è strettamente crescente e converge a $\sqrt{2}$, e che la d_k è strettamente decrescente e converge a $\sqrt{2}$. Si verifichi che definendo una terza successione $(c_k)_{k\geq 1} = (d_1, s_1, d_2, s_2, \ldots, d_j, s_j, \ldots)$ si ha

$$c_2 < c_4 < c_6 < \ldots < c_{2j} < \ldots < \sqrt{2} < \ldots < c_{2j+1} < \ldots < c_5 < c_3 < c_1$$

ma la successione $|\alpha - c_k|$ non è decrescente.

2.9 Le frazioni intermedie ed il loro uso

Introduciamo ora il concetto di *frazione intermedia.*

Definizione 2.9.1 *La* ***somma di Farey*** *o* ***mediante*** *di due frazioni a/b e c/d irriducibili (a, b, c, d interi; $b > 0, d > 0$) è la frazione*

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{a+c}{b+d}$$

Lemma 2.9.2 *La mediante di due frazioni diverse a/b e c/d irriducibili (a, b, c, d interi; $b > 0, d > 0$) è compresa strettamente fra esse.*

Dimostrazione. Supponiamo ad esempio che sia $a/b < c/d$. Allora $bc - ad > 0$ e quindi

$$\frac{a+c}{b+d} - \frac{a}{b} = \frac{bc-ad}{b(b+d)} > 0, \quad \frac{a+c}{b+d} - \frac{c}{d} = \frac{ad-bc}{b(b+d)} < 0$$

■

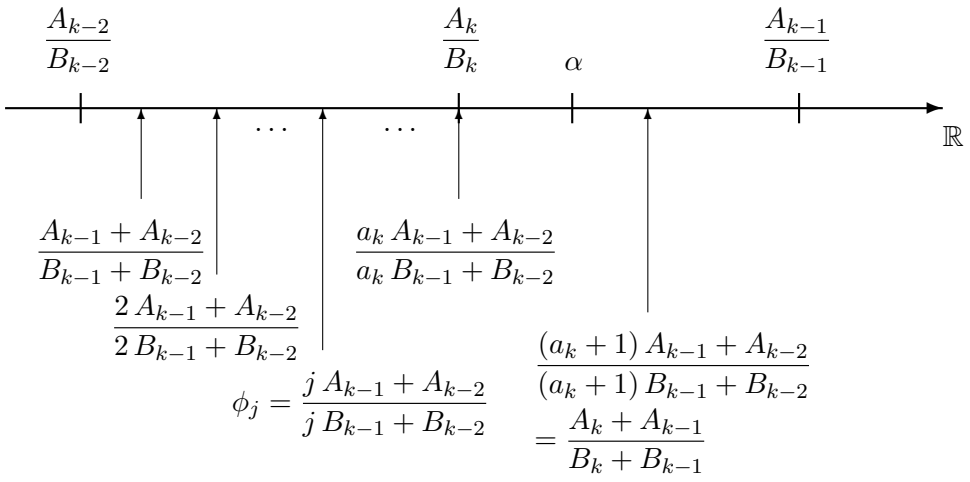


Figura 2.3: Le frazioni intermedie

Consideriamo ora *tre* convergenti successive dello sviluppo in frazione continua di un *irrazionale* $\alpha > 0$, corrispondenti a tre dati indici $k-2, k-1$ e k; per fissare la grafica supponiamo k pari, di modo che risulti:

$$\frac{A_{k-2}}{B_{k-2}} < \frac{A_k}{B_k} < \alpha < \frac{A_{k-1}}{B_{k-1}}$$

Nel proseguo supporremo vere queste disuguaglianze. Il lettore potrà facilmente modificare le cose nel caso in cui k sia dispari. Consideriamo la successione di frazioni

$$\phi_j = \frac{j\,A_{k-1}+A_{k-2}}{j\,B_{k-1}+B_{k-2}} \quad (j \geq 0) \tag{2.40}$$

Per $j = 0$ si ha $\phi_0 = A_{k-2}/B_{k-2}$, mentre per $j \to \infty$ si ha $\phi_j \to A_{k-1}/B_{k-1}$. Per $j = 1$, la ϕ_1 è la somma di Farey di A_{k-2}/B_{k-2} e di A_{k-1}/B_{k-1}; in generale, per $j \geq 1$ la ϕ_j è la somma di Farey di ϕ_{j-1} e di A_{k-1}/B_{k-1}; conseguentemente, la successione $(\phi_j)_{j\geq 0}$ è monotona, strettamente crescente, nell'intervallo $[A_{k-2}/B_{k-2},\ A_{k-1}/B_{k-1})$ con estremi le prime due convergenti date. Per $j = a_k$, per le formule di Eulero si ha

$$\phi_{a_k} = \frac{a_k\,A_{k-1}+A_{k-2}}{a_k\,B_{k-1}+B_{k-2}} = \frac{A_k}{B_k}$$

quindi la successione ϕ_j "passa" quando $j = a_k$ per la ulteriore convergente considerata A_k/B_k. Si noti che, dato che la A_k/B_k si trova rispetto ad α dalla

stessa parte di A_{k-2}/B_{k-2}, tutte le frazioni ϕ_j con $j \leq a_k$ (ed in particolare la $\phi_1 = (A_{k-1} + A_{k-2})/(B_{k-1} + B_{k-2})$) stanno rispetto ad α dalla stessa parte di A_{k-2}/B_{k-2}: si ha quindi, ed è un'osservazione importante, che *la mediante di due convergenti successive sta rispetto ad α dalla stessa parte della convergente di indice minore.*

Avendo assunto che α è irrazionale, dato che $\phi_j \to A_{k-1}/B_{k-1} > \alpha$ per $j \to \infty$, esiste il *primo* indice $j = j^* + 1$ tale che $\phi_{j^*+1} > \alpha$. Proviamo ora che si ha:

$$j^* = a_k$$

e quindi $\phi_{j^*} = A_k/B_k$. Infatti, $\phi_{a_k} = A_k/B_k < \alpha$ perché A_k/B_k deve stare rispetto ad α dalla stessa parte di A_{k-2}/B_{k-2}, nel mentre, aumentando l'indice di 1, si ha

$$\frac{(a_k + 1)\, A_{k-1} + A_{k-2}}{(a_k + 1)\, B_{k-1} + B_{k-2}} = \frac{A_k + A_{k-1}}{B_k + B_{k-1}} > \alpha$$

in quanto $(A_k + A_{k-1})/(B_k + B_{k-1})$, come somma di Farey di A_{k-1}/B_{k-1} e di A_k/B_k, si trova rispetto ad α dalla stessa parte di A_{k-1}/B_{k-1} (per la regola spiegata in precedenza: la mediante di due convergenti successive sta rispetto ad α dalla stessa parte di quella di indice minore).

Abbiamo quindi ottenuto anche una regola pratica:

Teorema 2.9.3 (regola della mediante) *Il valore α di una frazione continua irrazionale si trova sempre fra una qualunque convergente ed la mediante di questa e della convergente precedente.*

Dimostrazione. Siano infatti α irrazionale, Q una qualunque convergente, P la precedente ed M la mediante di Q, P. Se Q ha indice pari si ha $Q < \alpha < M < P$, mentre se Q ha indice dispari si ha $P < M < \alpha < Q$. ■

Definizione 2.9.4 *Per $k \geq 1$, se $a_k > 1$, le frazioni*

$$\phi_j = \frac{j\, A_{k-1} + A_{k-2}}{j\, B_{k-1} + B_{k-2}} \tag{2.41}$$

per $0 < j < a_k$ sono dette **frazioni intermedie**[16] *fra A_{k-2}/B_{k-2} ed A_{k-1}/B_{k-1}.*

Esempio numerico 2.9.5 Si è visto nell'Esempio 2.4.3 che si ha:

[16] Oppure, in taluni testi, frazioni *semiconvergenti*, per distinguerle dalle convergenti.

$$\pi = [a_0;\, a_1, a_2, a_3, a_4, \ldots] = [3;\, 7, 15, 1, 292, \ldots]$$

Le prime convergenti sono allora facilmente calcolabili:

$$\frac{A_0}{B_0} = 3, \quad \frac{A_1}{B_1} = \frac{22}{7}, \quad \frac{A_2}{B_2} = \frac{333}{106}, \quad \frac{A_3}{B_3} = \frac{355}{113}, \quad \frac{A_4}{B_4} = \frac{103993}{33102}, \ \ldots$$

Ricordiamo che, storicamente, l'approssimazione $A_1/B_1 = 22/7 = 3.14286\ldots$ è nota come *approssimazione di Archimede*, mentre $A_3/B_3 = 355/113 = 3.1415929\ldots$ è l'*approssimazione di Zu Chongzhi* (Martzloff, 2006, p. 281).[17] Fissiamo $k = 4$ e calcoliamo le frazioni

$$\phi_j = \frac{jA_3 + A_2}{jB_3 + B_2} = \frac{j \cdot 355 + 333}{j \cdot 113 + 106}$$

per $j = 0, 1, 2, \ldots$. Otteniamo la successione:

$$\frac{333}{106}, \frac{688}{219}, \frac{1043}{332}, \frac{103283}{32876}, \frac{103638}{32989}, \frac{103993}{33102}, \frac{104348}{33215}, \frac{104703}{33328}, \frac{105058}{33441}, \ldots$$

che inizia in $\phi_0 = A_2/B_2$ e tende, crescendo strettamente, a $\lim_{j\to\infty} \phi_j = A_3/B_3$.

Usando lo sviluppo decimale 3.14159265359 di π con precisione di 12 cifre decimali, si verifica numericamente che per $j = 0, \ldots, 292$ si ha $\phi_j < \pi$, mentre per $j \geq 293$ si ha $\phi_j > \pi$. In particolare, con l'approssimazione fissata:

$$\pi - \phi_{292} = \pi - \frac{103993}{33102} = 5.8 \times 10^{-10}, \quad \pi - \phi_{293} = \pi - \frac{104348}{33215} = -3.3 \times 10^{-10}$$

■

Abbiamo ancora due importanti corollari. Il primo individua una limitazione inferiore all'errore che si commette approssimando α con la convergente A_k/B_k.

Corollario 2.9.6 *Per ogni $k \geq 0$,*

$$\left|\alpha - \frac{A_k}{B_k}\right| \ > \ \frac{1}{B_k(B_{k+1} + B_k)} \tag{2.42}$$

[17] È curioso che le differenze fra queste due approssimazioni e π possono essere espresse come integrali definiti fra 0 ed 1 di semplici funzioni razionali fratte:

$$22/7 - \pi = \int_0^1 \frac{x^4(1-x)^4}{1+x^2}\, dx, \quad 355/113 - \pi = \frac{1}{3164} \int_0^1 \frac{x^8(1-x)^8\left(25 + 816x^2\right)}{(1+x^2)}\, dx$$

Gli integrali si calcolano come i consueti esercizi di integrazione delle funzioni razionali fratte basati sulla cosiddetta "formula di Hermite" discussa negli insegnamenti di analisi matematica di base.

DIMOSTRAZIONE. Fissiamo ad esempio k pari, ed applichiamo la *regola della mediante* 2.9.3 pensando A_{k+1}/B_{k+1} come "qualunque convergente":

$$\frac{A_k}{B_k} < \frac{A_k + A_{k+1}}{B_k + B_{k+1}} < \alpha < \frac{A_{k+1}}{B_{k+1}}$$

Quindi:

$$\left|\alpha - \frac{A_k}{B_k}\right| > \left|\frac{A_k + A_{k+1}}{B_k + B_{k+1}} - \frac{A_k}{B_k}\right| \geq \frac{1}{B_k(B_{k+1} + B_k)}$$

Se k è dispari si procede analogamente, "rovesciando" le disuguaglianze. ■

2.9.1 Algoritmo per il calcolo delle convergenti

In Fiori e Invernizzi (2009) abbiamo mostrato come lo sviluppo *decimale* di un numero reale irrazionale α si possa ottenere in modo algoritmico se si disponga di un *test* che, per ogni numero razionale r (dato come frazione) possa stabilire se $r < \alpha$ oppure $r > \alpha$.[18] Analogamente, se per un irrazionale α disponiamo di un tale *test*, possiamo ottenere in modo algoritmico la successione delle convergenti dello sviluppo in frazione continua di α. Infatti, supponiamo siano note *due* convergenti consecutive A_{k-2}/B_{k-2} e $A_{k-1}B_{k-1}$, e supponiamo per esempio che sia k pari e quindi

$$\frac{A_{k-2}}{B_{k-2}} < \alpha < \frac{A_{k-1}}{B_{k-1}}$$

Possiamo allora calcolare A_k/B_k *senza conoscere* a_k. Basta calcolare successivamente le frazioni

$$\phi_j = \frac{j\,A_{k-1} + A_{k-2}}{j\,B_{k-1} + B_{k-2}}$$

per $j = 0, 1, 2, \ldots$ e, usando il *test*, fermarsi al minimo valore di $j = j^*$ per cui $\phi_{j^*} > \alpha$. Allora necessariamente si ha $a_k = j^* - 1$ e $A_k/B_k = \phi_{j^*-1}$.

Esercizio 2.9.7 Dato $\alpha = \sqrt{7}$, e dato che

$$\frac{A_0}{B_0} = 2,\ \ \frac{A_1}{B_1} = 2 + \frac{1}{1} = 3,\ \ \frac{A_2}{B_2} = 2 + \frac{1}{1 + \frac{1}{1}} = \frac{5}{2},\ \ \frac{A_3}{B_3} = 2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}} = \frac{8}{3}$$

[18] Sostanzialmente, assegnato $\alpha = (A', A'')$ come sezione di Dedekind del campo razionale $\mathbb{Q}$, il *test* deve poter stabilire se $r \in A'$ oppure $r \in A''$. Questo è particolarmente semplice per i numeri algebrici, per i quali il *test* può basarsi sul segno del polinomio minimo calcolato in r (in un intorno opportuno di α). Per comprendere meglio questa nota, si pensi al numero di Nepero come sezione di Dedekind $e = (A', A'')$ del campo razionale, e si cerchi di immaginare come realizzare un *test* che stabilisca, ad esempio, a quale delle due classi A' o A'' appartiene il numero razionale $r = 46150226651233/16977719590391$ (non può essere $e = r$, in quanto, come dimostreremo in seguito, e è irrazionale).

si calcolino a_4 e A_4/B_4, a_5 e A_5/B_5 con il metodo dato.

SOLUZIONE. Iniziamo con $k = 4$. Abbiamo $A_2/B_2 = 5/2 < \sqrt{7} < 8/3 = A_3/B_3$. Dobbiamo tabulare per $j \geq 1$ le frazioni

$$\phi_j = \frac{j\,A_3 + A_2}{j\,B_3 + B_2} = \frac{j\,8 + 5}{j\,3 + 2}$$

Per $j = 0$ si ha il valore $5/2$ *minore* di $\sqrt{7}$, e per $j \to \infty$ si ha il limite $8/3$ *maggiore* di $\sqrt{7}$. Possiamo quindi calcolare il primo valore di j per il quale ϕ_j è *maggiore* di $\sqrt{7}$. Il *test* $\phi_j > \sqrt{7}$ equivale a

$$(j\,8 + 5)^2 - 7(j\,3 + 2)^2 > 0$$

Tabulando $(j\,8 + 5)^2 - 7(j\,3 + 2)^2$ per $j = 1, 2, 3, 4, 5$ si ottengono gli interi -6, -7, -6, -3, 2, per cui $j^* = 5$ e

$$a_k = j^* - 1 = 4, \quad \frac{A_4}{B_4} = \phi_4 = \frac{4 \cdot 8 + 5}{4 \cdot 3 + 2} = \frac{37}{14}$$

Per $k = 5$, che è dispari, dobbiamo tabulare per $j \geq 1$ le frazioni $(j\,37 + 8)/(j\,14 + 3)$, e verificare quando sono *minori* di $\alpha = \sqrt{7}$. Tabulando $(j\,37 + 8)^2 - 7(j\,14 + 3)^2$ per $j = 1, 2, 3$ si ottengono gli interi $2, -3, -14$, il cambio di segno si ha a $j^* = 2$ e quindi $a_5 = 1$ e $A_4/B_4 = \phi_1 = (37 + 8)/(14 + 3) = 45/17$. ■

Si noti come l'algoritmo consenta di calcolare un arbitrario convergente per $\sqrt{c}$ con c intero non quadrato, usando solo aritmetica intera.

Esercizio 2.9.8 (Approssimazione di $\sqrt{3}$ in Archimede) La celebre approssimazione di π fornita da Archimede nella breve nota *Sulla misura del circolo*

$$\frac{22}{7} = 3 + \frac{1}{7} > \pi > 3 + \frac{10}{71}$$

venne ottenuta dal matematico siracusano utilizzando la relazione ovvia $\tan(\pi/6) = 1/\sqrt{3}$ e la stima

$$\frac{1351}{780} > \sqrt{3} > \frac{265}{153}$$

che enunciò senza alcuna parola di spiegazione[19] (Heath, 1897). Vari autori hanno osservato (Audisio, 1930) che si tratta rispettivamente delle convergenti A_8/B_8 ed A_{11}/B_{11} dello sviluppo in frazione continua di $\sqrt{3}$. Per esercizio, si calcolino queste convergenti di $\sqrt{3}$ usando l'algoritmo precedentemente illustrato nel Corollario 2.9.1 basato solo sull'aritmetica intera, partendo dai due dati iniziali:

```
b ← intero positivo non quadrato
n ← numero di convergenti da calcolare
(definisci valori iniziali:)
A_{-1} ← 1; B_{-1} ← 0; A_0 ← [√b]; B_0 ← 1
PRINT A_0/B_0
FOR k FROM 1 TO (n − 1)
        j ← 1
        WHILE (−1)^k[(jA_{k−1}+A_{k−2})^2 − b(jB_{k−1}+B_{k−2})^2] < 0
          THEN
                A_k ← jA_{k−1} + A_{k−2}
                B_k ← jB_{k−1} + B_{k−2}
          INCREMENT j
        END WHILE
PRINT A_k/B_k
NEXT k
END
```

Figura 2.4: Pseudo–codice dell'algoritmo del Corollario 2.9.1 per il calcolo in aritmetica intera delle prime n convergenti di $\sqrt{b}$ ($b > 0$ intero non quadrato). Semplicissime modifiche consentono di calcolare le convergenti di irrazionali del tipo $\sqrt[m]{b}$, con $m \geq 3$: basta sostituire la parte intera $[\sqrt{b}]$ con $[\sqrt[m]{b}]$ nelle condizioni iniziali e l'esponente 2 con m nel test del comando WHILE. Analogamente, modificando la condizione iniziale ed il test in modo opportuno si possono calcolare facilmente le convergenti di un numero algebrico il cui polinomio minimo sia sufficientemente "trattabile", in sostanza di grado "basso".

$$\frac{A_{-1}}{B_{-1}} = \frac{1}{0}, \qquad \frac{A_0}{B_0} = \frac{[\sqrt{3}]}{1} = \frac{1}{1}$$

La Figura 2.4 mostra lo pseudo–codice dell'algoritmo del Corollario 2.9.1: realizzando il codice con *Mathematica*[20] e impostando i valori $n = 12$, $c = 3$ si ottengono le convergenti:

$$1, 2, \frac{5}{3}, \frac{7}{4}, \frac{19}{11}, \frac{26}{15}, \frac{71}{41}, \frac{97}{56}, \frac{265}{153}, \frac{362}{209}, \frac{989}{571}, \frac{1351}{780}$$

Esercizio 2.9.9 Si consideri la sezione aurea,[21] ossia $\phi = (\sqrt{5}+1)/2$. Si dimostri che p/q è un razionale positivo (p, q interi), e si ha $p/a < \phi$ se e solo se $p^2 - pq - q^2 < 0$. Si modifichi di conseguenza l'algoritmo descritto nella Figura 2.4 e lo si implementi in modo da ottenere le prime 16 convergenti A_k/B_k ($k = 1, 16$) della frazione continua di ϕ. Si osservi che le successioni A_k e B_k sono successioni di Fibonacci (ogni termine è somma dei due precedenti).

SOLUZIONE. Non serve assegnare b, si ponga $n \leftarrow 16$ come richiesto. Basta poi modificare il *test* del comando WHILE al modo seguente:

$$(-1)^k \left[\underbrace{(jA_{k-1} + A_{k-2})^2}_{p^2} - \underbrace{(jA_{k-1} + A_{k-2})(jB_{k-1} + B_{k-2})}_{pq} - \underbrace{(jB_{k-1} + B_{k-2})^2}_{q^2} \right] < 0$$

Implementando l'algoritmo così modificato ed aggiungendo all'inizio, manualmente, la convergente formale di indice $k = -1$, si ottengono le convergenti

$$\frac{1}{0}, \frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \frac{89}{55}, \frac{144}{89}, \frac{233}{144}, \frac{377}{233}, \frac{610}{377}, \frac{987}{610}, \frac{1597}{987}$$

[19] Torneremo in seguito su questo punto.

[20] Gli utenti di *Mathematica* possono usare il codice seguente:

```
b = 3;
n = 12;
A[-1]=1; B[-1]=0; A[0]=Floor[Sqrt[b]]; B[0]=1;
Print[A[0]/B[0]]
Do[  j=1;
     While[(-1)^k ((j A[k-1]+A[k-2])^2 - b (j B[k-1]+B[k-2])^2)<0,
        A[k]=j A[k-1]+A[k-2];
        B[k]=j B[k-1]+B[k-2];
     j++];
   Print[A[k]/B[k]],
{k,1,n-1}]
```

[21] Un rettangolo di lati disuguali, con lato maggiore a e lato minore b, è detto *rettangolo aureo* se b è medio proporzionale fra a ed $a - b$, ossia $a/b = b/(a - b)$. La proporzione si riscrive come $b/a = a/b - 1$. Posto per definizione $\phi = a/b$, si ha $1/\phi = \phi - 1$, ossia $\phi^2 - \phi - 1 = 0$. Quest'equazione (per la regola di Cartesio) ha una sola soluzione positiva $\phi = (\sqrt{5}+1)/2$, che è la sezione aurea. Approssimativamente, $\phi = 1.61803\ldots$

■

Esercizio 2.9.10 Dato $\alpha = \pi$, e date le convergenti

$$\frac{A_2}{B_2} = \frac{333}{106}, \quad \frac{A_3}{B_3} = \frac{355}{113}$$

si calcolino manualmente a_4 e A_4/B_4 con il metodo dato.

SOLUZIONE. Si utilizzi la successione ϕ_j definita nell'Esempio numerico 2.9.5 e le informazioni date sul suo "cambio di segno". ■

Concludiamo col risultato principale della sezione.

Teorema 2.9.11 *Sia α irrazionale, allora per ogni $n \geq 0$ si ha*

$$\frac{1}{B_n(B_n + B_{n+1})} < \left|\alpha - \frac{A_n}{B_n}\right| \leq \frac{1}{B_n B_{n+1}} \tag{2.43}$$

DIMOSTRAZIONE. La prima disuguaglianza è la (2.42) già dimostrata. La seconda deriva dal fatto che, vista la (2.16), una somma parziale di una serie convergente a segni alterni differisce dalla somma della serie per non più del primo termine trascurato. ■

Esercizio 2.9.12 Per il valore approssimato di π di Zu Chongzhi $A_3/B_3 = 355/113$ la (2.43) diventa

$$2.66 \times 10^{-7} \approx \frac{1}{113\,(113 + 33102)} < \left|\pi - \frac{355}{113}\right| \leq \frac{1}{113 \cdot 33102} \approx 2.67 \times 10^{-7}$$

■

2.10 Sviluppi notevoli

In questa sezione consideriamo alcuni numeri reali "notevoli" (la sezione aurea ϕ, il suo inverso $1/\phi$, $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{2}$, e, e^2, π, la costante γ di Eulero–Mascheroni, e la costante L di Liouville) e presentiamo il loro sviluppo in frazione continua, assieme ad alcune considerazioni "sperimentali" sulla "struttura" di tali sviluppi. A seconda della strumentazione a disposizione, il lettore può ripetere queste considerazioni con un software di computer algebra come *Mathematica*,[22] oppure, più elementarmente, procurandosi un adeguato sviluppo decimale del

[22] *Mathematica* ha il comando `ContinuedFraction` che calcola gli sviluppi in frazione continua.

numero di interesse (Sloane, 2010)[23] e poi utilizzando uno dei numerosi *script* disponibili liberamente online per eseguire, con tutti i passaggi, l'algoritmo euclideo del MCD (o fare le divisioni a mano).

La sezione aurea: $\phi = (\sqrt{5}+1)/2 = 1.61803\ldots$ È un irrazionale quadratico, con polinomio minimo $p(x) = x^2 - x - 1$. Ha quindi uno sviluppo in frazione continua periodico:

$$\phi = [1;\{1\}] = [1;1,1,1,1,\ldots] = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}$$

L'inverso della sezione aurea $1/\phi = (\sqrt{5}-1)/2 = 0.618034\ldots$ È un irrazionale quadratico, con polinomio minimo $p(x) = x^2 + x - 1$. Ha quindi uno sviluppo in frazione continua periodico:

$$1/\phi = [0;\{1\}] = [0;1,1,1,1,\ldots] = \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}$$

La radice di 2: $\sqrt{2} = 1.41421\ldots$ È ovviamente quadratico.

$$\sqrt{2} = [1;\{2\}] = [1;2,2,2,2,\ldots] = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ddots}}}}$$

La radice di 3: $\sqrt{3} = 1.73205\ldots$ È ovviamente quadratico.

$$\sqrt{3} = [1;\{1,2\}] = [1;1,2,1,2,\ldots] = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \ddots}}}}$$

[23] Nel database `http://oeis.org` le sequenze delle cifre decimali, tipicamente le prime 128, sono identificate con un codice, ad esempio: ϕ = `A001622`, $\sqrt{2}$ = `A002193`, $\sqrt{3}$ = `A002194`, e = `A001113`, π = `A000796`, γ = `A002852`, L = `A012245`. L'url per `A001113`, ad esempio, è `http://oeis.org/A001113`.

La radice cubica di 2: $\sqrt[3]{2} = 1.25992\ldots$ È un irrazionale cubico. Il suo sviluppo in frazione continua non ha regolarità apparenti.

$$\sqrt[3]{2} = [1;3,1,5,1,1,4,1,1,8,1,14,\ldots] = 1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \ddots}}}}}}$$

Il numero di Nepero $e = 2.71828\ldots$ Il suo sviluppo in frazione continua ha una struttura nota: dopo la parte intera $[2;]$ troviamo terne di interi del tipo $(1, 2n, 1)$, elencate secondo valori crescenti di $n \geq 1$:

$$e = [2;1,2,1,1,4,1,1,6,1,1,8,\ldots] = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \ddots}}}}}}$$

Formalmente, per queste frazioni continue si generalizza la notazione delle frazioni continue periodiche: nel caso di e si scrive:

$$e = [2; \{1, 2n, 1\}]_{n=1}^{\infty}$$

Questo risultato venne ottenuto da Eulero (1744a, pp. 120–121) che usò la sua consueta "induzione logica". Partendo dal valore decimale 2.71828182845905, egli ottenne la frazione continua sopra scritta, dalla quale osservò che

> . . . denominatores terni constituunt progressionem arithmeticam 2, 4, 6, 8 etc. reliqui sunt unitates.

Rendendosi ovviamente conto che si trattava di una conclusione piuttosto ardita, aggiunse fiduciosamente che:

> Quæ lex etsi ex sola observatione est deprehensa, tamen probabile videtur eam in infinitum valere, quod quidem infra certo confirmabitur.

Una dimostrazione moderna e semplice si trova in Olds (1970).

Il numero $e^2 = 7.38906\ldots$ Anche questo sviluppo in frazione continua ha una struttura nota:

$$e^2 = [7; 2, 1, 1, 3, 18, 5, 1, 1, 6, 30, 8, \ldots]$$

Si può infatti dimostrare (Olds, 1970) che

$$e^2 = [7; \{3n-1, 1, 1, 3n, 6(2n+1)\}]_{n=1}^{\infty}$$

Pi greco: $\pi = 3.14159\ldots$ Non è nota una "regola" per lo sviluppo in frazione continua di π.

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1\ldots] = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}}}}}$$

La costante di Eulero–Mascheroni: $\gamma = 0.577216\ldots$ Ricordiamo che $\gamma = \lim_{n\to\infty}\left(\sum_{k=1}^{\infty}\frac{1}{k} - \log n\right)$. Si tratta di un numero del quale, ad oggi (marzo 2012) non si sa neppure se è razionale o irrazionale. Lo sviluppo è:

$$\gamma = [0; 1, 1, 2, 1, 2, 1, 4, 3, 13, 5, 1, 1, 8, 1, 2, \ldots] = \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{2}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{\cdots}}}}}}}$$

La costante di Liouville $L = \sum_{k=1}^{\infty} 10^{-k!}$. La successione delle cifre decimali di $L = 0.d_1d_2d_3\ldots$ dopo la virgola è la funzione caratteristica dell'insieme $\{k! \mid k = 1, 2, \ldots\}$ dei fattoriali, cioè si ha $d_{k!} = 1$ e 0 altrimenti; come vedremo, L è un numero trascendente, anzi è il primo numero trascendente del quale siano esplicitamente conosciute le cifre decimali. Lo sviluppo in frazione

continua è:

$$
\begin{aligned}
L &= [0; 9, 11, 99, 1, 10, 9, 999999999999, 1, 8, 10, 1, 99, \ldots] \\
&= \cfrac{1}{9 + \cfrac{1}{11 + \cfrac{1}{99 + \cfrac{1}{1 + \cfrac{1}{10 + \cfrac{1}{9 + \cfrac{1}{999999999999 + \cfrac{1}{1 + \cfrac{1}{8 + \cfrac{1}{10 + \cfrac{1}{1 + \cfrac{1}{99 + \ddots}}}}}}}}}}}}
\end{aligned}
$$

2.10.1 Sperimentazioni con la DFT

Lo sviluppo in frazione continua $[a_0; a_1, a_2, \ldots]$ di un irrazionale α può essere considerato come un campionamento di un "segnale". Ad esempio, in linea di principio, fissato il *sampling rate*, potrebbe essere "suonato" con un player musicale come Windows Media Player (generando un suono a un canale di durata teorica illimitata univocamente associato al α). Possiamo anche troncare lo sviluppo $[a_0; a_1, a_2, \ldots]$ al termine a_N, ottenendo una $(N+1)$–pla di numeri interi in cui si possono ad esempio rintracciare le principali componenti periodiche (se ce ne sono) con uno strumento classico come la Trasformata Discreta di Fourier (DFT). Come si è visto, i numeri irrazionali quadratici (e solo questi) conducono a sviluppi in frazione continua definitivamente periodici. Altri numeri algebrici, come $\sqrt[3]{2}$, hanno sviluppi in frazione continua apparentemente casuali; e lo stesso accade per π, che, come si vedrà, è trascendente. Invece, altri numeri trascendenti come e ed e^2 hanno sviluppi in frazione continua che presentano dei *patterns* ben definiti. La Figura 2.5, creata con *Mathematica*, illustra queste analogie e differenze: per ciascuno dei quattro numeri citati è stato calcolato lo sviluppo in frazione continua fino al termine $150-$esimo e ne è stato rappresentato lo spettro usando la DFT. Sono evidenti delle "frequenze dominanti" per e e per e^2, mentre il "segnale" generato da $\sqrt[3]{2}$ o da π è apparentemente "caotico".

In questo testo non approfondiamo questo tema, e ci limitiamo a queste osservazioni sperimentali.

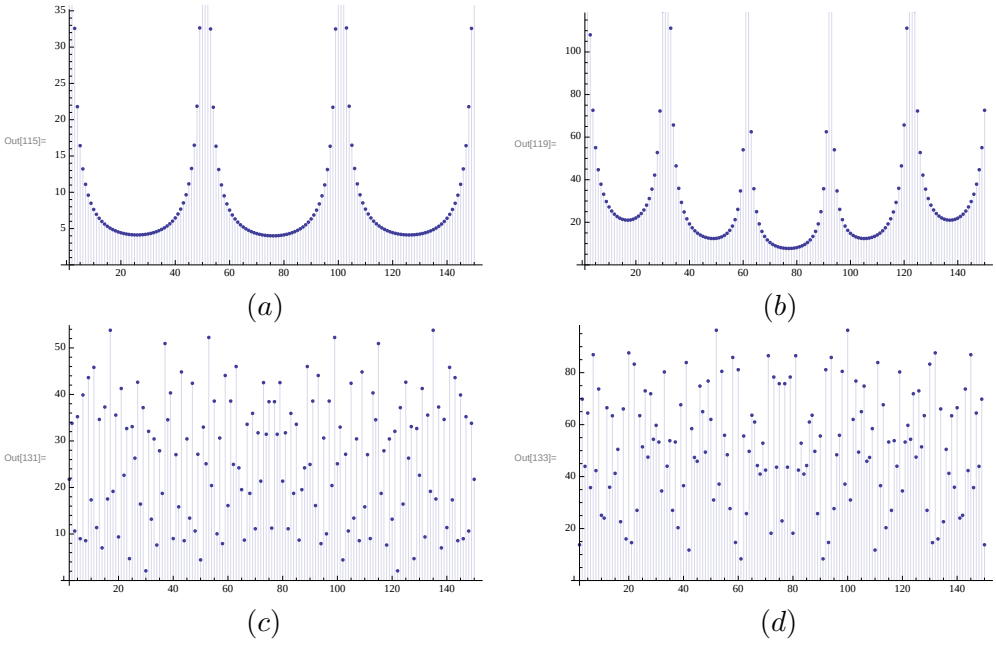


Figura 2.5: Spettri delle trasformate discrete di Fourier degli sviluppi in frazione continua dei numeri reali: (a) e, (b) e^2, (c) π, (d) $\sqrt[3]{2}$, troncate ai primi 150 termini; negli spettri è omesso il primo termine, corrispondente al valor medio della sequenza.

2.11 Approssimazione diofantea

Il termine "approssimazione diofantea"[24] è sinonimo di "approssimazione razionale", ossia approssimazione di numeri reali con numeri razionali. È chiaro che la densità di $\mathbb{Q}$ in $\mathbb{R}$ implica che ogni reale può essere approssimato "a piacere" con numeri razionali: per questo va precisato subito che il problema dell'approssimazione diofantea consiste nell'approssimare un numero reale α con razionali $r = a/b$ (a, b interi, $b > 0$) rappresentabili con denominatore *"piccolo"*. Per questo, il problema ha senso anche per α razionale: ad esempio, se la frazione ai minimi termini che rappresenta α ha denominatore $> 10^9$, può avere interesse stabilire se α è approssimabile con frazioni con denominatori < 100.

La misura più ovvia della "bontà dell'approssimazione di α con una frazione a/b è la distanza euclidea

$$\left|\alpha - \frac{a}{b}\right|$$

Quando viene usata la distanza euclidea, parliamo di *approssimazioni del I tipo*. Talvolta invece è utile usare come bontà dell'approssimazione di α con a/b la differenza

$$|b\alpha - a|$$

In questo caso si valuta quanto i multipli di α sono vicini ad un intero, e si parla di *approssimazioni del II tipo*.[25]

Definizione 2.11.1 *Sia α un numero reale positivo (razionale o irrazionale). Una frazione* ***irriducibile*** *a/b (a, b interi, $a \geq 0$, $b > 0$) è detta:*

- ***miglior approssimazione del I tipo*** *per α se per ogni c, d interi, con $c \geq 0$, $0 < d \leq b$ e inoltre $c \neq a$ nel caso in cui fosse $d = b$, si ha:*

$$\left|\alpha - \frac{c}{d}\right| \; > \; \left|\alpha - \frac{a}{b}\right|$$

- ***miglior approssimazione del II tipo*** *per α se per ogni c, d interi, con $c \geq 0$, $0 < d \leq b$ e inoltre $c \neq a$ nel caso in cui fosse $d = b$, si ha:*

$$|d\alpha - c| \; > \; |b\alpha - a|$$

[24] Dal nome di Diofanto d'Alessandria, vissuto probabilmente verso la metà del II secolo d.C., reso celebre specialmente dalle *Osservazioni su Diofanto*, il testo che raccoglie le annotazioni che Fermat trascrisse sui margini della propria copia dell'*Aritmetica* di Diofanto. Talvolta si usa l'aggettivo "diofantina" come sinonimo di "diofantea".

[25] Sull'origine storica e sullo sviluppo dei concetti di approssimazione di I e II tipo nell'opera di Lagrange si veda Giacardi, Roero e Viola (1995), specialmente p. 175.

La distinzione fra i due tipi di approssimazione può sembrare solo un fatto formale, in quanto si passa dall'una all'altra "misura" moltiplicando o dividendo per b, ma il punto è proprio questo, dato che b fa parte del problema, visto che sono maggiormente interessanti i denominatori b "piccoli". Peraltro si prova subito che:

Proposizione 2.11.2 *Ogni miglior approssimazione del II tipo è necessariamente una miglior approssimazione del I tipo, ed esistono miglior approssimazioni del I tipo che non lo sono del II.*

DIMOSTRAZIONE. Per assurdo, dalle disuguaglianze

$$\left|\alpha - \frac{c}{d}\right| \leq \left|\alpha - \frac{a}{b}\right|, \quad \frac{c}{d} \neq \frac{a}{b}, \quad d \leq b$$

moltiplicando termine a termine la prima per la terza, si ha:

$$|d\alpha - c| \leq |b\alpha - a|$$

ossia se a/b non è miglior approssimazione del I tipo, non può esserlo del II.

Ora $1/3$ è, come subito si vede, una miglior approssimazione del I tipo per $\alpha = 1/5$. Infatti, $|\frac{1}{5} - \frac{1}{3}| = \frac{2}{15}$, mentre con denominatori minori di 3 abbiamo le frazioni $0/1, 1/1, 1/2$ e quelle maggiori di 1, che sono tutte approssimazioni del I tipo "peggiori" di $1/3$. Ad esempio: $|\frac{1}{5} - \frac{1}{2}| = \frac{3}{10} > \frac{2}{15}$. Tuttavia, come approssimazione del II tipo, $0/1$ è migliore di $1/3$, in quanto $\left|1 \cdot \frac{1}{5} - 0\right| < \left|3 \cdot \frac{1}{5} - 1\right|$ e quindi $1/3$ *non* è miglior approssimazione del II tipo per $1/5$. ■

Osservazione 2.11.3 L'approssimazione del I tipo può sembrare la più intuitiva delle due, data la nostra abitudine di rappresentare numeri su una retta valutandone la distanza. Tuttavia l'approssimazione del II tipo è in un certo senso più "primitiva". Consideriamo ad esempio, come metafora, un artigiano che intende produrre una certa quantità di cerchi metallici per botti, al massimo una dozzina, da esporre e metter in vendita; i cerchi hanno 1 m di diametro, e sono prodotti con una sola saldatura; supponiamo infine che la banda di metallo venga venduta solo a metratura intera. Per minimizzare gli scarti, all'artigiano converrà fare un calcolo. Per produrre p cerchi servono esattamente $p\pi$ metri di banda, ma ne dovrà acquistare q, pari al minimo intero maggiore di $p\pi$, quindi con uno *scarto* di materiale pari a $q - p\pi$. Tabulando $p\pi$, q e lo scarto di materiale per $p = 1, \ldots, 12$ si ottiene la Tabella 2.4, dalla quale l'artigiano vedrà che, per una produzione fino a 12 cerchi, lo scarto minimo pari a meno di 1 cm, si ottiene producendo 7 cerchi utilizzando 22 m di banda. Naturalmente questo esempio presuppone da parte dell'artigiano

una conoscenza numerica di π di tipo decimale, come $\pi \approx 3.14159$, non il valore razionale archimedeo, $\pi \approx 22/7$, altrimenti il problema sarebbe risolto per definizione. Si noti ancora che, nel contesto delle migliori approssimazioni del secondo tipo, lo scarto ha esattamente la stessa dimensione (fisica) delle grandezze considerate. Si ritornerà su questo punto nella Sezione dedicata ai calendari.

cerchi	banda necessaria	acquisto	scarto
1	π	4	0.858407
2	$2\ \pi$	7	0.716815
3	$3\ \pi$	10	0.575222
4	$4\ \pi$	13	0.433629
5	$5\ \pi$	16	0.292037
6	$6\ \pi$	19	0.150444
7	$7\ \pi$	**22**	0.008851
8	$8\ \pi$	26	0.867259
9	$9\ \pi$	29	0.725666
10	$10\ \pi$	32	0.584073
11	$11\ \pi$	35	0.442481
12	$12\ \pi$	38	0.300888

Tabella 2.4: I calcoli del bottaio.

Osservazione 2.11.4 Discutiamo brevemente il ruolo della richiesta dell'irriducibilità della frazione a/b nella Definizione 2.11.1. Sia ad esempio $\alpha = \sqrt{5}$. È banale verificare che $9/4$ dista da α meno di ogni altra frazione c/d con denominatore $0 < d \leq 4$ e $c/d \neq 9/4$. Ovviamente $9/4$ è irriducibile, e quindi, in base alla Definizione 2.11.1, $9/4$ è migliore approssimazione del I tipo (di $\sqrt{5}$). Però se consideriamo $45/20$, che come numero razionale è lo stesso di $9/4$, si ha che

$$\left|\alpha - \frac{45}{20}\right| \ = \ 0.013932 \ > \ \left|\alpha - \frac{38}{17}\right| \ = 0.00077386$$

cioè vi sono frazioni con denominatore minore di 20 più vicine a $\sqrt{5}$ di quanto lo sia $45/20$. Questo prova che la proprietà di essere (o non essere) miglior

approssimazione del I tipo non può essere un attributo dei numeri razionali a/b, ma, caso mai, delle coppie (a, b) di interi $(a \geq 0, b > 0)$. Vale lo stesso per la proprietà di essere (o non essere) miglior approssimazione del II tipo. Infatti, sempre per $\alpha = \sqrt{5}$, si ha che se si tabula lo scarto $|q\alpha - p|$ per $1 \leq q \leq 12$ scegliendo il valore di p che lo minimizza (Tabella 2.5), allora si scopre che sia 9/4 che, risp., 18/8 danno scarto minore di ogni altra frazione c/d con denominatore d minore o uguale di 4 o risp. di 8 (con l'eccezione di 9/4 nel caso di 18/8), mentre si ha

$$|12\alpha - 27| = 0.167184 \ > \ |9\alpha - 20| = 0.124612$$

Quindi se si togliesse nella definizione di miglior approssimazione del II tipo la richiesta della irriducibilità, sia 9/4 che 18/8 sarebbero migliori approssimazioni del II tipo di $\sqrt{5}$, mentre 27/12 non lo sarebbe!

q	$q\alpha$	p =round$(q\alpha)$	$\lvert q\alpha - p\rvert$
1	2.23607	2	0.236068
2	4.47214	4	0.472136
3	6.7082	7	0.291796
4	8.94427	9	0.0557281
5	11.1803	11	0.18034
6	13.4164	13	0.416408
7	15.6525	16	0.347524
8	17.8885	18	0.111456
9	20.1246	20	0.124612
10	22.3607	22	0.36068
11	24.5967	25	0.403252
12	26.8328	27	0.167184

Tabella 2.5: Migliori approssimazioni del II tipo di $\alpha = \sqrt{5}$.

2.11.1 Caratterizzazione delle miglior approssimazioni del II tipo

I due teoremi seguenti costituiscono assieme il risultato principale che lega la miglior approssimazione del II tipo alle frazioni continue. Vedremo infatti che

le migliori approssimazioni di $\alpha > 0$ del II tipo coincidono, con una banale eccezione, con le convergenti dello sviluppo di α in frazione continua.

Teorema 2.11.5 *Sia α un numero reale positivo. Sia a/b una miglior approssimazione del II tipo di α. Allora a/b coincide con una convergente A_k/B_k dello sviluppo in frazione continua di α (per un opportuno $k \geq 0$).*

DIMOSTRAZIONE. Sia $\alpha = [a_0; a_1, a_2, \ldots]$ (se α è razionale utilizziamo lo sviluppo finito canonico, quello "più corto", con l'ultimo quoziente ≥ 2). Ricordiamo che

$$a_0 = \frac{A_0}{B_0} < \frac{A_2}{B_2} < \frac{A_4}{B_4} < \cdots \alpha \cdots < \frac{A_5}{B_5} < \frac{A_3}{B_3} < \frac{A_1}{B_1} < a_0 + 1$$

Supponiamo per assurdo che a/b sia una miglior approssimazione del II tipo di α, ma non sia una convergente. Questo esclude in particolare il caso $\alpha = a/b$ se α è razionale, dato che α è l'ultima convergente dello sviluppo finito; ovviamente $\alpha \neq a/b$ se α è irrazionale. Le restanti possibilità allora sono solo tre:

- $a/b < a_0 = A_0/B_0$. Dato che $b \geq 1$, sarebbe allora:

  $$|b\alpha - a| = b \cdot \left|\alpha - \frac{a}{b}\right| \geq \left|\alpha - \frac{a}{b}\right| > |\alpha - a_0|$$

  cioè $a_0/1$ darebbe uno scarto minore di a/b, contro l'ipotesi che a/b sia miglior approssimazione del II tipo ($1 \leq b$).

- $a/b > A_1/B_1$. Dato che $A_1/B_1 > \alpha$, sarebbe allora:

  $$|b\alpha - a| = b \cdot \left|\alpha - \frac{a}{b}\right| > b \cdot \left|\frac{A_1}{B_1} - \frac{a}{b}\right| \geq b\,\frac{1}{B_1 b} = \frac{1}{B_1} = \frac{1}{a_1}$$

  Essendo ovviamente $|\alpha - a_0| < 1/a_1$ (questa disuguaglianza deriva da $\alpha = a_0 + 1/(a_1 + \ldots)$), otteremmo $|b\alpha - a| > 1/a_1 > |\alpha - a_0|$ cioè ancora $a_0/1$ darebbe uno scarto minore di a/b, contro l'ipotesi che a/b sia miglior approssimazione del II tipo ($1 \leq b$).

- $a_0 = A_0/B_0 < a/b < A_1/B_1$. In questo caso a/b deve essere strettamente compresa fra due convergenti "dallo stesso lato" di α, e siano ad esempio A_{j-1}/B_{j-1} e A_{j+1}/B_{j+1} per un opportuno $j \geq 1$ (gli indici devono avere la stessa parità). Dalle due disuguaglianze:

  $$\left|\frac{a}{b} - \frac{A_{j-1}}{B_{j-1}}\right| \geq \frac{1}{b\,B_{j-1}}$$
  $$\left|\frac{a}{b} - \frac{A_{j-1}}{B_{j-1}}\right| < \left|\frac{A_j}{B_j} - \frac{A_{j-1}}{B_{j-1}}\right| = \frac{1}{B_j B_{j-1}}$$

la prima delle quali è ovvia, mentre la seconda delle quali viene dall'ordinamento

$$\frac{A_{j-1}}{B_{j-1}} < \frac{a}{b} < \frac{A_{j+1}}{B_{j+1}} < \ldots \alpha \ldots < \frac{A_j}{B_j} \tag{2.44}$$

e dall'uguaglianza $A_jB_{j-1} - A_{j-1}B_j = (-1)^{j-1}$ (2.11), otteniamo che

$$B_j < b$$

D'altra parte, sempre per l'ordinamento (2.44):

$$\left|\alpha - \frac{a}{b}\right| \geq \left|\frac{A_{j+1}}{B_{j+1}} - \frac{a}{b}\right| \geq \frac{1}{b\,B_{j+1}}$$

e quindi:

$$|b\alpha - a| \geq \frac{1}{B_{j+1}}$$

Tuttavia, per la (2.43):

$$|B_j\alpha - A_j| \leq \frac{1}{B_{j+1}}$$

Si avrebbe quindi che A_j/B_j darebbe uno scarto minore di a/b, contro l'ipotesi che a/b sia miglior approssimazione del II tipo ($B_j < b$).

Escluse quindi tutte le possibilità, il teorema è provato. ■

Il Teorema 2.11.5 si inverte con una fastidiosa eccezione relativa alle prime convergenti: A_0/B_0 e A_1/B_1 Infatti, non si può affermare in generale che A_0/B_0 sia sempre una miglior approssimazione del II tipo per un reale α. Controesempi ovvi sono i numeri del tipo $\alpha = n+\frac{1}{2}$ con n intero ≥ 0, per i quali si ha $|1\cdot\alpha - n| = |1\cdot\alpha - (n+1)| = \frac{1}{2}$, e per i quali $A_0/B_0 = n/1$ non è miglior approssimazione del II tipo, avendo scarto "a pari merito" con $(n+1)/1$ che ha lo stesso denominatore. Tuttavia vi sono altri controesempi, non del tipo "un intero $+\frac{1}{2}$", ma altrettanti ovvi, come $\alpha = 2.75 = 11/4 = [2;1,3] = 2 + \frac{1}{1+1/3}$. Si ha in questo caso $A_0/B_0 = 2/1$ e $A_1/B_1 = 3/1$. Ma:

$$\underbrace{|1\cdot\alpha - 3|}_{=0.25} < \underbrace{|1\cdot\alpha - 2|}_{=0.75}$$

e quindi $A_0/B_0 = 2/1$ non è miglior approssimazione del II tipo per α in quanto viene "battuta" da $3/1$. La stessa conclusione vale per gli α che verificano delle disuguaglianze del tipo $n + \frac{1}{2} < \alpha < (n+1)$ con n intero ≥ 0. Controesempi del tipo $\alpha = 11/4$ richiedono un perfezionamento degli enunciati

e delle dimostrazioni che si trovano in taluni testi classici (Khinchin, 1964, Teorema 17, p. 26; Rockett e Szüsz, 1992, Teorema 2, p. 21).[26] Qui seguiremo allora Hardy e Wright (1964, p. 151), che, per evitare i problemi con A_0/B_0 e A_1/B_1, si limitano alle sole convergenti di indice ≥ 2, e supporremo inoltre, per semplificare ulteriormente la dimostrazione, che α sia irrazionale.

Teorema 2.11.6 *Sia α un numero irrazionale positivo. Ogni convergente A_k/B_k con $k \geq 2$ dello sviluppo in frazione continua di α è miglior approssimazione del II tipo di α (e quindi anche del I tipo).*

DIMOSTRAZIONE. Sia dato A_k/B_k con $k \geq 2$. Dobbiamo provare che le disuguaglianze $0 < d \leq B_k$ e $A_k/B_k \neq c/d$ implicano che

$$|d\alpha - c| > |B_k\alpha - A_k| \tag{2.45}$$

Essendo $k \geq 2$ si ha $0 < d \leq B_k < B_{k+1}$. Consideriamo il sistema di equazioni lineari 2×2 nelle incognite x, y:

$$\begin{cases} A_{k+1}x + A_k y &= c \\ B_{k+1}x + B_k y &= d \end{cases}$$

Per la (2.11) il determinante della matrice dei coefficienti è

$$\begin{vmatrix} A_{k+1} & A_k \\ B_{k+1} & B_k \end{vmatrix} = A_{k+1}B_k - A_k B_{k+1} = (-1)^k$$

e quindi, per la Regola di Cramer, esiste un unica soluzione (x, y) del sistema, con x ed y interi:

$$x = \frac{\begin{vmatrix} c & A_k \\ d & B_k \end{vmatrix}}{(-1)^k}, \qquad y = \frac{\begin{vmatrix} A_{k+1} & c \\ B_{k+1} & d \end{vmatrix}}{(-1)^k}$$

• Per prima cosa proviamo che $x \neq 0$ e $y \neq 0$. Se per assurdo fosse $x = 0$ avremmo $cB_k = dA_k$, ossia $A_k/B_k = c/d$, contro l'ipotesi che sia $A_k/B_k \neq c/d$. Se per assurdo fosse $y = 0$ avremmo $x \neq 0$ (dato che $x = y = 0$ è impossibile),

[26] Per il lettore interessato, il punto tecnico in discussione è che se si sa che due denominatori di convergenti verificano la disuguaglianza $B_k \leq B_n$, da questa non si può dedurre $k \leq n$, in quanto se si verificasse il caso $B_k = B_n$ (cosa che accade per 11/4 per il quale $B_0 = B_1 = 1$) potrebbe essere $(k, n) = (0, 1)$ oppure anche $(k, n) = (1, 0)$, quindi, in questo secondo caso, si avrebbe $k > n$.

e dalla seconda equazione si ricaverebbe $d = xB_{k+1}$, contro la disuguaglianza $0 < d \leq B_k < B_{k+1}$.

• Verifichiamo ora che x ed y hanno segni opposti. Se $x < 0$, dalla seconda equazione si ha $B_k y = d - B_{k+1}x > d > 0$ e quindi $y > 0$. Se $x > 0$, allora la seconda equazione $B_k y = d - B_{k+1}x$, visto che $0 < d < B_{k+1}$, implica che $B_k y < 0$, e quindi $y < 0$.

• Ora le convergenti A_k/B_k e A_{k+1}/B_{k+1} si trovano da lati opposti rispetto ad α (irrazionale), per cui le differenze $(\alpha - A_k/B_k)$ e $(\alpha - A_{k+1}/B_{k+1})$ non sono nulle ed hanno segni opposti. Quindi, visto che B_k e B_{k+1} sono positivi, hanno segni opposti le differenze:

$$B_k\alpha - A_k \quad \text{e} \quad B_{k+1}\alpha - A_{k+1}$$

e di conseguenza

$$y\,(B_k\alpha - A_k) \quad \text{e} \quad x\,(B_{k+1}\alpha - A_{k+1})$$

hanno lo stesso segno.

Usando le due equazioni lineari si ottiene:

$$d\alpha - c = (B_{k+1}x + B_k y)\alpha - (A_{k+1}x + A_k y) = x\,(B_{k+1}\alpha - A_{k+1}) + y\,(B_k\alpha - A_k)$$

Prendendo i valori assoluti (dato che gli addendi hanno lo stesso segno):

$$\begin{aligned} |d\alpha - c| &= |x\,(B_{k+1}\alpha - A_{k+1})| + |y\,(B_k\alpha - A_k)| && (2.46)\\ &> |y\,(B_k\alpha - A_k)| \geq |B_k\alpha - A_k| && (2.47) \end{aligned}$$

dalla quale segue subito la 2.45 (si osservi che qui si usa ancora l'ipotesi che α sia irrazionale, perché altrimenti potrebbe essere $(B_{k+1}\alpha - A_{k+1}) = 0$). ■

Possiamo ora ridimostrare parte del Teorema 2.8.1 (ii):

Corollario 2.11.7 *Sia α un numero irrazionale positivo. Due successive convergenti A_{k-1}/B_{k-1} e A_k/B_k con $k \geq 2$ dello sviluppo in frazione continua di α verificano:*

$$\left|\alpha - \frac{A_{k-1}}{B_{k-1}}\right| > \left|\alpha - \frac{A_k}{B_k}\right|$$

Dimostrazione. La convergente A_k/B_k (con $k \geq 2$) è miglior approssimazione del II tipo per α, e quindi anche del I tipo. Si ha $0 < B_{k-1} \leq B_k$, e due qualunque convergenti sono diverse tra loro. Per definizione di miglior approssimazione del I tipo si ha la tesi. ■

Esercizio 2.11.8 Utilizzando un software di computer algebra, verificare direttamente in base alla definizione (senza far ricorso al Teorema 2.11.6) che l'approssimazione 355/113 di Zu Chongzhi è miglior approssimazione del II tipo per π.

SOLUZIONE. Si tratta di verificare che per ogni coppia (p, q) di interi $p \geq 1$ e $1 \leq q \leq 113$ si ha

$$|q\,\pi - p| > |113\,\pi - 355|$$

Usiamo *Mathematica* ed il valore di π implicito in questo software. Poniamo quindi $q =$ `Range[1,113]`; calcoliamo i multipli $q\pi$, per ciascuno di questi determiniamo l'intero più vicino $p =$ `Round[qπ]` e gli scarti corrispondenti $|q\pi - p| =$ `Abs[q pi - p]`. Basta poi trovare il minimo di questi: la risposta è `355 - 113 π`. ■

Osservazione 2.11.9 Il calcolo numerico di π può essere effettuato (per difetto) calcolando l'area di un n–gono regolare con "tanti" lati, inscritto nel cerchio di raggio $r = 1$ e di area $\pi r^2 = \pi$. Le aree di questi poligoni possono essere calcolate con una semplice formula di ricorrenza (che sfrutta solo il teorema di Pitagora) usando come punto di partenza l'esagono regolare e raddoppiando ad ogni iterazione il numero n dei lati che sarà quindi del tipo $n = 3 \times 2^k$, con $k = 1, 2, \ldots, k_{\max}$. Dal punto di vista del calcolo numerico, il problema è quello di mantenere costante una buona approssimazione nel calcolo delle radici quadrate richieste dall'applicazione del teorema di Pitagora quando si deve calcolare un lato di un triangolo rettangolo noti che siano gli altri due.

Per il calcolo di π nella matematica cinese antica si vedano Martzloff (2006, pp. 277–282) e Straffin (1998). Seguendo questi autori, Liu Hui (ca. 220–280) realizzò $k_{\max} = 5$ iterazioni, corrispondenti al calcolo dell'area di un poligono regolare di 192 lati, ottenendo $\pi \approx 3.14103$. Liu Hui stesso, o un suo allievo, estese il calcolo a $k_{\max} = 9$, corrispondente ad un poligono di 3072 lati, ottenendo $\pi \approx 3.14159$. Duecento anni dopo, vero l'anno 480, Zu Chongzhi usò $k_{\max} = 12$, corrispondente ad un poligono di 24576 lati, ottenendo $\pi \approx 3.1415926$.[27]

[27] Un semplice codice *Mathematica* che genera le iterazioni è:

```
kmax = 12;
k = 1;
c[1] = 1;
a[1] = Sqrt[1 - (c[1]/2)^2];
Do[n = 3 2^k; a[n] = Sqrt[1 - (c[n]/2)^2];
             c[2 n] = Sqrt[(c[n]/2)^2 + (1 - a[n])^2], {k, 1, kmax}]
Print[N[n c[n]/2, 8]]
```

In particolare il valore $k_{\max} = 12$ qui impostato genera l'approssimazione di Zu Chongzhi.

Non è invece ben conosciuto come successivamente Zu ottenne da questo dato la sua celebre approssimazione razionale $\pi \approx 355/133$. È notevole che l'approssimazione razionale $355/113$ di π fu scoperta in Europa appena verso la fine del XVI secolo, grazie agli studi di Valentinus Otho, Adriaan Anthonisz, ed Adriaan Metius.

2.11.2 Caratterizzazione delle miglior approssimazioni del I tipo

Abbiamo visto, come conseguenza del Teorema 2.11.6 e della Proposizione 2.11.2, che ogni convergente A_k/B_k con $k \geq 2$ dello sviluppo in frazione continua di un numero irrazionale α è miglior approssimazione del I tipo di α. Tuttavia, le convergenti non sono le sole migliori approssimazioni del I tipo. Vale infatti il risultato seguente, che estende in parte il Teorema 2.11.6:

Teorema 2.11.10 *Sia $\alpha > 0$ un irrazionale, e siano A_{k-2}/B_{k-2} e A_{k-1}/B_{k-1} due convergenti successive dello sviluppo di α in frazione continua. Allora ogni frazione intermedia*

$$\phi_j = \frac{j\,A_{k-1} + A_{k-2}}{j\,B_{k-1} + B_{k-2}} \tag{2.48}$$

con $a_k/2 < j < a_k$ è miglior approssimazione del I tipo di α.

Si noti che per $j = a_k$ la $\phi_{a_k} = A_k/B_k$ è una convergente, ed è quindi miglior approssimazione del I tipo per il Teorema 2.11.6. Il Teorema 2.11.10 si inverte quasi completamente: l'unica eventuale eccezione è per $j = a_k/2$ (se intero):

Teorema 2.11.11 *Ogni miglior approssimazione del I tipo di un irrazionale positivo α è una convergente oppure una frazione intermedia* (2.48) *con $a_k/2 \leq j < a_k$.*

Per le dimostrazioni e per una trattazione completa dell'argomento rimandiamo a Khinchin (1964, pp. 22–26); si veda anche Coppel (2009, p. 186).

Osservazione 2.11.12 Per illustrare i teoremi precedenti 2.11.10 e 2.11.11, consideriamo $\alpha = \pi$ e le due convergenti successive $A_2/B_2 = \frac{333}{106}$ e $A_3/B_3 = \frac{355}{113}$; ricordiamo che $\pi = [3;\, 7, 15, 1, 292, 1, \ldots]$ e quindi $a_4 = 292$. La successione delle frazioni

$$\phi_j = \frac{j\,A_3 + A_2}{j\,B_3 + B_2} = \frac{j \cdot 355 + 333}{j \cdot 113 + 106}$$

parte (per $j = 0$) da $\frac{333}{106}$ e tende (per $j \to \infty$) a $\frac{355}{113}$ (si veda la Figura 2.6). I suoi primi valori con $j \geq 1$ non possono essere miglior approssimazioni del

I tipo, in quanto vengono "battuti" da $\frac{355}{113}$. Ad un certo punto però la successione giunge, alla sinistra di π, ad una distanza da π simile a quella di $\frac{355}{113}$: il primo valore della successione che scende ad una distanza da π minore di quella di $\frac{355}{113}$ è $\phi_{146} = \frac{52163}{16604}$. Si noti che $146 = a_4/2$. I valori successivi per $146 < j < 292$ sono tutti miglior approssimazioni del I tipo, per il Teorema 2.11.10, e per $j = 292$ la successione assume il valore della convergente $\phi_{292} = A_4/B_4 = \frac{103993}{33102}$, che è miglior approssimazione del I tipo per il Teorema 2.11.6. In relazione al Teorema 2.11.11, in questo esempio si può verificare direttamente in base alla definizione (con il metodo dell'Esercizio 2.11.8) che anche $\phi_{146} = \frac{52163}{16604}$ (corrispondente all'indice $j = a_4/2$) è miglior approssimazione del I tipo di π. Sempre in riferimento alla Figura 2.6, se si calcola la frazione $\phi_{293} = \frac{104348}{33215}$, con $j = 293 > a_4 = 292$, si può verificare direttamente in base alla definizione (sempre con il metodo dell'Esercizio 2.11.8) che anche ϕ_{293} è miglior approssimazione del I tipo: questo può sembrare in contrasto con il Teorema 2.11.11, ma non lo è, in quanto

$$\frac{104348}{33215} = \frac{1 \cdot A_4 + A_3}{1 \cdot B_4 + B_3} = \frac{1 \cdot 103993 + 355}{1 \cdot 33102 + 113}$$

è una frazione intermedia del tipo (2.48) con $k = 5$ e $j = a_5 = 1$.

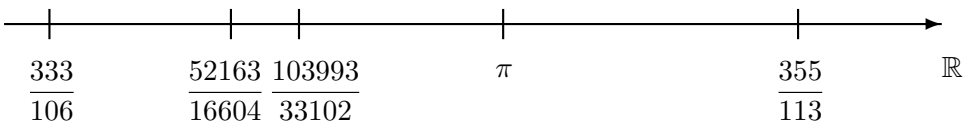


Figura 2.6: Miglior approssimazioni di π (distanze da π disegnate in scala logaritmica)

2.11.3 Approssimazione di $\sqrt{3}$ in Archimede

Abbiamo già osservato che Archimede enunciò senza alcuna spiegazione le stime:

$$\frac{265}{153} < \sqrt{3} < \frac{1351}{780}$$

e che alcuni autori (Audisio, 1930) hanno osservato che si tratta rispettivamente delle convergenti A_8/B_8 ed A_{11}/B_{11} dello sviluppo in frazione continua di $\sqrt{3}$. Da questa osservazione nasce il problema di investigare se Archimede

possedesse in un qualche senso un calcolo simile a quello delle nostre frazioni continue. Qui proporremo la tesi che l'uso delle "frazioni misteriose" 265/153 e 1351/780 derivi unicamente da una procedura molto comune all'epoca, ossia l'uso (e la lettura attenta) delle tavole.

Per semplicità, considerimo una tavola a 3 colonne, che contenga nella prima colonna gli interi $1 \leq k \leq 30$, nella seconda i loro quadrati k^2 e nella terza i tripli $3k^2$ di tali quadrati:

k	k^2	$3k^2$	k	k^2	$3k^2$	k	k^2	$3k^2$
1	1	3	11	121	363	21	441	1323
2	4	12	12	144	432	22	484	1452
3	9	27	13	169	507	23	529	1587
4	16	48	14	196	588	24	576	1728
5	25	75	15	225	675	25	625	1875
6	36	108	16	256	768	26	676	2028
7	49	147	17	289	867	27	729	2187
8	64	192	18	324	972	28	784	2352
9	81	243	19	361	1083	29	841	2523
10	100	300	20	400	1200	30	900	2700

Tavole di questo tipo erano già a disposizione dei Caldei (Rawlinson, 1842). Archimede sapeva[28] che la colonna del quadrati e quella dei tripli dei quadrati non possono avere elementi in comune (altrimenti esisterebbero due interi p, q tali che $p^2 = 3q^2$, ossia $\sqrt{3}$ sarebbe razionale). Diventa allora naturale chiedersi se si trovano nella tabella un quadrato p^2 ed un triplo di un quadrato $3q^2$ che siano *approssimativamente* uguali, nel senso che $|p^2 - 3q^2|$ sia il minimo possibile (atteso che tale minimo non può essere 0). Se supponiamo p, q primi fra loro, possiamo escudere che siano entrambi pari. Pertanto, i soli casi possibili per i valori p, q minimizzanti sono quelli per i quali p^2 e $3q^2$ siano consecutivi, uno pari ed uno dispari, ed allora $p^2 - 3q^2 = \pm 1$, e quelli in cui p^2 e $3q^2$ siano due numeri dispari consecutivi, ed allora $p^2 - 3q^2 = \pm 2$.

Esaminando sistematicamente la tabella, si individuano per ispezione diretta le coppie (p, q) per cui $p^2 - 3q^2$ vale ± 1 oppure ± 2. Tali coppie sono

[28] Almeno dal famosissimo passo di Platone: *Il nostro Teodoro ci disegnava certe figure sulle potenze, per esempio, su quella di tre piedi [quadrati] e quella di cinque, dimostrando che codeste potenze, rispetto alla lunghezza [del lato], non sono commensurabili con l'unità del piede* (*Teeteto*, 147d-148b).

esattamente $(1,1),(2,1),(5,3),(7,4),(19,11),(26,15)$, in corrispondenza alle quali la differenza p^2-3q^2 assume rispettivamente i valori $-2,1,-2,1,-2,1$. Usando l'identità:

$$(p+3q)^2-3(p+q)^2=-2\,(p^2-3q^2)$$

vediamo che se una coppia (p,q) verifica l'equazione $p^2-3q^2=1$, allora la coppia $(p',q')=(p+3q,p+q)$ verifica l'equazione $p'^2-3q'^2=-2$; e che se una coppia (p,q) verifica l'equazione $p^2-3q^2=-2$, allora la coppia $(p',q')=(p+3q,p+q)/2$ verifica l'equazione $p'^2=3q'^2=1$.[29]

Poniamo ora $(p_0,q_0)=(1,1)$, e definiamo per induzione una successione $(p_k,q_k)_{k\geq 1}$ ponendo:

$$(p_k,q_k)=\begin{cases}(p_{k-1}+3q_{k-1},\ p_{k-1}+q_{k-1}) & \text{per } k \text{ pari}\\ \left(\dfrac{p_{k-1}+3q_{k-1}}{2},\ \dfrac{p_{k-1}+q_{k-1}}{2}\right) & \text{per } k \text{ dispari}\end{cases} \tag{2.49}$$

Individuiamo alcuni elementi della successione:[30]

k	0	1	2	3	4	5	6	7	8	9	10	11	12
p_k	1	2	5	7	19	26	71	97	265	362	989	1351	3691
q_k	1	1	3	4	11	15	41	56	153	209	571	780	2131

Conoscendo ora lo sviluppo in frazione continua $\sqrt{3}=[1;\{1,2\}]$, possiamo verificare che le successioni p_k e q_k verificano le equazioni di Eulero che definiscono i numeratori A_k ed i denominatori B_k delle convergenti di $\sqrt{3}$. Infatti, si ha $p_0=1=[\sqrt{3}]=A_0$, $q_0=1=B_0$; $p_1=2=A_1$, $q_1=1=B_1$.

Se $k\geq 2$ è pari, poniamo $(p_{k-2},q_{k-2})=(P,Q)$, e quindi, essendo $k-1$ dispari, per la (2.49) si ha:

$$\begin{aligned}(p_{k-1},q_{k-1}) &= ((P+3Q)/2,\,(P+Q)/2)\\ (p_k,q_k) &= ((4P+6Q)/2,\,(2P+4Q)/2)=(2P+3Q,\,P+2Q)\end{aligned}$$

[29] Si vede subito che se p^2 e $3q^2$ sono dispari consecutivi, allora p, q e $3q$ sono dispari, per cui $p+3q$ e $p+q$ sono entrambi pari, e quindi, dividendo per 2, otteniamo interi.

[30] Gli utenti *Mathematica* possono usare i comandi:

```
p[0] = 1;
q[0] = 1;
Print[{p[0],q[0]}]
Do[ p[k] = If[EvenQ[k], p[k - 1] + 3 q[k - 1], (p[k - 1] + 3 q[k - 1])/2];
    q[k] = If[EvenQ[k], p[k - 1] + q[k - 1], (p[k - 1] + q[k - 1])/2];
Print[{p[k],q[k]}], {k, 1, 12}]
```

e sono quindi verificate le formule di Eulero per $k \geq 2$ pari (nelle quali $a_k = 2$), in quanto

$$\begin{cases} 2 \cdot p_{k-1} + p_{k-2} & = 2 \cdot (P + 3Q)/2 + P & = 2P + 3Q & = p_k \\ 2 \cdot q_{k-1} + q_{k-2} & = 2 \cdot (P + Q)/2 + Q & = P + 2Q & = q_k \end{cases}$$

Se invece $k \geq 3$ è dispari, poniamo $(p_{k-2}, q_{k-2}) = (P, Q)$, e quindi, essendo $k - 1$ pari, per la (2.49) si ha:

$$\begin{aligned} (p_{k-1}, q_{k-1}) &= (P + 3Q,\, P + Q)) \\ (p_k, q_k) &= (2P + 3Q,\, P + 2Q) \end{aligned}$$

e sono quindi verificate le formule di Eulero per $k \geq 3$ dispari (dove $a_k = 1$):

$$\begin{cases} 1 \cdot p_{k-1} + p_{k-2} & = 1 \cdot (P + 3Q) + P & = 2P + 3Q & = p_k \\ 1 \cdot q_{k-1} + q_{k-2} & = 1 \cdot (P + Q) + Q & = P + 2Q & = q_k \end{cases}$$

Abbiamo quindi dimostrato direttamente che:

Teorema 2.11.13 *Se p, q sono soluzioni intere (positive) prime fra loro dell'equazione*

$$p^2 - 3q^2 = 1$$

oppure dell'equazione

$$p^2 - 3q^2 = -2$$

allora p/q è una convergente della frazione continua di $\sqrt{3}$.

Possiamo quindi qui appoggiare la congettura (Zeuthen, 1893–1902; Heath, 1897) secondo la quale, sostanzialmente, le approssimazioni "misteriose" 265/153 e 1351/780 di $\sqrt{3}$ usate da Archimede derivino unicamente da una accurata ispezione di una tavola di quadrati sufficientemente estesa, cioè tale da poter riconoscere che $265^2 - 3 \times 153^2 = -2$ e che $1351^2 - 3 \times 780^2 = +1$, senza alcuna necessità di ricorrere a qualche forma della teoria delle frazioni continue e delle relative convergenti.

Osservazione 2.11.14 Un'equazione diofantea del tipo $p^2 - m\,q^2 = \pm 1$ (oppure del tipo $p^2 - m\,q^2 = \pm 2$), in cui m è un intero non quadrato e delle quali si cercano soluzioni intere p e q non nulle, sono dette *equazioni di Pell–Fermat*. Sono strettamente legate alla teoria delle frazioni continue, ma non vengono trattate sistematicamente in questo volume. Si veda ad esempio Chrystal (1886, Parte II, Cap. XXXIII, §18; pp. 482 segg.); per una trattazione di impronta storica, si veda Weil (1984), disponibile anche in italiano (1993).

2.12 Calendari

Una delle più interessanti applicazioni della teoria delle frazioni continue è l'interpretazione e la giustificazione delle regole dei calendari civili. Un calendario civile dipende essenzialmente da due parametri temporali: a, la durata dell'*anno tropico*, e b, la durata del *mese sinodico*, misurate entrambe in *giorni solari medi*. Rimandiamo ai manuali d'astronomia per le definizione formali di queste grandezze; ricordiamo solo che, essenzialmente, l'anno tropico è l'intervallo di tempo fra due successivi equinozi di primavera (transito del Sole al punto γ dell'eclittica), mentre il mese sinodico, o mese lunare, è l'intervallo di tempo fra due successivi noviluni (in un determinato luogo). L'unità di misura del tempo, il *giorno*, può essere definito come l'intervallo di tempo fra due successive culminazioni (massima altezza sull'orizzonte) del Sole in un determinato luogo. Tutte tre le grandezze, per la dinamica del sistema solare, sono in effetti variabili nel tempo. Come valori di a e b possono essere qui assunti i valori stimati al 1° gennaio 2000 (Doggett, 1992, pp. 575–608):

$$a = 365.2421896698, \quad b = 29.5305888531 \tag{2.50}$$

Nel caso dell'anno tropico, si studia preferibilmente la mantissa

$$a' = 0.2421896698$$

di a, ovvero l'eccesso della durata dell'anno tropico rispetto ad un numero intero di giorni. Accanto ad a e b va considerata la durata dell'anno tropico in mesi sinodici, che è semplicemente il rapporto

$$r = a/b = 12.3682663927$$

Ai fini del nostro studio è inessenziale sapere se i valori "veri" di questi tre numeri sono razionali o no (probabilmente non ha neppure senso porsi la domanda).

Dal punto di vista esclusivamente aritmetico, un calendario consiste in un'approssimazione diofantea di una delle tre costanti a, b, o r. Ad esempio, supponiamo di avere una "buona" approssimazione razionale p/q di a, ossia supponiamo di sapere che 1 anno tropico $\approx p/q$ giorni. Questo significa che q anni durano "quasi esattamente" p giorni, per cui il problema tecnico di un calendario che parta dall'approssimazione diofantea $\approx p/q$ consiste nella definizione di una regola che ripartisca p giorni in un periodo di q anni tropici. Un calendario di questo tipo è detto un *calendario solare*. Esempi di calendari solari sono il calendario giuliano ed il calendario gregoriano.

Se invece si considera una "buona" approssimazione razionale p/q di b, per cui 1 mese lunare $\approx p/q$ giorni, otteniamo che q mesi lunari durano "quasi esattamente" p giorni, per cui il problema tecnico di un calendario che parta dall'approssimazione diofantea di b consiste nella ripartizione di p giorni in un periodo di q mesi lunari. Un calendario di questo tipo è detto un *calendario lunare*. Un esempio di calendario lunare è il calendario islamico dell'Egira.

Se infine si considera una "buona" approssimazione razionale p/q di r, per cui 1 anno tropico $\approx p/q$ mesi lunari, otteniamo che q anni tropici durano "quasi esattamente" p mesi lunari, per cui il problema tecnico di un calendario che parta dall'approssimazione diofantea di r consiste nella ripartizione di p mesi in un periodo di q anni. Un calendario di questo tipo è detto un *calendario soli–lunare*. Esempi di calendari soli–lunari sono il calendario ebraico ed il calendario cinese Daming.

Dovendo approssimare a', b o r con razionali, è naturale pensare alle migliori approssimazioni date dalle convergenti degli sviluppi in frazione continua, o alle relative frazioni intermedie. Gli sviluppi in frazione continua dei parametri a', b ed r sono:

$$\begin{aligned} a' &= [0;\, 4, 7, 1, 3, \mathbf{27}, 1, 6, 1, 3, \ldots] \\ b &= [29;\, 1, 1, 7, 1, 2, \mathbf{17}, 2, 5, 2, \ldots] \\ r &= [12;\, 2, 1, 2, 1, 1, \mathbf{17}, 3, \ldots] \end{aligned}$$

con rispettive convergenti A_k/B_k (calcolate per $0 \le k \le 5$):

k	0	1	2	3	4	5	6	...
convergenti di a':	0	$\frac{1}{4}$	$\frac{7}{29}$	$\frac{8}{33}$	$\mathbf{\frac{31}{128}}$	$\frac{845}{3489}$	...	...
convergenti di b:	29	30	$\frac{59}{2}$	$\frac{443}{15}$	$\frac{502}{17}$	$\mathbf{\frac{1447}{49}}$	$\frac{25101}{850}$	...
convergenti di r:	12	$\frac{25}{2}$	$\frac{37}{3}$	$\frac{99}{8}$	$\frac{136}{11}$	$\mathbf{\frac{235}{19}}$	$\frac{4131}{334}$	...

Sono stati evidenziati in grassetto i denominatori parziali "grandi" e le convergenti immediatamente precedenti, che appaiono di conseguenza "buone" approssimazioni. Nel caso di un calendario solare, questo mostra che una regola buona dal punto di vista matematico sarebbe quella che inserisse 31 anni bisestili ogni 128 anni, o equivalentemente, 93 anni bisestili ogni 384 anni. Come spiegheremo nella sezione successiva, il calendario gregoriano, adottato dalla maggior parte degli stati cattolici nel 1582 o negli anni immediatamente

successivi, ma molto più tardi dagli altri stati cristiani,[31] inserisce 97 anni bisestili ogni 400. L'origine di questa "misteriosa" frazione 97/400 è l'oggetto della prossima sezione (Brusadin e Invernizzi, 2011).

2.12.1 La "misteriosa" frazione gregoriana 97/400

L'espansione geografica del dominio di Roma nel I secolo comportò la necessità di sincronizzare le date civili con le stagioni.[32] Nel 46 a.C. Giulio Cesare stabilì quindi che l'anno doveva avere di norma 365 giorni, ma che ogni 4 anni doveva essere intercalato un anno di 366 giorni (*annus intercalarius*), ottenuto aggiungendo 1 giorno al mese di febbraio. La regola giuliana, sufficientemente precisa ai fini agricoli, commerciali e militari, comporta comunque un errore che, accumulatosi durante 14 secoli, produsse nel XV secolo un errore di una decina di giorni: praticamente, ad esempio, il 21 marzo 1580, data teorica dell'equinozio di primavera, il Sole era già transitato al punto γ da una decina di giorni. Questo rendeva errata la determinazione annuale della data della Pasqua di Resurrezione, fissata dal Concilio di Nicea del 325 alla prima domenica successiva al primo plenilunio dopo l'equinozio di primavera. Nacque così la riforma del calendario voluta da papa Gregorio XIII e deliberata nel 1582. Come è noto, la riforma del calendario gregoriano afferma che un anno è un anno bisestile, composto di 366 giorni, se e solo se è divisibile per 4, esattamente come nel calendario giuliano, ma con l'eccezione degli anni secolari, che restano bisestili se e solo se sono divisibili per 400 (ad esempio il 1900 ed il 2100 non sono bisestili, mentre il 2000 lo è). Pertanto, il calendario gregoriano ha 97 anni bisestili ogni 400 anni. Ciò equivale a dire che la lunghezza media dell'anno tropico del calendario gregoriano è *implicitamente* definita da $365 + 97/400 = 365.2425$ giorni medi solari, cioè $365^d\,5^h\,49'\,12''$. In realtà, nessun documento della Commissione calendariale nominata da Papa Gregorio XIII contiene l'*esplicita* dichiarazione che un particolare valore sperimentale dell'anno tropico sia stato scelto come riferimento per la riforma. L'obiettivo della Commissione era il disegno di un calendario che fosse, da un lato, il più possibile coerente con i fenomeni astronomici comunemente osservati, come il novilunio o l'equinozio di primavera, ma che nel contempo non si appoggiasse a dati empirici sperimentali, suscettibili di cambiamento per la precisione crescente degli strumenti di misura, e che comunque fosse del tutto indipendente

[31] La Gran Bretagna, l'Impero britannico, e quindi gli U.S.A., nel 1752; l'Alaska nel 1867; la Russia nel 1818; la Grecia nel 1923.

[32] Ad esempio, una norma ipotetica che disponesse che i legionari in Britannia dovessero passare dagli abiti leggeri a quelli pesanti ai primi di novembre, sarabbe stata del tutto assurda se ai primi di novembre fosse stata piena estate.

da qualsiasi teoria dei moti celesti (Zoboli, 1877). Così si pone in modo molto naturale la questione da dove provenga la "misteriosa" frazione 97/400.

La prima spiegazione basata sulle frazioni continue della regola dei 97/400 risale ad Eulero (1797), che calcola i primi convergenti dello sviluppo in frazione continua di $a' = 20935/86400$, che è, secondo i suoi dati, la parte frazionaria della lunghezza media dell'anno tropico in giorni solari, ovvero $a' = 5^h\,48'\,55''$. Eulero dedica all'argomento solo quindici righe, alla fine delle quali conclude senza ulteriori commenti che

> ... unde sequitur quadringentis annis abundare 97 dies.

Qui assumeremo, come ipotesi di lavoro, che la commissione pontificia abbia utilizzato come durata dell'anno tropico il dato delle Tavole Alfonsine: $a = 365^d 5^h 49' 16''$ (Oriani, 1785; Brusadin e Invernizzi, 2011), che, convertito in un numero razionale di giorni, diventa $365 + a'$ con $a' = 5239/21600$. Le convergenti di a' sono:

$$0,\ \frac{1}{4},\ \frac{8}{33},\ \frac{57}{235},\ \frac{122}{503},\ \frac{301}{1241},\ \frac{5239}{21600}$$

nessuna delle quali ha denominatore 400. Storicamente, è ragionevole escludere che la Commissione pontificia abbia potuto nel 1582 calcolare queste convergenti usando una teoria simile a quella delle frazioni continue. Essa però potrebbe essere giunta agli stessi valori con il metodo "tabellare" che già abbiamo supposto possa esser stato usato da Archimede per il calcolo delle approssimazioni di $\sqrt{3}$.

Nella Tabella 2.12.1 mostriamo i semplici calcoli necessari per verificare che 1/4, 8/33 e 57/235 sono migliori approssimazioni del II tipo di $a' = \frac{5239}{21600} = 5^h 49' 16''$. Questi calcoli potevano essere effettuati molto facilmente a mano nel XVI secolo, usando la notazione sessagesimale, solo con addizioni ripetute di a', e individuando per ispezione visiva diretta i tre valori di $|qa' - p|$ (indicati dalle frecce) corrispondenti a tre miglior approssimazioni del II tipo: $p/q = 1/4,\ 8/33,\ 57/235$. Queste tre frazioni, per il Teorema 2.11.6, sono anche convergenti di a', ma in un certo senso "ad insaputa" della Commissione calendariale.

Resta da spiegare come dalle tre approssimazioni trovate, 1/4, 8/33 e 57/235, si possa giungere a 97/400. È conveniente escludere 1/4, che corrisponde proprio al calendario giuliano da riformare (1 anno bisestile ogni 4) e concentrarsi sulle due frazioni 8/33 e 57/235. La chiave per ottenere 97/400 sono le frazioni intermedie. Il calcolo della mediante di due frazioni era ben

noto ai calendaristi; anzi, essi possedevano una tecnica di interpolazione più raffinata, che consente di "modulare" il denominatore.[33]

q	qa'	p	$\lvert qa'-p\rvert$
1	$5^h49'16''$	0^d	$5^h49'16''$
2	$11^h38'32''$	0^d	$11^h38'32''$
3	$17^h27'48''$	1^d	$6^h32'12''$
$\longrightarrow$ **4**	$23^h17'\ 4''$	$\mathbf{1}^d$	$0^h42'56''$
...	...	...	...
32	$7^d18^h16'32''$	8^d	$5^h43'28''$
$\longrightarrow$ **33**	$8^d\ 0^h\ 5'48''$	$\mathbf{8}^d$	$0^h\ 5'48''$
34	$8^d\ 5^h55'\ 4''$	8^d	$5^h55'\ 4''$
...	...	...	...
234	$56^d18^h\ 8'24''$	57^d	$5^h51'36''$
$\longrightarrow$ **235**	$56^d23^h57'40''$	$\mathbf{57}^d$	$0^h\ 2'20''$
236	$57^d\ 5^h46'56''$	57^d	$5^h46'56''$
...	...	...	...

Tabella 2.6: Calcolo manuale delle migliori approssimazioni del II tipo di $a' = 5^h49'16''$.

Proposizione 2.12.1 *Siano a, b, c, d interi positivi tali che $a/b < c/d$. Allora per ogni coppia (m, n) di interi positivi si ha:*

$$\frac{a}{b} < \frac{ma+nc}{mb+nd} < \frac{c}{d} \tag{2.51}$$

La dimostrazione è immediata.

Atteso quindi che $8/33 < a' < 57/235$, si può trovare un'approssimazione nello stesso intervallo con denominatore multiplo di 100 (in modo che la riforma lasci inalterati gli anni bisestili del calendario giuliano, uno ogni quattro, con la sola eccezione di taluni anni secolari) semplicemente scegliendo $m = 5, n = 1$, ed ottenendo così la "misteriosa" frazione:

$$a' = 5^h49'16'' = \frac{5 \cdot 8 + 57}{5 \cdot 33 + 235}\ [\text{giorni}] = \frac{97}{400}\ [\text{giorni}]$$

[33] Questa tecnica era ad esempio già ben conosciuta in Cina nel IV–V secolo come "armonizzazione del denominatore [dei giorni]" (Martzloff, 2006), con evidente riferimento alle applicazioni ai calendari.

Alla fine, la durata dell'anno gregoriano è esattamente 365.2425 giorni, quindi più corto della misura moderna $a = 365.2421896698$ di circa $26.8''$ all'anno. Questa differenza produrrebbe un errore di un giorno in circa 3200 anni e teoricamente dovrebbe richiedere la soppressione di un giorno ulteriore ogni tremila o quattromila anni.[34]

2.12.2 Il ciclo metonico ed il calendario ebraico

Già Metone di Atene, astronomo greco del V sec. a.C., aveva osservato che 19 anni tropici corrispondono con buona approssimazione a 235 mesi lunari (ciclo metonico). Questo corrisponde all'approssimazione di r con la convergente $\frac{A_5}{B_5} = \frac{235}{19}$ del suo sviluppo. Sul ciclo metonico è basato il *calendario ebraico*, che appunto distribuisce 235 mesi lunari in 19 anni, 12 dei quali, gli *anni comuni*, sono composti ciascuno da 12 mesi, e 7 dei quali, detti *anni embolismici*, sono composti ciascuno da 13 mesi lunari ($12 \times 12 + 7 \times 13 = 235$). Si tratta di un calendario luni–solare, in quanto il mese è sempre quello lunare (per cui ad esempio tutti i pleniluni avvengono attorno al 15 del mese, ogni mese), ma, in ogni ciclo di 19 anni, a 7 di questi viene aggiunto un mese, che consente di tenere con buona approssimazione il passo con le stagioni. Un calendario luni–solare di questo tipo era già adottato dai babilonesi, ed era proprio quello in vigore a Roma prima della riforma di Giulio Cesare.

2.12.3 Il calendario islamico

Il *calendario islamico* dell'Egira (622) fornisce un esempio sull'uso delle frazioni intermedie. Prima della riforma del calendario di Maometto, i vari popoli arabi utilizzavano il calendario luni–solare di origine babilonese, basato sul ciclo metonico, con anni di 12 ed anni di 13 mesi. La rivelazione coranica fissò la durata dell'anno in 12 mesi lunari e proibì espressamente il tredicesimo mese (Sura 9, *Del Pentimento*, 36–37). Per ottenere un calendario lunare puro restava quindi da sincronizzare il più possibile l'inizio dei mesi con i noviluni. Ciò è legato allo sviluppo di b. Anche qui, come nel caso della riforma gregoriana, il primo problema è il valore scelto per b. Per il calendario islamico non è irragionevole assumere il valore del mese sinodico calcolato verso il 150 da Claudio Tolomeo e riportato nell'*Almagesto* (IV, 4), ossia, in

[34] Ad esempio, John Herschel (1792–1871) propose la soppressione del 29 febbraio 4000. Per lo più, si ritiene che il rallentamento del periodo di rivoluzione della Terra renderà non necessarie queste correzioni.

notazione sessagesimale, $b = 29; 31, 50, 8, 20$. La frazione corrispondente è

$$b = 29 + \frac{31}{60} + \frac{50}{60^2} + \frac{8}{60^3} + \frac{20}{60^4} = \frac{765433}{25920} = 29.530594\,\overline{135802469}$$

che ha come sviluppo in frazione continua:

$$b = [29;\, 1, 1, 7, 1, 2, 22, 1, 1, 1, 7]$$

e per convergenti:

$$29,\, 30,\, \frac{59}{2},\, \frac{443}{15},\, \frac{502}{17},\, \frac{1447}{49},\, \frac{32336}{1095},\, \frac{33783}{1144},\, \frac{66119}{2239},\, \frac{99902}{3383},\, \frac{765433}{25920}$$

La convergente $A_2/B_2 = 59/2$ suggerisce, in prima approssimazione, di distribuire $29 + 30 = 59$ giorni in 2 mesi, e questo si ottiene alternando mesi di 29 e mesi di 30 giorni. Per migliorare l'approssimazione, le convergenti successive sono poco pratiche, in quanto richiederebbero regole per periodi di 15, di 17 o di 49 mesi; sarebbe evidentemente utile una convergente con denominatore multiplo di 12, in modo da avere una regola fissa pluriannuale,[35] ma di queste non ce ne sono, almeno fra le prime 7 convergenti. Tuttavia, se consideriamo le frazioni intermedie fra le convergenti $A_4/B_4 = 502/17$ e $A_5/B_5 = 1447/49$, ossia le frazioni:

$$\frac{jA_5 + A_4}{jB_5 + B_4} = \frac{j \cdot 1447 + 502}{j \cdot 49 + 17}$$

con $0 < j < a_6 = 17$, vediamo che per $j = 7$ otteniamo

$$\frac{7 \cdot 1447 + 502}{7 \cdot 49 + 17} = \frac{10631}{360}$$

che è una frazione (intermedia) del tipo voluto. Pertanto, suddividendo 10631 giorni in 360 mesi lunari, ossia in 30 anni del calendario, si ottiene un risultato migliore della semplice alternanza fra mesi di 29 e mesi di 30 giorni. Dato che l'alternanza fornisce $180 \times (29 + 30) = 10620$ giorni in 30 anni, il calendario islamico, in seconda approssimazione, istituisce $10631 - 10620 = 11$ anni "bisestili" di $6 \times 29 + 6 \times 30 + 1 = 355$ giorni in ogni periodo di 30 anni.[36]

Notiamo che, per il Teorema 2.11.11, l'intermedia 10631/360 non è una miglior approssimazione del I tipo di α, in quanto deriva dall'indice $j = 7$ che è minore di $a_6/2 = 17/2 = 8.5$, ed infatti la convergente 1447/49 ha denominatore minore di 360 e dista da α meno dell'intermedia 10631/360. Si ha infatti:

$$\left|\alpha - \frac{1447}{49}\right| = 0.0000231249 < \left|\alpha - \frac{10631}{360}\right| = 0.0000335644$$

[35] Qui per "anno" va inteso ovviamente un periodo di 12 mesi lunari.

[36] Per la precisione, in ogni ciclo di 30 anni, numerati da 1 a 30, gli anni bisestili sono quelli di indice 2, 5, 8, 10, 13, 16, 19, 21, 24, 27 e 29.

2.13 Le convergenti come funzioni

Nella sezione conclusiva di questo capitolo vogliamo introdurre lo studio dello sviluppo in frazione continua semplice

$$[a_0(x), a_1(x), a_2(x), \ldots]$$

di un numero reale $x \in [0,1]$ come funzione della variabile x. Lo studio di queste funzioni è alla base della *teoria della misura delle frazioni continue* (Khinchin, 1964, Cap. III).

In particolare ci interessa considerare le convergenti:

$$c_0(x) = a_0(x), \quad c_1(x) = a_0(x) + \frac{1}{a_1(x)}, \quad c_2(x) = a_0(x) + \frac{1}{a_1(x) + \dfrac{1}{a_2(x)}}, \quad \ldots$$

come funzioni di x, $0 \le x \le 1$. Bisogna porre particolare attenzione al dominio delle convergenti come funzioni, in quanto se $x = p/q \in \mathbb{Q}$, lo sviluppo in frazione continua di x non ha *tutte* le convergenti, in quanto ad un certo punto termina con l'ultima convergente calcolabile uguale esattamente a p/q.

2.13.1 Le convergenti di ordine 0 ed 1

La convergente di ordine $k = 0$ è banale, ed è definita da:

$$c_0(x) = \begin{cases} 0 & \text{se } 0 \le x < 1 \\ 1 & \text{se } x = 1 \end{cases} \tag{2.52}$$

Le convergenti degli interi 0 ed 1 terminano con quella di ordine 0 e quindi la convergente $c_1(x)$ di ordine $k = 1$ non è definita sugli elementi di $E_0 = \{0, 1\}$. Consideriamo $\frac{1}{2} < x < 1$: si ha $a_1(x) = \left[\frac{1}{x}\right] = 1$ e $c_1(x) = 1$. Se invece $x = \frac{1}{2}$ si ha evidentemente $c_1(x) = \frac{1}{2}$. Consideriamo ora valori $x < \frac{1}{2}$: questi, al decrescere di x a partire da $\frac{1}{2}$ (escluso), hanno uno sviluppo del tipo

$$x = \frac{1}{2 + \xi}$$

con ξ che rappresenta una frazione continua $\xi = 1/\ldots < 1$, e cresce $(0 < \xi < 1)$ fino a che asintoticamente si ottiene $\frac{1}{2+1} = \frac{1}{3}$; questo implica che:

$$c_1(x) = \begin{cases} 1 & \text{se } \frac{1}{2} < x < 1 \\ \frac{1}{2} & \text{se } \frac{1}{3} < x \le \frac{1}{2} \end{cases} \tag{2.53}$$

Induttivamente[37] otteniamo che la convergente $c_1(x)$ di ordine $k = 1$ è costante a tratti, ed è definita da:

$$c_1(x) = \begin{cases} 1 & \text{se } \frac{1}{2} < x < 1 \\ \frac{1}{2} & \text{se } \frac{1}{3} < x \leq \frac{1}{2} \\ \frac{1}{3} & \text{se } \frac{1}{4} < x \leq \frac{1}{3} \\ \dots & \\ \frac{1}{i} & \text{se } \frac{1}{i+1} < x \leq \frac{1}{i} \\ \dots & \end{cases} \tag{2.54}$$

I punti di discontinuità di $c_1(x)$, di tipo salto, sono gli elementi dell'insieme

$$E_1 = \left\{ \frac{1}{i} \ : \ i \geq 2 \right\} = \left\{ \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots \right\}$$

che sono esattamente i razionali le cui convergenti terminano con quella di ordine 1.

Si noti che $c_1(x)$, che a priori non è definita sugli elementi di $E_0 = \{0, 1\}$, può essere prolungata per continuità ponendo $c_1(0) = 0$ e $c_1(1) = 1$, definendo quindi $c_1(x)$ su tutto $[0, 1]$. Nella Figura 2.7 è rappresentato il grafico di $c_1(x)$ su $[0, 1]$.

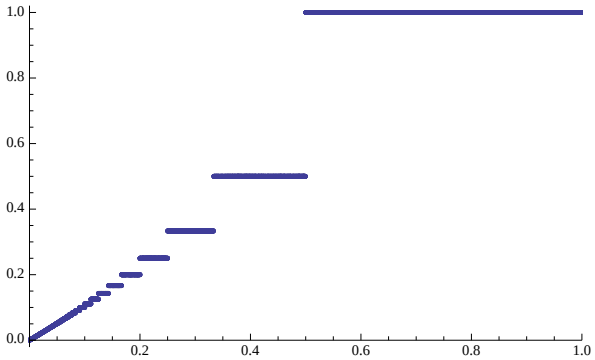


Figura 2.7: Grafico di $c_1(x)$ su $[0, 1]$. La funzione è costante a tratti, monotona crescente, e continua a destra.

[37] In questa sezione, lasciamo alcuni dettagli dimostrativi al lettore come esercizio; in taluni casi può trattarsi di esercizi formalmente impegnativi.

2.13.2 La convergente di ordine 2

Le convergenti degli elementi $\frac{1}{i}$ $(i \geq 2)$ di E_1 terminano con quella di ordine 1 e quindi, a priori, la convergente $c_2(x)$ di ordine $k = 2$ non è definita sugli elementi di $E_0 \cup E_1$. Consideriamo l'insieme

$$E_2 = \left\{ \frac{1}{i + \frac{1}{j}} \, : \, i \geq 1, j \geq 1 \right\}$$

costituito dai razionali di $[0,1] \setminus (E_0 \cup E_1)$ le cui convergenti terminano con quella di ordine 2. Ne esemplifichiamo un sottoinsieme

$$\begin{array}{cccccccccccccc}
\frac{1}{2} & \frac{2}{3} & \frac{3}{4} & \frac{4}{5} & \frac{5}{6} & \frac{6}{7} & \frac{7}{8} & \frac{8}{9} & \frac{9}{10} & \frac{10}{11} & \frac{11}{12} & \frac{12}{13} & \frac{13}{14} & \frac{14}{15} & \frac{15}{16} \\
\frac{1}{3} & \frac{2}{5} & \frac{3}{7} & \frac{4}{9} & \frac{5}{11} & \frac{6}{13} & \frac{7}{15} & \frac{8}{17} & \frac{9}{19} & \frac{10}{21} & \frac{11}{23} & \frac{12}{25} & \frac{13}{27} & \frac{14}{29} & \frac{15}{31} \\
\frac{1}{4} & \frac{2}{7} & \frac{3}{10} & \frac{4}{13} & \frac{5}{16} & \frac{6}{19} & \frac{7}{22} & \frac{8}{25} & \frac{9}{28} & \frac{10}{31} & \frac{11}{34} & \frac{12}{37} & \frac{13}{40} & \frac{14}{43} & \frac{15}{46} \\
\frac{1}{5} & \frac{2}{9} & \frac{3}{13} & \frac{4}{17} & \frac{5}{21} & \frac{6}{25} & \frac{7}{29} & \frac{8}{33} & \frac{9}{37} & \frac{10}{41} & \frac{11}{45} & \frac{12}{49} & \frac{13}{53} & \frac{14}{57} & \frac{15}{61} \\
\frac{1}{6} & \frac{2}{11} & \frac{3}{16} & \frac{4}{21} & \frac{5}{26} & \frac{6}{31} & \frac{7}{36} & \frac{8}{41} & \frac{9}{46} & \frac{10}{51} & \frac{11}{56} & \frac{12}{61} & \frac{13}{66} & \frac{14}{71} & \frac{15}{76} \\
\frac{1}{7} & \frac{2}{13} & \frac{3}{19} & \frac{4}{25} & \frac{5}{31} & \frac{6}{37} & \frac{7}{43} & \frac{8}{49} & \frac{9}{55} & \frac{10}{61} & \frac{11}{67} & \frac{12}{73} & \frac{13}{79} & \frac{14}{85} & \frac{15}{91} \\
\frac{1}{8} & \frac{2}{15} & \frac{3}{22} & \frac{4}{29} & \frac{5}{36} & \frac{6}{43} & \frac{7}{50} & \frac{8}{57} & \frac{9}{64} & \frac{10}{71} & \frac{11}{78} & \frac{12}{85} & \frac{13}{92} & \frac{14}{99} & \frac{15}{106} \\
\frac{1}{9} & \frac{2}{17} & \frac{3}{25} & \frac{4}{33} & \frac{5}{41} & \frac{6}{49} & \frac{7}{57} & \frac{8}{65} & \frac{9}{73} & \frac{10}{81} & \frac{11}{89} & \frac{12}{97} & \frac{13}{105} & \frac{14}{113} & \frac{15}{121} \\
\frac{1}{10} & \frac{2}{19} & \frac{3}{28} & \frac{4}{37} & \frac{5}{46} & \frac{6}{55} & \frac{7}{64} & \frac{8}{73} & \frac{9}{82} & \frac{10}{91} & \frac{11}{100} & \frac{12}{109} & \frac{13}{118} & \frac{14}{127} & \frac{15}{136} \\
\frac{1}{11} & \frac{2}{21} & \frac{3}{31} & \frac{4}{41} & \frac{5}{51} & \frac{6}{61} & \frac{7}{71} & \frac{8}{81} & \frac{9}{91} & \frac{10}{101} & \frac{11}{111} & \frac{12}{121} & \frac{13}{131} & \frac{14}{141} & \frac{15}{151}
\end{array}$$

in forma di matrice $(1 \leq i \leq 10,\ 1 \leq j \leq 15)$ dove, in ogni riga, il primo elemento è punto di discontinuità della convergente $c_1(x)$ precedente, di ordine $k = 1$. Si può verificare che $c_1(x)$ è costante a tratti, ed in particolare è costante in ciascun intervallo di estremi due razionali consecutivi della matrice doppiamente infinita $r_{ij} = 1/(i + 1/j)$, $i \geq 1, j \geq 1$.

Vediamo in particolare il caso dell'intervallo $(\frac{1}{2}, \frac{2}{3})$. Sia quindi $\frac{1}{2} < x < \frac{2}{3}$. Dato che $x > \frac{1}{2}$ si ha $a_1(x) = 1$ e quindi x ha uno sviluppo del tipo

$$x = 0 + \frac{1}{1 + \xi}$$

dove $\frac{1}{2} < \xi < 1$ (disuguaglianze si dimostrano facilmente equivalenti a $\frac{1}{2} < x < \frac{2}{3}$), e quindi $c_1(\xi) = 1$ (costante). Quindi

$$c_2(x) = \frac{1}{1 + c_1(\xi)} = \frac{1}{1 + 1} = \frac{1}{2}$$

Consideriamo come secondo esempio l'intervallo $(\frac{2}{9}, \frac{3}{13})$, che, leggendo la matrice r_{ij}, è il secondo della quarta riga, sottointervallo di $(\frac{1}{5}, \frac{1}{4})$. Sia quindi $\frac{2}{9} < x < \frac{3}{13}$. Dato che sull'intervallo $(\frac{1}{5}, \frac{1}{4})$ la convergente $a_1(x)$ è costante uguale a 4, x ha uno sviluppo del tipo

$$x = 0 + \frac{1}{4 + \xi}$$

dove $\frac{1}{3} < \xi < \frac{1}{2}$ (disuguaglianze si dimostrano facilmente equivalenti a $\frac{2}{9} < x < \frac{3}{13}$), e quindi $c_1(\xi) = \frac{1}{2}$ (costante). Quindi

$$c_2(x) = \frac{1}{4 + c_1(\xi)} = \frac{1}{4 + \frac{1}{2}} = \frac{2}{9}$$

Nella Figura 2.8 è rappresentato il grafico di $c_1(x)$ su $[0, 1]$. Quindi la conver-

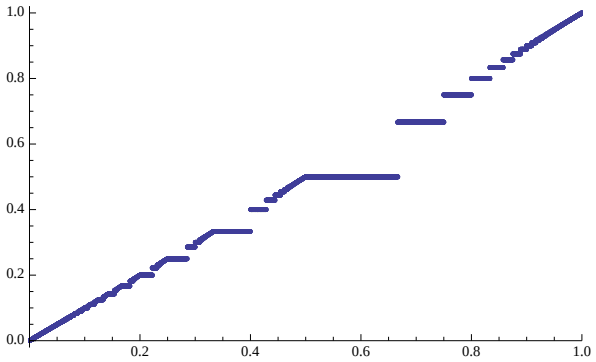


Figura 2.8: Grafico di $c_2(x)$ su $[0, 1]$.

gente $c_2(x)$ di ordine $k = 2$ è costante a tratti; assume un valore costante in ciascuno dei sottointervalli $\left(1/(i + \frac{1}{j}),\ 1/(i + \frac{1}{j+1})\right)$, ed è monotona crescente.

Osservazione 2.13.1 Il grafico di $c_2(x)$ presenta aspetti di "autosimilarità": in ciascuno degli intervalli in cui il grafico della precedente c_1 è costante, il grafico di c_2 è "invariante". Nella Figura 2.9 sono rappresentate parti diverse del grafico di $c_2(x)$, definite su intervalli del tipo $(\frac{1}{i+1}, \frac{1}{i})$.

2.13.3 Le convergenti di ordine $k \geq 3$

Per la convergente $c_3(x)$ ci limitiamo a riportarne il grafico nella Figura 2.10.

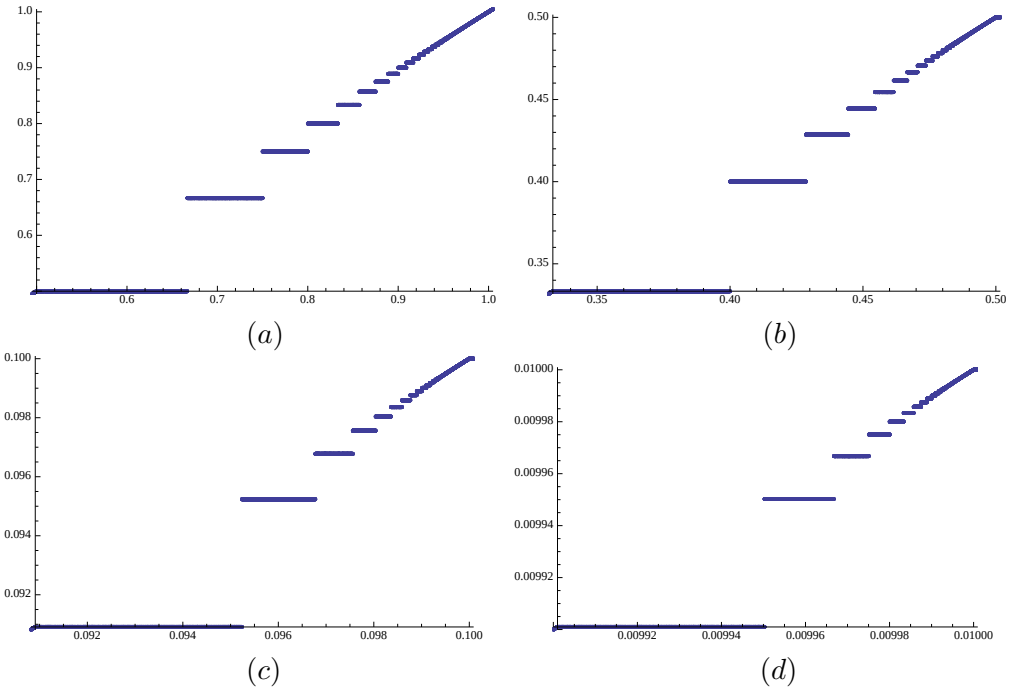


Figura 2.9: Parti diverse del grafico di $c_2(x)$, definite sugli intervalli: (a) $(\frac{1}{2}, 1)$; (b) $(\frac{1}{3}, \frac{1}{2})$; (c) $(\frac{1}{11}, \frac{1}{10})$; (d) $(\frac{1}{101}, \frac{1}{100})$.

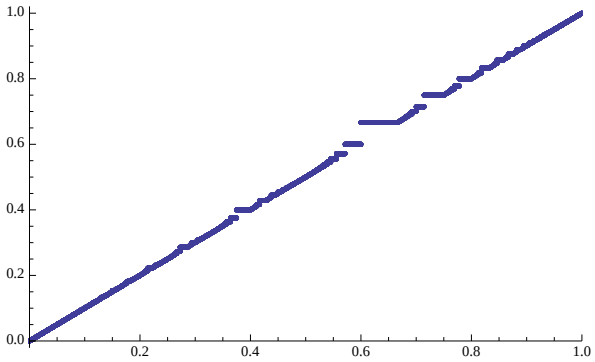


Figura 2.10: Grafico di $c_3(x)$ su $[0, 1]$

Per $c_3(x)$ si possono ripetere le stesse considerazioni presentate per le convergenti precedenti. Si noti come il grafico di $c_3(x)$ già approssima il grafico dell'identità, ovvero si "intuisce graficamente" che (almeno per x irrazionale) $c_k(x) \to x$ per $k \to \infty$.

Esercizio 2.13.2 Utilizzare i risultati di questa sezione per dimostrare direttamente, per via aritmetica, che se $x \in [0, 1]$ è irrazionale, lo sviluppo in frazione continua semplice di x converge ad x.

SUGGERIMENTO: Individuare aritmeticamente due rette $y = x \pm \epsilon_k$ che racchiudono il grafico di $c_k(x)$ (ossia $x - \epsilon_k \leq c_k(x) \leq x + \epsilon_k$), mostrando che $\epsilon_k \to 0$ per $k \to \infty$.

Capitolo 3

Approssimazione diofantea

3.1 Teorema di Dirichlet

La densità dei numeri razionali nei numeri reali implica banalmente che per ogni numero reale α esiste una successione $(p_n/q_n)_{n\geq 1}$ di numeri razionali che converge ad α. Si può anche fare in modo che questi razionali p_n/q_n (al variare di $n \geq 1$) siano tutti distinti, e quindi infiniti. Ad esempio, possiamo considerare lo sviluppo decimale $\alpha = a_0.\, a_1a_2a_3\ldots$ prendendo quello 9–periodico nei casi di doppia rappresentazione, e definire $p_n/q_n = a_0.\, a_1a_2a_3\ldots a_n$. Si può scegliere per p_n l'intero la cui rappresentazione in base 10 è costituita dalle cifre decimali dell'intero a_0 seguite dalle cifre "$a_1a_2a_3\ldots a_n$", e per q_n si deve scegliere allora $q_n = 10^n$. In questi casi, evidentemente, si ha

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{C}{q_n}$$

dove C è una costante. Ad esempio, se $\alpha = \pi$, abbiamo $p_1/q_1 = 31/10$, $p_2/q_2 = 314/100$, ecc., ed è

$$\left|\pi - \frac{314}{100}\right| < \frac{1}{100} \quad (C = 1)$$

Se invece $\alpha = 1$, possiamo prendere $p_2/q_2 = 99/100$, ed abbiamo

$$\left|1 - \frac{99}{100}\right| = \frac{1}{100} < \frac{2}{100} \quad (C = 2)$$

Una domanda che si pone naturalmente è allora se esiste una successione di razionali p_n/q_n tale che, al crescere di n, gli errori di approssimazione

$$\left|\alpha - \frac{p_n}{q_n}\right|$$

diminuiscano in modo "più rapido" di $1/q_n$, ad esempio come $(1/q_n)^2$, o come $(1/q_n)^3$, eventualmente moltiplicati per una costante C. E questo genera spontaneamente la seguente definizione.

Definizione 3.1.1 *Sia $\mu \geq 1$ un numero reale. Un numero $\alpha \in \mathbb{R}$ è detto* ***approssimabile di ordine*** *μ se*

- *esiste una costante $C > 0$, e*
- *esistono* ***infiniti*** *razionali r tali che per la loro rappresentazione irriducibile $r = p/q$ (p, q interi, $q \neq 0$) sia:*

$$\left|\alpha - \frac{p}{q}\right| < \frac{C}{q^\mu} \tag{3.1}$$

Come sempre in matematica, l'importanza e l'interesse della Definizione 3.1.1 dipenderanno dai teoremi che ne conseguiranno.

Osservazione 3.1.2 È utile notare che, se α è irrazionale, nella Definizione 3.1.1 la richiesta che esistano infiniti razionali r tali che per ***la*** loro rappresentazione irriducibile $r = p/q$ valga la (3.1) ***equivale*** a richiedere che esistano infiniti razionali r tali che per ***una*** loro rappresentazione $r = p/q$ valga la (3.1). Infatti, se la (3.1) è soddisfatta da infinite frazioni irriducibili, è anche soddisfatta in modo banale da infinite frazioni. Viceversa, supponiamo che la (3.1) sia sodisfatta da infinite frazioni, e valutiamo quante di queste sono irriducibili. Se ce ne fossero solo in numero finito, necessariamente la (3.1) dovrebbe valere per infinite rappresentazioni non irriducibili $(kp)/(kq)$ (k intero) dello stesso razionale $r = p/q$ (p, q primi fra loro), ossia:

$$\left|\alpha - \frac{p}{q}\right| = \left|\alpha - \frac{kp}{kq}\right| < \frac{C}{(kq)^\mu}$$

per infiniti valori di k, e quindi, essendo $C/(kq)^\mu$ piccolo a piacere, si avrebbe che α è razionale, uguale a p/q. ■

Iniziamo con il provare il fatto semplice che:

Proposizione 3.1.3 *Sia α approssimabile di ordine $\mu > 1$; sia ν tale che $1 \leq \nu < \mu$; allora α è approssimabile di ordine ν.*

Dimostrazione. Per ipotesi esistono C ed infiniti razionali p/q irriducibili tali che $|\alpha - p/q| < C/q^\mu$. Consideriamo le funzioni $x \mapsto C/x^\mu$ e $x \mapsto 1/x^\nu$

definite per $x \geq 1$. Quale che sia C, al crescere di x, il grafico della prima "scende sotto" quello della seconda: pertanto possono esistere solo un numero finito di q per i quali $C/q^\mu \geq 1/q^\nu$, e per tutti gli altri (che sono infiniti) si ha $|\alpha - p/q| < C/q^\mu < 1/q^\nu$. ■

Il prossimo teorema riguarda l'ordine di approssimabilità degli irrazionali, ed è conosciuto come *Teorema di Dirichlet sull'approssimazione diofantea*:[1]

Teorema 3.1.4 (Teorema di Dirichlet) *Sia α irrazionale. Per ogni intero $n > 0$ esistono interi p, q con $0 < q \leq n$ tali che*

$$|q\alpha - p| < \frac{1}{n} \quad \textit{cioè} \quad \left|\alpha - \frac{p}{q}\right| < \frac{1}{nq} \tag{3.2}$$

Dimostrazione. Come prima cosa notiamo che la (3.2) equivale (moltiplicando per $q > 0$) a

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq}$$

Consideriamo ora gli $n + 1$ numeri reali

$$0,\ \alpha - [\alpha],\ 2\alpha - [2\alpha],\ 3\alpha - [3\alpha],\ \ldots,\ n\alpha - [n\alpha]$$

e la loro distribuzione negli n intervalli

$$j/n \leq x < (j+1)/n, \quad j = 0, 1, \ldots, n-1$$

che costituiscono una partizione di $[0, 1)$. Per lo *Schubfachprinzip* di Dirichlet (nota a pie' di p. 43) esistono due numeri distinti $h\alpha - [h\alpha]$ e $k\alpha - [k\alpha]$ nello stesso intervallo, con $0 \leq h < k \leq n$. Gli intervalli hanno ampiezza $1/n$ e sono chiusi a sinistra e aperti a destra: quindi la differenza fra due suoi elementi è $< 1/n$, e quindi

$$\mid k\alpha - [k\alpha] - h\alpha - [h\alpha] \mid \ < \ \frac{1}{n}$$

Posto $q = k - h$ e $p = [k\alpha] - [h\alpha]$ si ha $|q\alpha - p| < 1/n$. ■

[1] Il Teorema 3.1.4 ed il suo importante Corollario 3.1.5 sono attribuiti a Dirichlet perché vengono citati nel rendiconto della seduta matematica di Berlino (*Berliner Sitzungsberichte*) del 14 aprile 1842 (Dirichlet Lejeune, 1889, p. 635). Tuttavia il risultato principale 3.1.5 qui presentato viene definito da Dirichlet come una conseguenza "nota da tempo" della teoria delle frazioni continue (*wie dies aus der Theorie der Kettenbrüche längst bekannt ist*) e gli stessi Hardy e Littlewood (1914, nota a pie' di p. 157) ammettono di non esser stati capaci di trovare (*we have been unable to discover*) il vero autore o i veri autori del "Teorema di Dirichlet sull'approssimazione diofantea".

Corollario 3.1.5 *Sia α irrazionale. Sia $C = 1$. Esistono infiniti razionali p/q tali che*

$$\left|\alpha - \frac{p}{q}\right| < \frac{C}{q^2} \tag{3.3}$$

Ovvero: ogni numero irrazionale è approssimabile di ordine 2 (o inferiore).

DIMOSTRAZIONE. Supponiamo per assurdo che esistano solo un numero finito r di coppie (p_i, q_i) $(i = 1, 2, \ldots, r)$ che verificano la (3.3) con $C = 1$. Dimostreremo che ce ne è una in più. Poniamo

$$\epsilon = \min\left\{\left|\alpha - \frac{p_i}{q_i}\right| \mid i = 1, 2, \ldots, r\right\}$$

Si ha $\epsilon > 0$ dato che α è irrazionale. Scegliamo $n > 0$ tale che $1/n < \epsilon$. Per il Teorema di Dirichlet (3.1.4) esiste un razionale p/q tale che $\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq} \leq \frac{1}{n} < \epsilon$: quindi, per definizione di ϵ, tale p/q è diverso da tutti i p_i/q_i. Inoltre $\left|\alpha - \frac{p}{q}\right| < \frac{1}{nq} \leq \frac{1}{q^2}$, dato che nel Teorema di Dirichlet (3.1.4) è $0 < q \leq n$: quindi p/q verifica la (3.3), assurdo. ■

DIMOSTRAZIONE ALTERNATIVA. Essendo α irrazionale, esistono infiniti convergenti A_n/B_n che, per la (2.43) nel Teorema 2.9.11, verificano le disuguaglianze

$$\left|\alpha - \frac{A_n}{B_n}\right| \leq \frac{1}{B_n B_{n+1}} < \frac{1}{B_n^2} \tag{3.4}$$

■

L'ordine di approssimabilità dei razionali è anche ben noto ed è facilmente determinato:

Teorema 3.1.6 *Sia $\epsilon > 0$ arbitrario. Un numero α* ***razionale*** *è approssimabile di ordine 1, ma non di ordine $1 + \epsilon$.*

DIMOSTRAZIONE. Sia $\alpha = a/b$ con a, b interi primi fra loro, $b \neq 0$. Le coppie di interi $(a \cdot 2^n + 1, b \cdot 2^n)$ con $b \cdot 2^n \neq 0$, per $n = 1, 2, \ldots$, sono infinite, e verificano la (3.1) con $\mu = 1$ ed un qualunque $C < 1$. Infatti

$$\left|\alpha - \frac{a \cdot 2^n + 1}{b \cdot 2^n}\right| = \left|\frac{a \cdot 2^n}{b \cdot 2^n} - \frac{a \cdot 2^n + 1}{b \cdot 2^n}\right| = \frac{1}{b \cdot 2^n} < \frac{C}{b \cdot 2^n}$$

Per la seconda parte del teorema, per ogni possibile approssimante $p/q \neq a/b$ si ha

$$\left|\frac{a}{b} - \frac{p}{q}\right| = \left|\frac{aq - pb}{bq}\right| \geq \frac{1}{bq}$$

Ora non esiste una costante $C > 0$ tale che (per $\epsilon > 0$)

$$\frac{1}{bq} < \frac{C}{q^{1+\epsilon}}$$

per infiniti valori di q (intero), in quanto il grafico di $C/x^{1+\epsilon}$ va sotto quello di $1/(bx)$ da un certo punto in poi, e quindi solo un numero finito di interi q può soddisfare $1/(bq) < C/q^{1+\epsilon}$. ■

Esempio 3.1.7 Sia

$$\alpha = \sum_{k=0}^{\infty} 10^{-2^k} = 0.11010001000000010000000000000010 \ldots\ldots 1 \ldots$$

Poniamo

$$\begin{aligned} r_0 &= 0.1 \\ r_1 &= 0.11 \\ r_2 &= 0.1101 \\ r_3 &= 0.11010001 \\ r_4 &= 0.1101000100000001 \\ r_5 &= 0.11010001000000010000000000000001 \end{aligned}$$

in generale ($m \geq 0$)

$$r_m = \sum_{k=0}^{m} 10^{-2^k}$$

Osserviamo che

$$\begin{aligned} |\alpha - 1/10| &= 0.01 \ldots < 2/10^2 \\ \left|\alpha - 11/10^2\right| &= 0.0001 \ldots < 2/10^4 \\ \left|\alpha - 1101/10^4\right| &= 0.00000001 \ldots < 2/10^8 \\ \left|\alpha - 11010001/10^8\right| &= 0.0000000000000001 \ldots < 2/10^{16} \end{aligned}$$

in generale ($m \geq 0$)

$$|\alpha - r_m| = \sum_{i=1}^{\infty} 10^{-2^{m+i}} < 2 \cdot 10^{-2^{m+1}} = 2 \cdot 10^{-2^m \cdot 2} = 2 \cdot (10^{-2^m})^2$$

Gli r_m hanno denominatore $q_m = 10^{2^m}$ e un certo numeratore p_m che non interessa scrivere ora, per cui

$$\left|\alpha - \frac{p_m}{q_m}\right| < \frac{2}{q_m^2}$$

Dato che gli r_m sono infiniti, si conclude che α è approssimabile di ordine 2, e quindi *è irrazionale*, cosa che si vedeva subito dallo sviluppo, ma il bello viene ora. Con gli stessi calcoli si prova immediatamente che

$$\alpha = \sum_{k=0}^{\infty} 10^{-3^k} = 0.10100000100000000000000000010000000000000000\ldots$$

ha le cifre 1 ai posti numero $1, 3, 9, 27, \ldots, 3^k, \ldots$ dopo la virgola, è approssimabile di ordine 3 (e quindi di ordine 2). Se le cifre 1 fossero ai posti numero $1, 4, 16, 64, \ldots, 4^k, \ldots$ dopo la virgola avremmo un numero irrazionale approssimabile di ordine 4 (e quindi di ordine 2 e 3). Cosa accadrebbe se le cifre 1 fossero ai posti di una successione a_k definitivamente $> n^k$ per ogni n? α sarebbe approssimabile di ordine n per ogni n? Quale potrebbe essere una tale successione a_k?

3.2 Teorema di Liouville

Il fatto che un razionale (algebrico di grado 1) non sia approssimabile di ordine $1 + \epsilon$, $(\epsilon > 0)$, viene facilmente esteso come segue (Liouville 1844, 1851).

Teorema 3.2.1 (Teorema di Liouville) *Sia α un numero **algebrico** di grado $n \geq 2$ (cioè un algebrico irrazionale). Poniamo $\lambda = n$. Allora esiste una costante $c = c(\alpha)$ (che dipende solo da α) tale che **per ogni** razionale p/q (p, q interi, $q > 0$) sia:*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^\lambda} \tag{3.5}$$

Inoltre, la costante $c = c(\alpha)$ è esplicitamente calcolabile (in funzione di α e dei coefficienti interi del polinomio irriducibile di cui α è radice).

Corollario 3.2.2 *Un numero α **algebrico** di grado $n \geq 2$ non è approssimabile di ordine $n + \epsilon$ $(\epsilon > 0)$.*

Dimostrazione. [Corollario 3.2.2] Vista la (3.5), se esistesse una costante C tale che per infiniti razionali irriducibili p/q sia $\left|\alpha - \frac{p}{q}\right| < \frac{C}{q^{n+\epsilon}}$, avremmo

per gli stessi infiniti razionali la doppia disuguaglianza:

$$\frac{C}{q^{n+\epsilon}} > \left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^n}$$

che è impossibile valga per infiniti valori di q (intero), in quanto il grafico di $C/x^{n+\epsilon}$ va sotto quello di $c(\alpha)/q^n$ da un certo punto in poi, e quindi solo un numero finito di interi q può soddisfare la disuguaglianza $C/q^{n+\epsilon} > c(\alpha)/q^n$. ■

Dimostrazione. [Teorema 3.2.1] Per ipotesi α è radice di un polinomio a coefficienti interi irriducibile su $\mathbb{Q}$

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

Fissiamo x nell'intervallo $[\alpha - 1, \alpha + 1]$. Allora

$$|x| < |\alpha| + 1$$

e derivando, definiamo una costante A come segue:

$$\begin{aligned} \left|f'(x)\right| &= \left|na_0x^{n-1} + (n-1)a_1x^{n-2} + \ldots + a_{n-1}\right| \\ &\leq \left|na_0x^{n-1}\right| + \left|(n-1)a_1x^{n-2}\right| + \ldots + |a_{n-1}| \\ &< n\,|a_0|\,\{|\alpha| + 1\}^{n-1} + (n-1)\,|a_1|\,\{|\alpha| + 1\}^{n-2} + \ldots + |a_{n-1}| := A \end{aligned}$$

Ora se p/q è una approssimazione razionale di α possiamo presumere[2] che $p/q \in [\alpha - 1, \alpha + 1]$ e che $f(p/q) \neq 0$ (infatti altrimenti $f(x)$ sarebbe riducibile su $\mathbb{Q}$). Quindi

$$|f(p/q)| = \frac{a_0p^n + a_1p^{n-1}q + \ldots + a_nq^n}{q^n}$$

Per il Teorema di Lagrange del valor medio (o dell'incremento finito) esiste ξ fra α e p/q tale che

$$f(p/q) = f(p/q) - f(\alpha) = f'(\xi) \cdot (p/q - \alpha)$$

da cui (notando che deve essere $f'(\xi) \neq 0$ poiché altrimenti $f(p/q) = 0$)

$$\left|\frac{p}{q} - \alpha\right| = \frac{|f(p/q)|}{|f'(\xi)|} > \frac{A^{-1}}{q^n}$$

cioè la (3.5) con $\lambda = n$ e $c = c(\alpha) = 1/A$. ■

[2] La disuguaglianza (3.5) diventa banale se p/q è "lontano" da α, ad esempio se dista da α più di 1, dato che $1/q^n$ vale al massimo proprio 1.

3.2.1 I numeri trascendenti di Liouville

Il Teorema 3.5 ed il Corollario 3.2.2 consentirono a Liouville di "esibire" espressamente (cioè tramite lo sviluppo decimale o lo sviluppo in frazione continua) alcuni numeri trascendenti, detti poi *numeri di Liouville*. Va notato che sino a quel punto l'esistenza dei numeri trascendenti, cioè quelli che "trascendono i poteri dell'algebra", era nota solo grazie a valutazioni di cardinalità.[3]

Definizione 3.2.3 *Un numero reale α è un* numero di Liouville *se per ogni intero $m \geq 1$ esiste* ***un*** *razionale p/q con $q > 1$ tale che*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m}$$

Esempio 3.2.4 Il numero

$$L = \sum_{k=1}^{\infty} 10^{-k!} = 0.11000100000000000000000001000\ldots$$

detto *costante di Liouville* è un numero di Liouville; infatti, dato un intero $m \geq 1$, poniamo:

$$p = \sum_{k=1}^{m} 10^{m!-k!}; \quad q = 10^{m!}$$

Consideriamo

$$\delta = \left|L - \frac{p}{q}\right| = \sum_{k=m+1}^{\infty} 10^{-k!} = 10^{-(m+1)!} + 10^{-(m+2)!} + \cdots < 10 \cdot 10^{-(m+1)!} \quad (3.6)$$

La disuguaglianza si giustifica semplicemente riflettendo sulla notazione posizionale: δ ha la prima cifra non nulla, pari a 1, al posto di ordine $(m+1)!$ dopo la virgola, mentre $10 \cdot 10^{-(m+1)!}$ ha la prima cifra non nulla, pari a 1, al posto precedente, quello di ordine $(m+1)! - 1$. Ora abbiamo:

$$\begin{aligned} 10 \cdot 10^{-(m+1)!} &= 10 \cdot 10^{-m! \cdot (m+1)} \\ &= 10 \cdot (10^{-m!})^{m+1} \\ &= 10 \cdot (10^{-m!})^{m} \cdot \overbrace{(10^{-m!})^{1}}^{\leq 1/10} \\ &\leq (10^{-m!})^{m} = \frac{1}{q^m} \end{aligned}$$

■

[3] Dato che i numeri algebrici sono numerabili e che i numeri reali non lo sono, devono esistere numeri non–algebrici, ossia trascendenti (Fiori e Invernizzi, 2009).

Teorema 3.2.5 *Ogni numero α di Liouville è un numero trascendente.*

DIMOSTRAZIONE. Supponiamo α algebrico di grado n. Per ogni intero $m \geq n+1$ la definizione di numero di Liouville implica che esiste un razionale p/q con $q > 1$ tale che

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^m} < \frac{1}{q^{n+1}}$$

cioè α è approssimabile di ordine $n+1$, assurdo. ■

Si noti che la costante L di Liouville è un esempio esplicito di un numero trascendente del quale si conoscono *esattamente tutte* le cifre decimali. Trascriviamo qui nel seguito, come spunto storico, il passo di Liouville (1851) in cui egli stabilisce la trascendenza di L (per ottenere L si scelga $\ell = 10$).

> **1**. J'ai présenté, il y a longtemps, sur ce sujet, à l'Académie des Sciences, et fait insérer ans le tome XVIII des *Comptes rendues* (pages 883 et 910; séances des 13 et 20 mai 1844) deux Notes que je crois devoir reproduire ici en les colplétant. La première est ansi conçue:
>
> « Pour donner des examples de fractions continues dont on puisse démontrer en toute rigueur que leur valeur n'est racine d'aucune équation algébrique
>
> $$f(x) = ax^n + bx^{n-1} + \ldots + gx + h - 0,$$
>
> $a, b, \ldots, g, h$ étant des entiers, il suffit de se rappeler que $\frac{p_0}{q_0}$ et $\frac{p}{q}$ étant deux réduites successives de la fraction continue qui exprime le développement d'une racine incommensurable x de cette équation, le quotient incomplet μ, qui vient après la réduite $\frac{p}{q}$, et sert à former la réduite suivante, finira (cela résulte d'une formule de Lagrange, *voyez* les Mémoires de Berlin, année 1768) par être, pou les valeurs de q très–grandes, constamment inférieur à
>
> $$\pm \frac{df p, q}{q\, f(p,q)\, dp},$$
>
> expression essentiellement positive où l'on suppose
>
> $$f(p,q) = q^n\, f\left(\frac{p}{q}\right) = ap^n + bp^{n-1}q + \ldots + hq^n.$$
>
> » Abstraction faite des signes, on aura dès lors, à plus forte raison,
>
> $$\mu < \frac{df(p,q)}{q\, dp}$$
>
> puisque $f(p,q)$ est un entier égal au moins à l'unité si l'on admet (ce qui est permis) que l'équation
>
> $$f(x) = 0$$
>
> a été débarrassée de tout facteur commensurable; $f(p,q) = 0$ donnerait, en effet,
>
> $$f\left(\frac{p}{q}\right) = 0$$

» Maintenant représentons par $f'(x)$ la dérivée de $f(x)$; l'inégalité ci–dessous deviendra

$$\mu < q^{n-2}\, f'\left(\frac{p}{q}\right).$$

Or, $f'\left(\frac{p}{q}\right)$ est une quantité finie qui tend vers la limite $f'(x)$, comme $\frac{p}{q}$ vers la limite x. En désignant par A un certain nombre fixe supérieur à cette limite, on sera donc certain d'avoir

$$\mu < A\, q^{n-2}.$$

» Ainsi, *les quotients incomplets d'une fraction continue représentant la racine x d'une équation algébrique de degré n, à coefficients rationnels, sont assujettis à ne jamais dépasser le produit d'un certain nombre constant par la puissance $(n-2)^{ième}$ du dénominateur de la réduite précédente.*

» Il suffira de donner aux quotients incomplets μ un mode de formation qui les fasse grandir au delà du terme indiqué, pour obtenir des fractions continues dont la valeur ne pourra satisfaire à aucune équation algébrique proprement dit; cela arrive, par example, si partant d'un premier quotient incomplet quelconque, on forme chacun des suivants μ à l'aide de la réduite $\frac{p}{q}$ qui la précède, d'après la loi $\mu = q^q$, ou bien encore d'après la loi $\mu = q^m$, m étant l'indice du rang de μ.

» Au reste, la métode précédente, qui s'est offerte la première, n'est la seule ni même la plus simple pu'on puisse employer. Ajoutons qu'il y a aussi des théorèmes analoques pour les séries ordinaires. Nous citerons en particulier la série

$$\frac{1}{\ell} + \frac{1}{\ell^{1\cdot 2}} + \frac{1}{\ell^{1\cdot 2\cdot 3}} + \ldots + \frac{1}{\ell^{1\cdot 2\cdot 3\cdots m}} + \ldots,$$

ℓ étant un nombre entier. »

3.3 Teorema di Hurwitz–Borel

Una linea di ricerca iniziata da Adolf Hurwitz (1894) e da Émile Borel (1903) migliora il risultato del Corollario 3.1.5 identificando la costante C ottimale nella disuguaglianza (3.3).

Teorema 3.3.1 (Teorema di Hurwitz–Borel) *Sia α irrazionale. Sia $C = 1/\sqrt{5}$. Esistono infiniti razionali p/q tali che*

$$\left|\alpha - \frac{p}{q}\right| < \frac{C}{q^2} \tag{3.7}$$

La costante $C = 1/\sqrt{5}$ è ottimale, nel senso che esiste un irrazionale α^* con la proprietà che se $0 < \theta < 1/\sqrt{5}$ la disuguaglianza

$$\left|\alpha^* - \frac{p}{q}\right| < \frac{\theta}{q^2} \tag{3.8}$$

ha solo un numero finito di soluzioni razionali p/q.

Prima di dimostrare il teorema, vogliamo soddisfare la curiosità del lettore che desidera sapere in anticipo qual è l'irrazionale α^* che sarà esibito nella dimostrazione; intuitivamente, è quello con "maggiore avversione" alla approssimazione con razionali, ed è $\alpha^* = (\sqrt{5}-1)/2 \approx 0.618034\ldots$, l'inverso della sezione aurea.[4]

DIMOSTRAZIONE. La dimostrazione consiste nel mostrare che, date *tre* successive convergenti di α, almeno una di queste soddisfa la (3.7). Usiamo la rappresentazione

$$\alpha = [a_0;\, a_1, a_2, \ldots, a_{n-1}, \xi_n]$$

e dalla (2.23), aumentando di 1 l'indice n, otteniamo

$$\left|\alpha - \frac{A_n}{B_n}\right| = \frac{1}{B_n\,(\xi_{n+1}B_n + B_{n-1})} = \frac{1}{B_n^2\,(\xi_{n+1} + \rho_{n+1})} \tag{3.9}$$

dove abbiamo posto $\rho_{n+1} = B_{n-1}/B_n$. Tutto quindi dipende dal confronto della somma $\xi_{n+1} + \rho_{n+1}$ con $\sqrt{5}$. Supporremo allora che sia

$$\xi_i + \rho_i \geq \sqrt{5} \tag{3.10}$$

per *tre* valori consecutivi $i = n-1, n, n+1$ dell'indice i, e proveremo che da questo segue un assurdo: questo dimostrerà il teorema.

Per la definizione di ρ_i e per le formule di Eulero:

$$\frac{1}{\rho_i} = \frac{B_{i-1}}{B_{i-2}} = \frac{a_{i-1}B_{i-2} + B_{i-3}}{B_{i-2}} = a_{i-1} + \rho_{i-1} \tag{3.11}$$

Dalla definizione delle ξ abbiamo $\xi_{n-1} = a_{n-1} + 1/\xi_n$. Eliminando a_{n-1} da questa e dalla (3.11) con $i = n$, otteniamo

$$\frac{1}{\rho_n} = \underbrace{\rho_{n-1} + \xi_{n-1} \leq \sqrt{5}}_{\text{per la (3.10) con } \boxed{i = n-1}} \quad \Rightarrow \frac{1}{\xi_n} \leq \sqrt{5} - \frac{1}{\rho_n}$$

Inoltre

$$\underbrace{\xi_n \leq \sqrt{5} - \rho_n}_{\text{per la (3.10) con } \boxed{i = n}}$$

[4] Per precisione, possono anche essere usati la stessa sezione aurea $(\sqrt{5}-1)/2 \approx 1.61803\ldots$, oppure gli irrazionali precisati nell'Esercizio 3.3.2 e nella nota successiva.

Per costruzione, $\xi_n > 0$, e quindi possiamo moltiplicare termine a termine le ultime due disuguaglianze:

$$1 \leq 6 - \sqrt{5}\left(\rho_n + \frac{1}{\rho_n}\right) \quad \Rightarrow \quad \rho_n + \frac{1}{\rho_n} \leq \sqrt{5}$$

L'ultima disuguaglianza scritta è in effetti stretta, poiché ρ_n è razionale; essendo anche, per definizione, $\rho_n > 0$, possiamo moltiplicare per ρ_n:

$$\rho_n^2 + 1 - \sqrt{5}\,\rho_n < 0 \Rightarrow \left(\frac{\sqrt{5}}{2} - \rho_n\right)^2 < \frac{1}{4}$$

La quantità nella $(\ldots)$ è positiva, in quanto $\sqrt{5}/2 = 1.118\ldots$, e, per la crescenza dei B_i, $\rho_n < 1$. Possiamo quindi estrarre la radice ottenendo:

$$\frac{\sqrt{5}}{2} - \rho_n < \frac{1}{2} \quad \Rightarrow \quad \rho_n > \frac{\sqrt{5}-1}{2} = 0.618\ldots$$

Per ipotesi però la (3.10) vale anche per $\boxed{i = n}$ e $\boxed{i = n+1}$: quindi allo stesso modo otteniamo che:

$$\rho_{n+1} > \frac{\sqrt{5}-1}{2} = 0.618034\ldots \quad \Rightarrow \quad \frac{1}{\rho_{n+1}} < \frac{\sqrt{5}+1}{2} = 1.61803\ldots$$

Utilizzando queste disuguaglianze alla (3.11) con $i = n+1$, otteniamo

$$a_n = \frac{1}{\rho_{n+1}} - \rho_n < \frac{\sqrt{5}+1}{2} - \frac{\sqrt{5}-1}{2} = 1$$

in contraddizione con l'assunzione di base che sia $a_n \geq 1$. La prima parte è dimostrata.

Poniamo $\alpha^* = (\sqrt{5}-1)/2$, e supponiamo che la (3.8) abbia soluzioni con q arbitrariamente grande. Riscrivendo la stessa (3.8) abbiamo:

$$\frac{\sqrt{5}-1}{2} = \frac{p}{q} + \frac{\delta}{q^2}$$

dove $|\delta| < \theta < 1/\sqrt{5}$, cioè, moltiplicando per q:

$$-\frac{\delta}{q} + \frac{\sqrt{5}}{2}\,q = \frac{q}{2} + p$$

ed elevando al quadrato ambo i membri, dopo una semplificazione ($\frac{1}{4}-\frac{5}{4}=-1$)

$$\frac{\delta^2}{q^2}-\delta\sqrt{5}=p^2+pq-q^2$$

Essendo che $-1<-\delta\sqrt{5}<1$, abbiamo che, per q sufficientemente grande:

$$-1<\frac{\delta^2}{q^2}-\delta\sqrt{5}<1$$

e quindi $p^2+pq-q^2=0$. Questo implica $(2p+q)^2=5q^2$, che, per l'irrazionalità di $\sqrt{5}$ è impossibile. ■

Esercizio 3.3.2 Provare che un altro controesempio per il Teorema 3.3.1 di Hurwitz–Borel è il numero $\alpha^*=(3+\sqrt{5})/2$.

SOLUZIONE. Procedendo esattamente come nella dimostrazione del Teorema 3.3.1, si giunge all'uguaglianza

$$\frac{\delta^2}{q^2}-\delta\sqrt{5}=p^2-3pq+q^2$$

Si conclude poi che $p^2-3pq+q^2=0$, e da questo viene l'assurdo $(2p-3q)^2=5q^2$. ■

È possibile dimostrare (Coppel, 2009, Proposition 6, pp. 188–190) che è possibile scegliere come controesempio α^* nel Teorema 3.3.1 un qualunque numero del tipo $\alpha^*=[a_0,\ldots,a_m,\{1\}]$, cioè tale che sia definitivamente $a_k=1$. L'inverso della sezione aurea $\alpha^*=(-1+\sqrt{5})/2=[\{1\}]$ è la scelta più semplice. Nell'esercizio precedente abbiamo scelto $\alpha^*=(3+\sqrt{5})/2=[2,\{1\}]$. Si può ancora dimostrare (Coppel, 2009) che:

Teorema 3.3.3 *Se $\alpha=[a_0,a_1,\ldots]$ è un irrazionale tale che non sia definitivamente $a_k=1$, allora esistono infiniti razionali p/q tali che*

$$\left|\alpha-\frac{p}{q}\right|<\frac{1/\sqrt{8}}{q^2} \tag{3.12}$$

Fissato un $0<\theta<1/\sqrt{8}$, per ogni numero reale $\alpha^*=[a_0,\ldots,a_m,\{2\}]$ (come ad esempio $1+\sqrt{2}=[\{2\}]$) la disuguaglianza

$$\left|\alpha^*-\frac{p}{q}\right|<\frac{\theta}{q^2} \tag{3.13}$$

ha solo un numero finito di soluzioni razionali p/q.

Sono possibili ulteriori generalizzazioni. Questo mostra che fra tutti gli irrazionali, quelli "più malamente" approssimabili con razionali, ovvero quelli "meno irrazionali", sono gli $\alpha^* = [a_0, \ldots, a_m, \{1\}]$, connessi con la $\sqrt{5}$, fra i quali il "meno irrazionale" di tutti è l'inverso della sezione aurea $\phi^{-1} = [\{1\}]$. Seguono gli $\alpha^* = [a_0, \ldots, a_m, \{2\}]$, connessi con la $\sqrt{2}$. Ne viene la curiosa coincidenza che, come affermano taluni storici, il primo irrazionale "scoperto" fu proprio $\sqrt{5}$ e successivamente proprio $\sqrt{2}$.

3.4 Cenni al Teorema di Roth

I risultati pionieristici di Liouville del 1844 (Teorema 3.5 e Corollario 3.2.2) sono stati perfezionati nei cento anni successivi con lo scopo fondamentale di diminuire l'esponente λ (che nei risultati di Liouville è pari al grado n del numero algebrico irrazionale α in esame). In questo filone di ricerca vanno ricordati i risultati del matematico norvegese Axel Thue (1863–1922), che dimostrò che si può assumere $\lambda = \frac{1}{2}n+1+\epsilon$, del matematico tedesco Carl Ludwig Siegel (1896–1981), molto noto anche come grande specialista di meccanica celeste, che ridusse λ al valore $2\sqrt{n} + \epsilon$, ed infine il contributo conclusivo del britannico Klaus Friedrich Roth (1925–), che svincolò il valore di λ dal grado di α, dimostrando che vale la stima ottimale $\lambda = 2 + \epsilon$ (Roth, 1955). Per questo risultato Roth vinse la Medaglia Fields nel 1958, assieme a René Thom. Enunciamo espressamente il teorema di Roth.

Teorema 3.4.1 (Teorema di Roth, 1955) *Sia α è un numero **algebrico** di grado ≥ 2 (cioè un algebrico irrazionale) e sia $\epsilon > 0$. Allora esiste una costante $c(\alpha, \epsilon)$ tale che per ogni razionale p/q (p, q interi, $q > 0$)*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha, \epsilon)}{q^{2+\epsilon}} \tag{3.14}$$

*Tuttavia la costante $c(\alpha, \epsilon)$ **non** è esplicitamente calcolabile (in funzione del numero α).*

Il Teorema di Roth è *equivalente* al seguente

Teorema 3.4.2 *Sia α è un numero **algebrico** di grado ≥ 2 (cioè un algebrico irrazionale) e sia $\epsilon > 0$. Allora esiste solo un numero **finito** di frazioni irriducibili p/q tali che:*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}} \tag{3.15}$$

Dimostrazione.

Parte 1: *Teorema di Roth* $\Rightarrow$ *Teorema* 3.4.2

Supponiamo che, dati α ed ϵ, la disuguaglianza (3.15) valga per infiniti valori del denominatore q. Applicando il Teorema di Roth, ma con $0 < \epsilon' < \epsilon$, avremmo una costante $c(\alpha, \epsilon')$ tale che per tutti i $p, q > 0$ valga la (3.14) con ϵ' al posto di ϵ, e quindi per infiniti q avremmo

$$\frac{c(\alpha, \epsilon')}{q^{2+\epsilon'}} < \frac{1}{q^{2+\epsilon}} \tag{3.16}$$

che è impossibile in quanto il grafico di $1/x^{2+\epsilon}$ va sotto quello di $c(\alpha, \epsilon')/x^{2+\epsilon'}$ da un certo punto in poi, e quindi solo un numero finito di interi q può soddisfare la (3.16). ■

Parte 2: *Teorema* 3.4.2 $\Rightarrow$ *Teorema di Roth*

Sia

$$D = \{q_1, q_2, \ldots, q_N\}$$

l'insieme finito di tutti i denominatori q di tutte le frazioni irriducibili p/q che verificano la (3.15). Allora per ogni intero $q \notin D$ e quale che sia l'intero p, primo con q, non vale la (3.15), ossia si ha

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{q^{2+\epsilon}} \tag{3.17}$$

Esaminiamo ora i denominatori $q_k \in D$, in numero finito, $1 \leq k \leq N$: fissiamo uno di questi, ad esempio q_1, e consideriamo tutti i razionali p/q_1 al variare di $p \in \mathbb{Z}$. Fra questi ne esiste uno a distanza minima da α, ad esempio sia:

$$\left|\alpha - \frac{p_1}{q_1}\right| = \min\left\{\left|\alpha - \frac{p}{q_1}\right| : p \in \mathbb{Z}\right\}$$

Quindi per $q = q_1 \in D$ e quale che sia l'intero p, primo con q, si ha

$$\left|\alpha - \frac{p}{q_1}\right| \geq \left|\alpha - \frac{p_1}{q_1}\right| = \frac{c_1}{q_1^{2+\epsilon}} \tag{3.18}$$

dove c_1 è definita da

$$c_1 := q_1^{2+\epsilon}\left|\alpha - \frac{p_1}{q_1}\right|$$

si ha $c_1 \neq 0$ *poiché* α *è irrazionale*, ed evidentemente c_1 è una costante che dipende solo da α e da ϵ. Quindi per ogni $q \in D$ e quale che sia l'intero p, primo con q, si ha

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{\min\{c_1, c_2, \ldots, c_N\}}{q^{2+\epsilon}} \tag{3.19}$$

Le (3.17) per $q \notin D$ e la (3.19) per $q \in D$ mostrano che, ponendo

$$c(\alpha, \epsilon) = \min\{1, c_1, c_2, \ldots, c_N\}$$

si ottiene la (3.14). ■

Esempio 3.4.3 *Siano n, m interi, con $n > 0$, $m > 0$, e sia $\alpha := \sqrt[3]{n}$* ***irrazionale****. Allora l'equazione diofantea*

$$x^3 - ny^3 = m$$

ha solo un numero finito di soluzioni intere x, y.

DIMOSTRAZIONE. Siano x, y soluzioni intere. Se $x = 0$ esiste al massimo un numero finito (eventualmente 0) di interi y tali che $-ny^3 = m$, e se $y = 0$ esiste al massimo un numero finito (eventualmente 0) di interi x tali che $x^3 = m$. Esaminiamo ora ciascun quadrante.

I e III quadrante. Siano $x > 0$, $y > 0$ oppure siano $x < 0$, $y < 0$. Dividendo l'equazione $x^3 - ny^3 = m$ per $|y|^3$ e prendendo i valori assoluti otteniamo

$$\left|(x/y)^3 - n\right| = \left|(x/y)^3 - \alpha^3\right| = m/|y|^3$$

Infatti, nel I quadrante $x^3/|y|^3 = (x/y)^3$ e $-ny^3/|y|^3 = -n$; nel III quadrante, $x^3/|y|^3 = -(x/y)^3$ e $-ny^3/|y|^3 = n$, ed evidentemente $\left|(x/y)^3 - n\right| = \left|-(x/y)^3 + n\right|$. Fattorizzando: $(x/y)^3 - \alpha^3 = (x/y - \alpha) \cdot ((x/y)^2 + \alpha(x/y) + \alpha^2)$, e visto che in ogni caso $\alpha > 0$, $x/y > 0$, $\alpha^2 > 0$, si ha

$$\left|(x/y)^3 - \alpha^3\right| = |x/y - \alpha| \cdot \left\{\left|\alpha(x/y) + \alpha^2\right| + \left|\alpha^2\right|\right\} > |x/y - \alpha| \cdot \alpha^2$$

Quindi $|x/y - \alpha| < m\alpha^{-2}/|y|^3$. Se le soluzioni (x, y) fossero infinite, ve ne sarebbero infinite in almeno uno dei due quadranti in esame, e quindi l'algebrico irrazionale $\alpha > 0$ sarebbe approssimabile di ordine 3: con razionali x/y se vi sono infinite soluzioni intere x, y di $x^3 - ny^3 = m$ nel I quadrante e/o con razionali $-x/|y|$ se vi sono infinite soluzioni nel III quadrante, in ogni caso contro il Teorema di Roth nella forma 3.4.2.

II quadrante. Sia $x < 0$, $y > 0$. Quindi $x^3 - ny^3 < 0$, mentre $m > 0$. Quindi in questo quadrante non ci sono soluzioni intere.

IV quadrante. Sia $x > 0$, $y < 0$. Quindi, se tali x, y sono soluzioni, sia ha $x^3 - ny^3 = |x|^3 - n(-|y|)^3 = |x|^3 + n|y|^3 = m$. Quindi contemporaneamente si ha $|x|^3 < m$ e $|y|^3 < m/n$, disuguaglianze che possono essere soddisfatte solo da un numero finito di interi x, y.

La Figura 3.1 rappresenta la cubica $x^3 - 5y^3 = 2048$, alla quale, in base a quanto ora dimostrato, appartengono solo un numero finito di punti (x, y) con coordinate intere. ■

Esempio numerico 3.4.4 Verificare numericamente che i due punti $(-8,-8)$ e $(12,-4)$ sono le uniche soluzioni intere dell'equazione diofantea $x^3 - 5y^3 = 2048$ tali che $\max\{|x|\,,\,|y|\} \leq 10^6$.

SOLUZIONE. Si tabulino su un computer la lista $2048+5y^3$ e la lista x^3 per x, y interi, $-10^6 \leq x, y \leq 10^6$, e si ricerchi se hanno elementi in comune. Gli utenti *Mathematica* possono usare i comandi:

```
M = 10^6; x = y = Range[-M, M]; Intersection[x^3, 5 y^3 + 2048].
```

che danno come output `{-512, 1728}`; l'equazione $x^3 = -512$ ha la soluzione reale $x = -8$ e l'equazione $2048 + 5y^3 = -512$ ha la soluzione reale $y = -8$; invece l'equazione $x^3 = 1728$ ha la soluzione reale $x = 12$ e l'equazione $2048 + 5y^3 = 1728$ ha la soluzione reale $y = -4$. ■

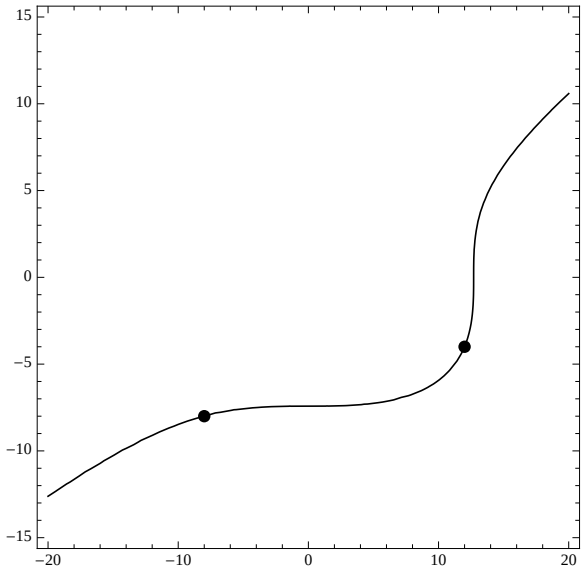
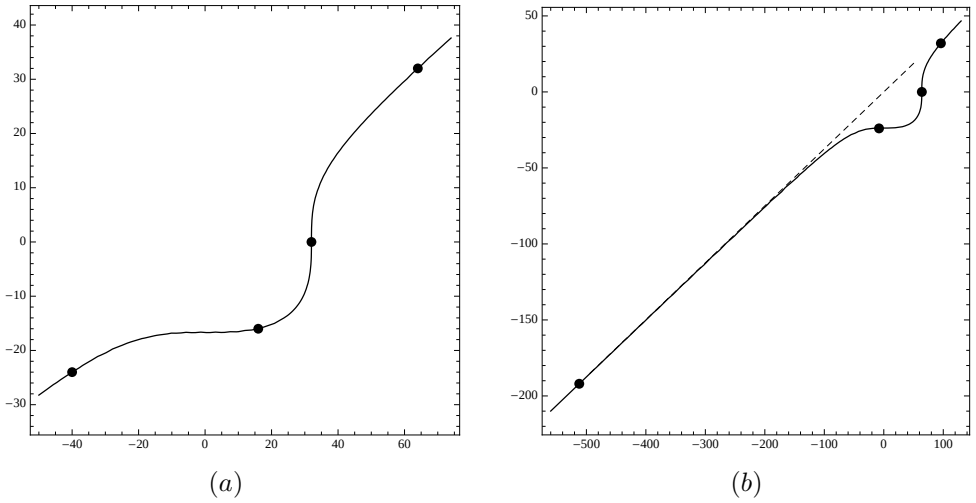


Figura 3.1: La cubica $x^3 - 5y^3 = 2048$. Il numero $\sqrt[3]{5}$ è un algebrico irrazionale, e pertanto sulla curva ci sono solo un numero finito di punti (x, y) con coordinate intere; i pallini evidenziano due di questi: $(-8,-8)$ e $(12,-4)$.

Esempio numerico 3.4.5 (a) Verificare numericamente che i quattro punti $(-40,-24)$, $(16,-16)$, $(32,0)$, e $(64,32)$ sono le uniche soluzioni intere dell'equazione diofantea $x^3-7y^3 = 32768$ tali che $\max\{|x|\,,\,|y|\} \leq 10^6$. (b) Verificare numericamente che i quattro punti $(-512,-192)$, $(-8,-24)$, $(64,0)$, $(96,32)$ sono le uniche soluzioni intere dell'equazione diofantea $x^3-19y^3 = 262144$ tali

che $\max\{|x|\,,\,|y|\} \leq 10^6$. Si veda la Figura 3.2: si osservi "sperimentalmente" nel caso (b) la possibilità dell'esistenza di soluzioni "lontane" dall'origine, nella "zona" dove la curva si confonde graficamente con l'asintoto (obliquo), che ha equazione $y = (1/\sqrt[3]{19})\,x$.



(a) (b)

Figura 3.2: (a) La cubica $x^3 - 7y^3 = 32768$; i pallini evidenziano quattro punti con coordinate intere sulla curva: $(-40, -24)$, $(16, -16)$, $(32, 0)$, e $(64, 32)$. (b) La cubica $x^3 - 19y^3 = 262144$; i pallini evidenziano quattro punti con coordinate intere sulla curva: $(-512, -192)$, $(-8, -24)$, $(64, 0)$, $(96, 32)$; la linea tratteggiata rappresenta l'asintoto obliquo, che ha equazione $y = (1/\sqrt[3]{19})\,x$.

Capitolo 4

Da Hermite a Lindemann

4.1 Premesse

I due numeri reali e e π appaiono numeri "centrali" fin dalla matematica di base, come coefficienti di normalizzazione. Infatti, il numero di Nepero e è l'unica base a per la funzione esponenziale reale $x \mapsto a^x$ per la quale il coefficiente k di proporzionalità nella formula $\frac{d}{dx}a^x = k \cdot a^x$ è pari a $k = 1$. Analogamente, π è la misura che si deve attribuire all'angolo piatto in modo che il coefficiente k nella formula $\frac{d}{dx}\sin(x) = k \cdot \cos(x)$ valga $k = 1$. I due numeri sono legati fra loro dall'uguaglianza $e^{i\pi} = -1$, che, come vedremo nel seguito, ha un'importanza fondamentale in questo capitolo, e sono entrambi numeri *trascendenti*. La trascendenza di e fu provata da Charles Hermite (1873), e la trascendenza di π da Ferdinand von Lindemann (1882) nove anni dopo, seguendo, come lui stesso riconosce, l'idea utilizzata da Hermite, e che in seguito chiameremo "metodo di Hermite". Il risultato di Lindemann, definito da Enrico Bombieri "un trionfo della matematica moderna" (Bombieri, 2006), rappresenta la soluzione definitiva, in termini negativi, di uno dei tre problemi classici della matematica ellenica: la quadratura del cerchio. Presenteremo queste problematiche in modo dettagliato nell'Appendice B. Chi desidera una trattazione ampia e sistematica della teoria dei numeri trascendenti può consultare il classico testo di Alan Baker (1975); una trattazione più specializzata, che comprende in particolare i contributi della scuola sovietica successivi agli anni '50, si trova in Shidlovskii (1989).[1]

Il metodo di Hermite appare più chiaro se il percorso che porta dalla trascendenza di e a quella di π viene fatto precedere da risultati di irrazionalità per e e π, nella forma più generale in cui si dimostra, seguendo Niven (1967)

[1] In inglese; la versione originale in russo è del 1987.

l'irrazionalità di e^r e $\cos(r)$ per r razionale non nullo; per l'analisi di alcuni semplici esempi di queste affermazioni si veda Niven (1961).

4.2 Se $r \neq 0$ è razionale, e^r è irrazionale

Applicheremo ora il metodo di Hermite per provare che e^r è irrazionale per ogni r razionale non nullo. Ai fini didattici abbiamo incluso nell'Appendice A vari approcci alla definizione del numero di Nepero, della funzione esponenziale e delle funzioni coseno e seno. La "definizione" forse più popolare di e, cioè quella basata sul cosiddetto "limite notevole"

$$\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = e,$$

non è quella che serve per dimostrare l'irrazionalità e successivamente la trascendenza di e.

Quello che serve invece è che la formula di integrazione per parti

$$\int_0^t u(x)v'(x)\,dx = [u(x)v(x)]_0^t - \int_0^t u'(x)v(x)\,dx \tag{4.1}$$

applicata alla funzione $v(x) = e^x$ si "semplifica" viste le proprietà della funzione esponenziale in base e

$$\frac{d}{dx}\,e^x = e^x, \quad e^0 = 1.$$

Il metodo di Hermite procede per assurdo: supponendo che $\alpha = e^r$ sia razionale, quando r è un razionale non nullo, si costruisce un numero *intero* M tale che $0 < M < 1$, un evidente assurdo. Osserviamo che mentre è abbastanza banale dimostrare che per ogni intero positivo b risulta che $e^{1/b}$ è irrazionale (si veda l'Appendice), non è così immediato dimostrare il seguente

Teorema 4.2.1 *Se $r \neq 0$ è razionale, e^r è irrazionale.*

Dimostrazione. Dato che $e^{-r} = 1/e^r$, possiamo assumere che r sia un razionale *positivo*. Inoltre, osserviamo che basta dimostrare che per ogni $a \in \mathbb{N}$, $a \neq 0$, e^a è irrazionale. Infatti, una volta dimostrato questo risultato, se per qualche razionale $r = a/b \neq 0$ (a, $b \in \mathbb{N}$, $b \neq 0$) risultasse che $e^{a/b}$ è uguale ad un razionale M/N, si giungerebbe, elevando all'esponente intero b, all'assurdo

$$e^a = \left(\frac{M}{N}\right)^b.$$

Supponiamo dunque che $r \in \mathbb{N}$, $r \neq 0$. Come abbiamo già premesso, il metodo di Hermite per provare l'irrazionalità di e^r prende spunto dalla formula di integrazione per parti del prodotto $f(x)e^x$, fra 0 ed r, dove $f(x)$ è una funzione "generica":

$$\begin{aligned}\int_0^r f(x)e^x\,dx &= [f(x)e^x]_0^r - \int_0^r f'(x)e^x\,dx \\ &= \{f(r)e^r - f(0)\} - \int_0^r f'(x)e^x\,dx\end{aligned}$$

Assumendo l'opportuna regolarità, possiamo continuare integrando per parti $-\int_0^r f'(x)e^x\,dx = -\{f'(r)e^r - f'(0)\} + \int_0^r f''(x)e^x\,dx$, ottenendo

$$\int_0^r f(x)e^x\,dx = (f(r) - f'(r))\,e^r \;-\; (f(0) - f'(0)) + \int_0^r f''(x)e^x\,dx$$

Iterando l'integrazione, otteniamo una formula del tipo:

$$\int_0^r f(x)e^x\,dx =$$
$$(f(r) - f'(r) + f''(r) - \ldots)\,e^r \;-\; (f(0) - f'(0) + f''(0) - \ldots) \pm \int_0^r (\ldots)\,dx$$

in cui la funzione integranda $(\ldots)$ è il prodotto di e^x con una derivata di ordine "alto" di $f(x)$. Se assumiamo che $f(x)$ sia un *polinomio*, pur di derivarlo abbastanza volte, la sua derivata è 0 e quindi $\int_0^r (\ldots)\,dx$ "scompare" dalla formula precedente. Supponiamo quindi che $f(x)$ sia un polinomio di grado "alto" da determinare, e poniamo:

$$F(x) = f(x) - f'(x) + f''(x) - f'''(x) + \ldots$$

dove la somma si arresta non appena si incontra una derivata successiva di $f(x)$ uguale a 0, e pertanto

$$\int_0^r f(x)e^x\,dx = F(r)\,e^r \;-\; F(0)$$

Per effettuare la valutazione di $F(0)$ ed $F(r)$ in modo semplice, conviene che siano "poche" quelle derivate di $f(x)$ che sono $\neq 0$ in 0 e r. Ciò si può realizzare scegliendo

$$f(x) = \frac{1}{n!}\,x^n(r-x)^n \tag{4.2}$$

con l'intero n da determinare. Il grafico di f quando $r = 1$ e $n = 10$ è rappresentato nella Figura 4.1. Notiamo che il grado di f è $2n$, e quindi per

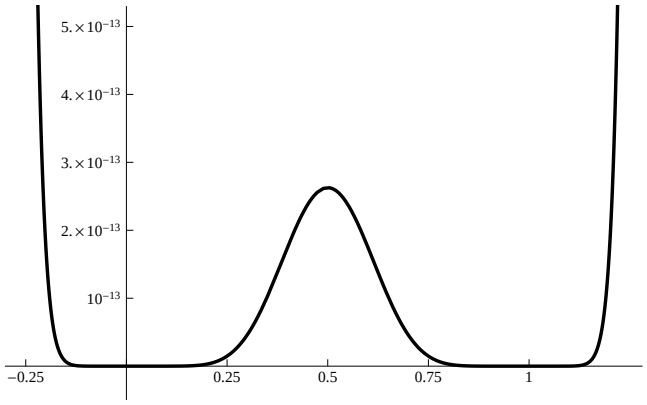


Figura 4.1: Grafico di $\frac{1}{10!}\,x^{10}(1-x)^{10}$. Si noti la simmetria rispetto all'asse $x = 1/2$ e la "piattezza" in $x = 0$ e $x = 1$. Il valore approssimato del massimo relativo in $x = 1/2$ è $f(1/2) \approx 2.62807 \times 10^{-13}$.

$j > 2n$ le derivate $f^{(j)}(0)$ sono tutte nulle. Ricordiamo inoltre che per un polinomio generico di grado m

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$$

si ha:

$$a_0 = f(0), \quad a_1 = f'(0), \quad a_2 = \frac{f''(0)}{2!}, \quad \ldots, \quad a_m = \frac{f^{(m)}(0)}{m!},$$

e quindi, in generale per $0 \le j \le m$:

$$f^{(j)}(0) = j! \times \{\text{coefficiente di } x^j\}$$

Essendo nel nostro caso $m = 2n$, per lo sviluppo del binomio $(r - x)^n$:

$$f(x) = \frac{1}{n!}\, x^n \left\{ \sum_{k=0}^{n} \binom{n}{k} r^{n-k} (-x)^k \right\} \tag{4.3}$$

Otteniamo così le derivate

$$f^{(j)}(0) = \begin{cases} 0 & \text{per } 0 \le j < n \\ j! \cdot \dfrac{1}{n!}\, r^n = r^n & \text{per } j = n + k, \text{ con } k = 0 \\ j! \cdot \dfrac{1}{n!} \binom{n}{k} r^{n-k} (-1)^k & \text{per } j = n + k, \text{ con } 1 \le k \le n \\ 0 & \text{per } j > 2n \end{cases}$$

che sono tutte dei numeri interi. Infatti, il termine di grado più basso rispetto a x di f ha grado n e quindi le derivate $f^{(j)}(0)$ sono tutte nulle per $0 \le j < n$, ed ovviamente $f^{(j)}(0) = 0$ quando j supera il grado del polinomio; mentre per $n \le j \le 2n$, posto $j = n + k$ con $0 \le k \le n$, il coefficiente di x^j si ottiene considerando nella sommatoria il termine di indice k. La Tabella 4.1 tabula i valori delle derivate $f^{(j)}(0)$ per $0 \le j \le 26$ per la $f(x) = (1/10!)\, x^{10}(1-x)^{10}$ della Figura 4.1.

Quando le derivate $f^{(j)}(0)$ non sono uguali a 0, sono comunque numeri interi, e quindi $F(0)$ è un intero.

La simmetria di f rispetto all'asse $x = r/2$ significa che $f(x) = f(r-x)$, e quindi

$$f^{(j)}(r) = (-1)^j\, f^{(j)}(0)$$

Pertanto anche $F(r)$ è intero.

Supponiamo ora per assurdo che sia $e^r = p/q$, p, q interi, $q > 0$. Abbiamo

$$q \int_0^r f(x) e^x\, dx = pF(r) - qF(0)$$

Ora, dato che la funzione integranda è positiva su $(0, r)$, si ha che $\int_0^r f(x)e^x\, dx > 0$ e quindi l'intero

$$M := pF(r) - qF(0) \ge 1$$

D'altra parte la $f(x)$ ha massimo in $r/2$ pari a $2^{-2n} r^{2n}/n!$. Quindi

$$0 < M = q \int_0^r f(x) e^x\, dx \le \frac{1}{n!} qr \cdot 2^{-2n} r^{2n} \cdot e^r \le \frac{1}{n!} qr \cdot r^{2n} \cdot \frac{p}{q} = \frac{1}{n!} p r^{2n+1} \to 0$$

per $n \to \infty$ (per le proprietà asintotiche della successione $A^n/n!$ per $A > 0$). Quindi per n abbastanza grande abbiamo l'assurdo che M è intero e

$$0 < M < 1$$

Si osservi che l'ipotesi essenziale $r \neq 0$ è utilizzata nella dimostrazione nel punto in cui si afferma che $\int_0^r f(x)e^x\, dx > 0$. ■

4.3 π^2 è irrazionale

Storicamente, l'irrazionalità di π venne dimostrata per primo da J.H. Lambert nel 1761, utilizzando sviluppi in frazione continua. Nel 1794, Legendre, negli *Éleménts de Géométrie*, utilizzò ancora il metodo delle frazioni continue per provare l'irrazionalità di π^2. Il metodo di Hermite venne poi applicato da

j	$f^{(j)}(0)$	$n = 10$
0	0	per $0 \le j < n$
1	0	
2	0	
3	0	
4	0	
5	0	
6	0	
7	0	
8	0	
9	0	
10	1	per $j = n$
11	-110	per $n < j \le 2n$
12	5 940	
13	$-205\,920$	
14	5 045 040	
15	$-90\,810\,720$	
16	1 210 809 600	
17	$-11\,762\,150\,400$	
18	79 394 515 200	
19	$-335\,221\,286\,400$	
20	670 442 572 800	
21	0	per $j > 2n$
22	0	
23	0	
24	0	
25	0	
26	0	

Tabella 4.1: Valori di $f^{(j)}(0)$ per $0 \le j \le 26$ per $f(x) = \frac{1}{10!}\, x^{10}(1-x)^{10}$. In questo caso $F(0) = 1\,098\,127\,402\,131$.

I. Niven per provare l'irrazionalità di π in una famosa dimostrazione di una sola pagina (Niven, 1947), che venne estesa da Y. Iwamoto (1949) per dimostrare l'irrazionalità di π^2. Qui presentiamo quest'ultima dimostrazione seguendo Niven (1967).

Teorema 4.3.1 *π^2 è irrazionale.*

DIMOSTRAZIONE. Supponiamo per assurdo $\pi^2 = a/b$ con a, b interi positivi. Definiamo la funzione

$$\begin{aligned} f(x) &= \frac{x^n(1-x)^n}{n!} = \frac{x^n}{n!} \cdot \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^k \\ &= \frac{1}{n!} \cdot \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^{n+k} \\ &= \frac{1}{n!} \cdot \left\{ x^n - n x^{n+1} + \binom{n}{2} x^{n+2} + \ldots + (-1)^{n-1} n x^{2n-1} + (-1)^n x^{2n} \right\} \end{aligned}$$

dove n è un intero positivo "grande" da definire in seguito. Questa differisce dalla funzione f data in (4.2) usata nella dimostrazione del Teorema 4.2.1 solo per il fatto che si è posto $r = 1$.

Quindi sappiamo già che le derivate $f^{(j)}(0)$ sono tutte dei numeri interi e poiché per $0 < x < 1$ si ha $0 < 1 - x < 1$ e quindi anche

$$0 < f(x) < \frac{1}{n!}$$

Ricordiamo che f è un polinomio di grado $2n$, per cui le sue derivate di ordine $> 2n$ sono $= 0$. Usiamo ora le derivate di ordine **pari** dalla 0−esima alla $2n$−esima per definire

$$\begin{aligned} F(x) &= b^n \sum_{k=0}^{n} (-1)^k \pi^{2n-2k} f^{(2k)}(x) \\ &= b^n \left\{ \pi^{2n} f(x) - \pi^{2n-2} f''(x) + \pi^{2n-4} f^{\mathrm{IV}}(x) - \ldots \right. \\ &\quad \left. + (-1)^{n-1} \pi^2 f^{(2n-2)}(x) + (-1)^n f^{(2n)}(x) \right\} \end{aligned}$$

Allora:

$$\begin{aligned} \pi^2 F(x) &= b^n \sum_{k=0}^{n} (-1)^k \pi^{2n-2k+2} f^{(2k)}(x) \\ &= b^n \left\{ \pi^{2n+2} f(x) - \pi^{2n} f''(x) + \pi^{2n-2} f^{\mathrm{IV}}(x) - \ldots \right. \\ &\quad \left. + (-1)^{n-1} \pi^4 f^{(2n-2)}(x) + (-1)^n \pi^2 f^{(2n)}(x) \right\} \end{aligned}$$

$$\begin{aligned} F''(x) &= b^n \sum_{k=0}^{n} (-1)^k \pi^{2n-2k} f^{(2k+2)}(x) \\ &= b^n \Big\{ \pi^{2n} f''(x) - \pi^{2n-2} f^{\mathrm{IV}}(x) + \pi^{2n-4} f^{(6)}(x) - \dots \\ &\quad + (-1)^{n-1} \pi^2 f^{(2n)}(x) + (-1)^n f^{(2n+2)}(x) \Big\} \end{aligned}$$

Quindi: $\pi^2 F(x) + F''(x)$

$$= b^n \left\{ \sum_{k=0}^{n} (-1)^k \pi^{2n-2k+2} f^{(2k)}(x) + \sum_{k=0}^{n} (-1)^k \pi^{2n-2k} f^{(2k+2)}(x) \right\}$$

$$= b^n \left\{ \underbrace{\pi^{2n+2} f(x)}_{k=0} + \sum_{k=1}^{n} (-1)^k \pi^{2n-2k+2} f^{(2k)}(x) + \sum_{k=0}^{n-1} (-1)^k \pi^{2n-2k} f^{(2k+2)}(x) \right\}$$

$$= b^n \left\{ \underbrace{\pi^{2n+2} f(x)}_{k=0} + \sum_{k=1}^{n} (-1)^k \pi^{2n-2k+2} f^{(2k)}(x) + \sum_{h=1}^{n} (-1)^{h-1} \pi^{\overbrace{2n-2(h-1)}^{=2n-2h+2}} f^{\overbrace{(2(h-1)+2)}^{=(2h)}}(x) \right\}$$

$$= b^n \pi^{2n+2} f(x)$$

avendo posto $h = k+1$, $k = h-1$. Quindi:

$$\begin{aligned} \frac{d}{dx}\{F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\} &= \{F''(x) + \pi^2 F(x)\}\sin(\pi x) \\ &= b^n \pi^{2n+2} f(x)\sin(\pi x) \\ &= \pi^2 a^n f(x)\sin(\pi x) \end{aligned}$$

$$\pi a^n \int_0^1 f(x)\sin(\pi x)dx = \left[\frac{F'(x)\sin(\pi x)}{\pi} - F(x)\cos(\pi x)\right]_0^1 = F(1) + F(0)$$

Ora sappiamo che tutte le derivate $f^{(j)}(0)$ sono interi, ed essendo $f(x) = f(1-x)$ abbiamo anche che tutte le derivate $f^{(j)}(1)$ sono interi (pari a $f^{(j)}(0)$ se j pari, a $-f^{(j)}(0)$ se j dispari). Pertanto $F(0)$ ed $F(1)$ sono interi, e la somma $F(0) + F(1)$ è un intero, *positivo, perché l'integrale è positivo.* Però

$$0 < \pi a^n \int_0^1 f(x)\sin(\pi x)dx < \frac{\pi a^n}{n!} \to 0$$

per $n \to \infty$ (per il comportamento asintotico di $A^n/n!$), assurdo. ■

Corollario 4.3.2 *π è irrazionale.*

Osservazione 4.3.3 Notiamo che il punto della dimostrazione in cui si utilizza il fatto che il simbolo π rappresenta "pi greco" (e non un altro numero) è nella integrazione per parti

$$\ldots = \left[\frac{F'(x)\sin(\pi x)}{\pi} - F(x)\cos(\pi x)\right]_0^1 = F(1) + F(0)$$

che è il punto esatto in cui si sfrutta il fatto che il numero π è caratterizzato dalle condizioni:

$$\begin{cases} \cos(\pi) &= -1 \\ \sin(\pi) &= 0 \end{cases}$$

In altri termini, il teorema potrebbe essere enunciato nella forma: *Se* $u \in \mathbb{R}$ *verifica* $\cos(u) = -1$ *e* $\sin(u) = 0$*, allora* u^2*, e quindi* u*, è irrazionale.*

4.4 Se $r \neq 0$ è razionale, $\cos(r)$ è irrazionale

Il metodo di Hermite viene anche utilizzato per provare l'irrazionalità dei valori delle funzioni trigonometriche per valori razionali $\neq 0$ della variabile.

Teorema 4.4.1 *Se* $f \in \{\cos, \sin, \tan\}$ *e se* $r \neq 0$ *è razionale, allora* $f(r)$ *è irrazionale.*

Notiamo che basta provare che:

Teorema 4.4.2 *Se* $r \neq 0$ *è razionale, allora* $\cos(r)$ *è irrazionale.*

Infatti, dalle formule

$$\cos(2r) = 1 - 2\sin^2 r = \frac{1 - \tan^2 r}{1 + \tan^2 r}$$

si deduce l'irrazionalità di $\sin(r)$ e $\tan(r)$ per $r \neq 0$.

Premettiamo alla dimostrazione due lemmi:

Lemma 4.4.3 *Sia dato un polinomio del tipo:*

$$h(x) = x^n g(x)/n! = (c_n/n!)x^n + (c_{n+1}/n!)x^{n+1} + (c_{n+2}/n!)x^{n+2} + \ldots$$

dove $g(x) = c_n + c_{n+1}x + c_{n+2}x^2 + \ldots$ *è un polinomio a coefficienti interi. Per* $j \geq 0$*:*

$$h^{(j)}(0) = \begin{cases} 0 & \text{se } j < n \\ n!\,(c_n/n!) = c_n = g(0) & \text{se } j = n \\ j!\,(c_j\,/n!) & \text{se } j > n \end{cases}$$

Allora $h^{(j)}(0)$ è sempre divisibile per $n+1$ per ogni $j \neq n$, ed è divisibile per $n+1$ quando $j = n$ se si ha $g(0) = 0$.

Lemma 4.4.4 *Se f è un polinomio in $(x-r)^2$, allora tutte le derivate di ordine j **dispari** si annullano in r, cioè $f^{(j)}(r) = 0$.*

Dimostrazione. Infatti, per ipotesi, $f(x) = p((x-r)^2)$ con p un polinomio. Posto $x-r = z$, la funzione $q(z) = f(z+r) = p(z^2)$ è pari, quindi q' è dispari, q'' è pari, ecc., per cui se j è dispari la derivata $j-$esima $q^{(j)}$ è dispari, e quindi vale 0 in 0. Tornando alla variabile x si ha per j dispari che $0 = q^{(j)}(0) = f^{(j)}(r)$. ■

Dato che $\cos(-r) = \cos(r)$, possiamo assumere che r sia un razionale *positivo*: poniamo $r = a/b$ con $a > 0, b > 0$ interi. Definiamo:

$$\begin{aligned} f(x) &= \frac{x^{p-1}(a-bx)^{2p}(2a-bx)^{p-1}}{(p-1)!} \\ &= \frac{\left[x^{p-1}(\frac{a-bx}{b})^{2p}(\frac{2a-bx}{b})^{p-1}\right] b^{2p+(p-1)}}{(p-1)!} \\ &= \frac{\left[x^{p-1}(\frac{a}{b}-x)^{2p}(2\frac{a}{b}-x)^{p-1}\right] b^{3p-1}}{(p-1)!} \\ &= \frac{\left[x^{p-1}(r-x)^{2p}(2r-x)^{p-1}\right] b^{3p-1}}{(p-1)!} \\ &= \frac{\left[(r-x)^{2p}(2rx-x^2)^{p-1}\right] b^{3p-1}}{(p-1)!} \\ &= \frac{(r-x)^{2p}\{r^2-(r-x)^2\}^{p-1}b^{3p-1}}{(p-1)!} \end{aligned}$$

dove p è un primo "grande" da definire in seguito. Possiamo comunque assumere subito $p \geq 3$.

Per $0 < x < r$ si ha $0 < r - x < r$ e quindi

$$0 < f(x) < \frac{r^{2p}\{r^2\}^{p-1}b^{3p-1}}{(p-1)!} = \frac{r^{4p-2}b^{3p-1}}{(p-1)!}$$

Notiamo che f è un polinomio di grado $p-1+2p+p-1 = 4p-2$, per cui le sue derivate di ordine $> 4p-2$ sono $= 0$. Usiamo quelle non nulle di ordine **pari** per definire

$$F(x) = f(x) - f''(x) + f^{(iv)}(x) - f^{(vi)}(x) + \ldots - f^{(4p-2)}(x)$$

dove l'ultimo segno è "meno" perché, essendo p dispari, sia ha $(4p-2) = 2 \mod 4$. Allora:

$$\begin{aligned}\frac{d}{dx}\{F'(x)\sin(x) - F(x)\cos(x)\} &= \{F''(x) + F(x)\}\sin(x) \\ &= \{\underbrace{-f^{(4p)}(x)}_{=0} + f(x)\}\sin(x) = f(x)\sin(x)\end{aligned}$$

Quindi:

$$\int_0^r f(x)\sin(x)dx = F'(r)\sin(r) - F(r)\cos(r) - \{F'(0)\sin(0) - F(0)\cos(0)\}$$

Ora f e le sue derivate pari (ogni due derivazioni si scala di 2 il grado dei monomi) sono polinomi in $(r-x)^2$, quindi F è un polinomio in $(x-r)^2$, e per il Lemma 4.4.4 si ha $F'(r) = 0$. Quindi:

$$\int_0^r f(x)\sin(x)dx = -F(r)\cos(r) + F(0) \tag{4.4}$$

Calcoleremo ora i valori $F(0)$ ed $F(r)$, e proveremo che:

(i) $F(0)$ è un intero q ***non*** *divisibile* per p se si sceglie $p > \max\{3, a\}$.

(ii) $F(r)$ è un intero s *divisibile* per p.

Questi due punti sono sufficienti per dimostrare la tesi. Infatti, assumiamo per assurdo che sia $\cos(r) = d/k$ razionale ($d, k > 0$ interi). Nella (4.4) possiamo allora sostituire $\cos(r)$ con d/k; per la (i) possiamo sostituire $F(0)$ con un intero q; per la (ii) possiamo sostituire $F(r)$ con un multiplo intero $s = pm$ di p; moltiplicando infine termine a termine per k otteniamo:

$$k\int_0^r f(x)\sin(x)dx = -pmd + kq$$

Fissiamo ora $p > \max\{3, a, k\}$. Così p non divide k, e dato che p non divide q, abbiamo che p non divide il prodotto kq, mentre banalmente p divide pmd. Deve essere $kq \neq pmd$ e quindi

$$|-pmd + kq| \geq 1$$

Invece

$$\left|k\int_0^r f(x)\sin(x)dx\right| < kr\frac{r^{4p-2}b^{3p-1}}{(p-1)!} = kr^3b^2\frac{(r^4b^3)^{p-1}}{(p-1)!} \to 0$$

per $p \to \infty$ (per il comportamento asintotico di $A^n/n!$), il che è assurdo.

- Calcolo di $F(0)$.

Notiamo che $f(x)$ ha la forma della $h(x)$ del Lemma 4.4.3, con $n = p-1$. Quindi $f^{(j)}(0)$ è un intero divisibile per $n+1 = p$, con la sola eventuale eccezione del caso $j = n = p-1$. Per calcolo diretto, $f^{(p-1)}(0)$ è il termine noto in $(a-bx)^{2p}(2a-bx)^{p-1}$, ossia si ha

$$f^{(p-1)}(0) = a^{2p}(2a)^{p-1}$$

Scegliendo $p > \max\{3, a\}$ risulta che p è dispari e non compare nella fattorizzazione in primi di $a^{2p}(2a)^{p-1}$, e quindi $f^{(p-1)}(0)$ è un intero non divisibile per p. La derivata di ordine $p-1$ compare in quelle di ordine pari sommate per definire $F(x)$, che per $x = 0$ sono tutte interi divisibili per p tranne una, quella di ordine $p-1$ che è comunque un intero. Quindi $F(0)$ è un intero non divisibile per p.

- Calcolo di $F(r)$.

Notiamo che $f(r-x)$ ha la forma della $h(x)$ del Lemma 4.4.3, con $n = p-1$:

$$\begin{aligned} f(r-x) &= \frac{x^{2p}\{r^2-x^2\}^{p-1}\overbrace{b^{3p-1}}^{b^{2(p-1)+(p+1)}}}{(p-1)!} \\ &= \frac{x^{2p}\{a^2-b^2x^2\}^{p-1}b^{p+1}}{(p-1)!} \\ &= \frac{x^{p-1}\overbrace{x^{p+1}\{a^2-b^2x^2\}^{p-1}b^{p+1}}^{g(x)}}{(p-1)!} \end{aligned}$$

dove $g(x) = x^{p+1}\{a^2-b^2x^2\}^{p-1}b^{p+1}$ vale 0 in 0. Per cui non ci sono eccezioni e ogni $f^{(j)}(r)$ è un intero divisibile per p. Quindi $F(r)$ è un intero divisibile per p. ■

Osservazione 4.4.5 Notiamo che il Teorema precedente fornisce una ulteriore prova dell'irrazionalità di π, in quanto $\cos(\pi) = -1$ è razionale.

In effetti la strategia della dimostrazione dell'irrazionalità di π di Lambert è analoga: Lambert, e successivamente Legendre (Berggren, Borwein e Borwein,

1997), considerano uno sviluppo in frazione continua di $\tan(x)$:

$$\tan(x) = \cfrac{x}{1 - \cfrac{x^2}{3 - \cfrac{x^2}{5 - \cfrac{x^2}{7 - \ddots}}}}$$

e provano che se x è un razionale non nullo, la frazione è illimitata e quindi è convergente ad un numero irrazionale. Ne consegue l'irrazionalità di π, in quanto $\tan(\pi/4) = 1$ è razionale.

4.5 Il numero di Nepero *e* è trascendente

Vediamo ora il contributo fondamentale di C. Hermite (1873), che ha dato nome al metodo.

Teorema 4.5.1 (Hermite, 1873) *Il numero di Nepero e è trascendente.*

Dimostrazione. Supponiamo per assurdo che e sia un numero algebrico di grado $m \geq 1$, cioè che esistano degli interi a_k $(k = 0, \ldots, m)$ tali che

$$\sum_{k=0}^{m} a_k e^k = a_0 + a_1 e + a_2 e^2 + \ldots + a_m e^m = 0$$

Possiamo supporre senza perdere in generalità che sia $a_0 \neq 0$ (eventualmente si divide per una potenza di e). Definiamo

$$f(x) = \frac{x^{p-1}(x-1)^p(x-2)^p(x-3)^p \cdots (x-m)^p}{(p-1)!}$$

dove $p \geq 3$ è un numero primo da scegliere in seguito. Notiamo che f è un polinomio di grado $mp + p - 1$, per cui le sue derivate di ordine $> mp + p - 1$ sono tutte identicamente nulle. Usiamo tutte quelle di ordine $\leq mp + p - 1$ per definire

$$F(x) = f(x) + f'(x) + f''(x) + f'''(x) + f^{(iv)}(x) + \ldots + f^{(mp+p-1)}(x)$$

Per $0 < x < m$ si ha la maggiorazione:

$$|f(x)| < \frac{m^{p-1}\overbrace{m^p m^p \cdots m^p}^{m}}{(p-1)!} = \frac{m^{mp+p-1}}{(p-1)!},$$

e inoltre poiché

$$\frac{d}{dx}\{e^{-x}F(x)\} = e^{-x}\{F'(x) - F(x)\} = -e^{-x}f(x)$$

per $k = 0, \ldots, m$ si ha

$$a_k \int_0^k e^{-x} f(x)dx = a_k \left[-e^{-x}F(x)\right]_0^k = a_k F(0) - a_k e^{-k} F(k)$$

Moltiplicando per e^k e sommando sull'indice $k = 0, \ldots, m$ otteniamo:

$$\begin{aligned}
\sum_{k=0}^{m} a_k e^k \int_0^k e^{-x} f(x)dx &= F(0)\overbrace{\sum_{k=0}^{m} a_k e^k}^{=0} - \sum_{k=0}^{m} a_k F(k) \\
&= -\sum_{k=0}^{m} a_k F(k) \\
&= -\sum_{k=0}^{m} \sum_{j=0}^{mp+p-1} a_k f^{(j)}(k) \qquad (4.5)
\end{aligned}$$

- *Calcolo delle derivate* $f^{(j)}(0)$.

Notiamo che $f(x)$ ha la forma della $h(x)$ del Lemma 4.4.3 con $n = p - 1$. Infatti

$$f(x) = \frac{x^{p-1} \cdot \overbrace{(x-1)^p(x-2)^p(x-3)^p \cdots (x-m)^p}^{g(x)}}{(p-1)!}$$

Quindi la generica derivata $f^{(j)}(0)$ è un intero divisibile per $n + 1 = p$, con la sola eventuale eccezione del caso $j = n = p - 1$. Per calcolo diretto, $f^{(p-1)}(0)$ è il termine noto $g(0)$ del polinomio $g(x)$, ossia si ha

$$f^{(p-1)}(0) = g(0) = (-1)^p(-2)^p(-3)^p \cdots (-m)^p$$

Scegliamo ora $p > m$, per modo che p non compaia nella scomposizione in fattori primi di $2^p 3^p \ldots m^p$ e quindi $f^{(p-1)}(0)$ risulti essere un intero non divisibile per p.

- *Calcolo delle derivate* $f^{(j)}(1)$.

Le derivate $f^{(j)}(1) = \partial_x^j f(x)|_{x=1}$ coincidono con le derivate $\partial_x^j f(x+1)|_{x=0}$. Notiamo che $f(x + 1)$ ha la forma della $h(x)$ del Lemma 4.4.3 con $n = p - 1$,

e $g(0) = 0$. Infatti:

$$\begin{aligned} f(x+1) &= \frac{(x+1)^{p-1}x^p(x-1)^p(x-2)^p\cdots(x+1-m)^p}{(p-1)!} \\ &= \frac{x^{p-1}\cdot\overbrace{x\,(x+1)^{p-1}(x-1)^p(x-2)^p\cdots(x+1-m)^p}^{g(x)}}{(p-1)!} \end{aligned}$$

Quindi la generica derivata $f^{(j)}(1)$ è un intero che è sempre divisibile per $n+1=p$. Analogamente abbiamo che:

- *Calcolo delle derivate $f^{(j)}(k)$ per $k = 2, \ldots, m$.*

Le derivate $f^{(j)}(k) = \partial_x^j f(x)|_{x=k}$ coincidono con le derivate $\partial_x^j f(x+k)|_{x=0}$. Notiamo che $f(x+k)$ ha la forma della $h(x)$ del Lemma 4.4.3 con $n = p-1$, e $g(0) = 0$. Quindi la generica derivata $f^{(j)}(k)$ è un intero sempre divisibile per $n+1=p$. Pertanto, scegliendo $p > |a_0|$, la somma a destra nella uguaglianza (4.5) ha addendi interi, tutti multipli di p tranne l'addendo $-a_0 f^{(p-1)}(0)$. Se tale somma, che è un numero intero, fosse uguale a 0, avremmo la contraddizione che un multiplo di p è uguale a un numero che non è multiplo di p. Quindi tale somma è un numero intero $\neq 0$, in particolare con modulo ≥ 1.

D'altra parte, scegliendo $p \geq m+2$ si ha

$$m \cdot m^{mp+p-1} = m^{mp+p} \leq m^{mp+p+(p-m-2)} = m^{mp-m+2p-2} = (m^{m+2})^{p-1}$$

e quindi, se consideriamo l'integrale a sinistra nella uguaglianza (4.5), per $p \to \infty$ abbiamo che:

$$\begin{aligned} 1 \leq \left|\sum_{k=0}^{m} a_k e^k \int_0^k e^{-x} f(x)dx\right| &\leq \sum_{k=0}^{m} \left|a_k e^k \int_0^k e^{-x} f(x)dx\right| \\ &\leq \sum_{k=0}^{m} |a_k|\, e^k \cdot k \cdot 1 \cdot \frac{m^{mp+p-1}}{(p-1)!} \\ &\leq \left\{\sum_{k=0}^{m} |a_k|\right\} e^m \cdot m \cdot \frac{m^{mp+p-1}}{(p-1)!} \\ &\leq \left\{\sum_{k=0}^{m} |a_k|\right\} e^m \cdot \frac{(m^{m+2})^{p-1}}{(p-1)!} \to 0, \end{aligned}$$

una contraddizione che prova la trascendenza di e. ■

Esempio numerico 4.5.2 Illustriamo numericamente la dimostrazione del teorema di Hermite 4.5.1 supponendo per assurdo che in corrispondenza agli interi $a_0 = 17$, $a_1 = -28$, $a_2 = 8$ risulti $17 - 28\,e + 8\,e^2 = 0$. Notiamo che il polinomio $17 - 28\,x + 8\,x^2$ di grado $m = 2$ a coefficienti interi ha una radice $x = \frac{1}{4}\left(7 + \sqrt{15}\right) \approx 2.71825$, e che $17 - 28\,e + 8\,e^2 \approx 0.000557595$. In questo semplicissimo caso particolare possiamo assumere come numero primo p "sufficientemente grande" già $p = 3$. La definizione di $f(x)$ è allora:

$$f(x) = \frac{x^2\,(x-1)^3\,(x-2)^3}{2}$$

e si ha di conseguenza

$$F(x) = \frac{12544 + 12544x + 6272x^2 + 2088x^3 + 531x^4 + 93x^5 + 26x^6 - x^7 + x^8}{2}$$

L'identità della formula (4.5)

$$\sum_{k=0}^{m} a_k e^k \int_0^k e^{-x} f(x)dx = F(0)\sum_{k=0}^{m} a_k e^k - \sum_{k=0}^{m} a_k F(k) \tag{4.6}$$

può essere verificata direttamente. Conoscendo espicitamente $f(x)$, l'integrale a sinistra nella (4.6) può essere calcolato esattamente, e si ottiene:

$$\sum_{k=0}^{m} a_k e^k \int_0^k e^{-x} f(x)dx = 4\left(26655 - 43904\,e + 12544\,e^2\right) \approx -0.502767$$

Conoscendo esplitamente $F(x)$, possiamo calcolare $F(0) = 6272$, $F(1) = 17\,049$ ed $F(2) = 46\,344$, ed otteniamo i valori numerici dei due addendi nel membro di destra della (4.6):

$$\begin{cases} F(0)\displaystyle\sum_{k=0}^{m} a_k e^k &= 6272\left(17 - 28\,e + 8\,e^2\right) &\approx 3.49723 \\ -\displaystyle\sum_{k=0}^{m} a_k F(k) &= -(17 \times 6272 - 28 \times 17\,049 + 8 \times 46\,344) &= -4 \end{cases}$$

La (4.5) diventa quindi numericamente l'identità (vera!):

$$\underbrace{4\left(26655 - 43904\,e + 12544\,e^2\right)}_{\approx -0.502767} = \underbrace{6272\left(17 - 28\,e + 8\,e^2\right)}_{\approx 3.49723} - 4$$

Avendo però assunto, per assurdo che sia $17 - 28\,e + 8\,e^2 = 0$, questo porta alla contraddizione $-0.502767\ldots = -4$. ■

4.6 π è trascendente

4.6.1 Calcolo con riga e compasso

La riga ed il compasso sono i principali strumenti analogici di calcolo del passato.[2]

4.6.2 Numeri costruibili

Ricordiamo qui brevemente quali sono le regole euclidee ammesse nelle costruzioni geometriche "con riga e compasso". Per maggiori dettagli si veda l'Appendice B. Ricordiamo innanzitutto che la riga euclidea non è graduata e che il compasso euclideo non conserva le distanze tra un utilizzo ed il successivo.

- Dati due punti possiamo tracciare la retta che li congiunge.
- Dati due punti possiamo tracciare la circonferenza che ha centro in uno di essi e passa per il secondo.
- Date due rette possiamo trovare la loro intersezione.
- Data una retta e una circonferenza possiamo trovare le loro intersezioni.
- Date due circonferenze possiamo trovare le loro intersezioni.

Definizione 4.6.1 *Un* punto *è* costruibile *se è ottenibile a partire da un segmento unitario con un numero finito di passi euclidei. Un* numero reale *è* costruibile *se è ascissa di un punto costruibile. Poniamo*

$$\mathcal{C} = \{x \in \mathbb{R} \mid (x, 0) \text{ è costruibile}\}$$

Ricordiamo alcuni risultati sui punti costruibili:

1. il punto (a, b) è costruibile se e solo se $a, b \in \mathcal{C}$;
2. se x, y sono costruibili, allora sono costruibili $x + y$, xy, $y - x$ e se $x \neq 0$ è costruibile y/x (Teorema B.4.4);
3. se $x > 0$, allora è costruibile $\sqrt{x}$ (Teorema B.4.4).

[2] Citiamo come esempio Galileo, che premette un capitolo sulle costruzioni con riga e compasso al suo *Trattato di fortificazione*, scritto verso il 1594. Galileo tuttavia non segue qui strettamente le regole euclidee.

Alcuni di questi risultati sono ovvi. Per il prodotto si usa il teorema di Talete, per la radice quadrata si usa il secondo teorema di Euclide. In sostanza, $x \in \mathcal{C}$ se e solo se x si può scrivere usando i numeri razionali, le quattro operazioni e la radice quadrata. Evidentemente ogni numero costruibile è algebrico (Teorema B.4.5).

Una conseguenza della trascendenza di π, che proveremo nella prossima sezione, è l'impossibilità di "quadrare il cerchio con riga e compasso". Infatti, in base alle osservazioni precedenti il problema della quadratura del cerchio è risolubile "con riga e compasso" se e solo se $\sqrt{\pi} \in \mathcal{C}$ e quindi se e solo se è $\pi \in \mathcal{C}$.

4.6.3 Trascendenza di π

Premettiamo alcuni risultati che saranno utilizzati nel corso della dimostrazione della trascendenza di π. Si noti che la trascendenza di π è "sovrabbondante" per dimostrare l'impossibilità di quadrare il cerchio con riga e compasso, in quanto:

$$\pi \text{ trascendente} \iff \pi \text{ non algebrico} \implies \pi \notin \mathcal{C}$$

In altri termini, visto il Teorema B.4.8, se si riuscisse a provare (indipendentemente dal Teorema di Lindemann) che π non è radice di un polinomio irriducibile su $\mathbb{Q}$ di grado che non è una potenza di 2 (quindi senza dover provare che π non è radice di *alcun* polinomio irriducibile su $\mathbb{Q}$), ne conseguirebbe l'impossibilità di quadrare il cerchio con riga e compasso.

(A) **Il campo dei numeri algebrici**. *Sia $\mathbb{K} \subseteq \mathbb{L}$ un ampliamento di campi. L'insieme degli elementi di $\mathbb{L}$ algebrici su $\mathbb{K}$ costituisce un sottocampo di $\mathbb{L}$.* (Teorema B.3.27)

(B) **Il polinomio minimo**. *Sia $\mathbb{K} \subseteq \mathbb{L}$ un ampliamento di campi e sia α un elemento di $\mathbb{L}$, algebrico su $\mathbb{K}$. Sia $p \in \mathbb{K}[x]$ un polinomio di grado minimo tale che $p(\alpha) = 0$. Allora p è irriducibile rispetto a $\mathbb{K}$, e p è determinato a meno di una costante moltiplicativa $\neq 0$; quindi p è univocamente determinato dalla condizione di essere monico* (Sezione B.3.2).

(C) **Teorema di d'Alembert–Gauss, o teorema fondamentale dell'algebra**. *Ogni polinomio $p \in \mathbb{R}[x]$ di grado $d = \deg(p) \geq 1$ si fattorizza in $\mathbb{C}[x]$ in d fattori di primo grado.*

(D) **I polinomi simmetrici e i polinomi simmetrici elementari**. *Ricordiamo che un* polinomio *p in m indeterminate $x_1, x_2, \ldots, x_m$ è* simmetrico *se resta "inalterato" a seguito di una permutazione delle variabili,*

cioè, se per ogni permutazione τ degli indici $\{1, 2, \ldots, m\}$ si ha

$$p(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(m)}) = p(x_1, x_2, \ldots, x_m)$$

Inoltre, se $0 \leq k \leq m$, il ***polinomio simmetrico elementare***

$$\sigma_k(x_1, x_2, \ldots, x_m)$$

di grado k nelle variabili $x_1, x_2, \ldots, x_m$ è la somma di tutti i prodotti distinti di k delle m variabili.[3]

(E) **Il teorema fondamentale dei polinomi simmetrici** (Gabelli, 2008, Teorema 2.7.7, p. 81). *Sia $\mathbb{G}$ un sottogruppo del gruppo additivo dei numeri reali, e sia f un polinomio simmetrico nelle m indeterminate $x_1, x_2, \ldots, x_m$, con coefficienti in $\mathbb{G}$. Siano $\sigma_1, \sigma_2, \ldots, \sigma_m$ i polinomi simmetrici elementari nelle indeterminate $x_1, x_2, \ldots, x_m$. Allora esiste un unico polinomio g in m indeterminate,*[4] *con coefficienti in $\mathbb{G}$ e grado $\deg(g) \leq \deg(f)$ tale che*

$$f(x_1, x_2, \ldots, x_m) = g(\sigma_1, \sigma_2, \ldots, \sigma_m)$$

(E′) **Corollario del teorema fondamentale dei polinomi simmetrici**. *Sia f un polinomio di grado m a coefficienti razionali. Siano α_1, α_2,..., α_m le radici complesse (non necessariamente distinte) di f, e sia c un polinomio simmetrico in m indeterminate con coefficienti razionali. Allora $c(\alpha_1, \alpha_2, \ldots, \alpha_m)$ è un numero razionale.*

DIMOSTRAZIONE. Per il teorema (E), $c(\alpha_1, \ldots, \alpha_m)$ è un polinomio a coefficienti razionali nei polinomi simmetrici elementari nelle α_1, α_2,..., α_m. Ma questi sono, a meno del segno, i coefficienti di f divisi per il coefficiente direttore, e quindi sono razionali. Infine, è ovvio che se si valuta un polinomio a coefficienti razionali in mumeri razionali si ottiene un numero razionale.

▼ Illustriamo il risultato precedente con un esempio. Consideriamo gli $m = 2$ numeri complessi

$$\alpha_1 = \frac{2}{3}\left(5 + i\sqrt{2}\right), \quad \alpha_2 = \frac{2}{3}\left(5 - i\sqrt{2}\right)$$

[3] In *Mathematica*, il polinomio simmetrico elementare di grado k nelle variabili $x_1, x_2, \ldots, x_m$ è implementato dal comando `SymmetricPolynomial[`k`, {`$x_1, x_2, \ldots, x_m$`} ]` .

[4] In *Mathematica*, il calcolo simbolico del polinomio g è implementato dal comando della libreria standard `SymmetricReduction[` $f(x_1, x_2, \ldots, x_m)$ `, {` $x_1, x_2, \ldots, x_m$ `} ]` .

Essi sono le radici del polinomio monico di grado 2

$$f(z) = (z - \alpha_1)(z - \alpha_2) = z^2 - \frac{20}{3}\, z + 12$$

che ha coefficienti in $\mathbb{Q}$. Sia ora

$$c(X, Y) = \frac{4}{3}\, X^2 - \frac{3}{5}\, XY + \frac{4}{3}\, Y^2$$

un polinomio simmetrico in 2 indeterminate con coefficienti razionali. Calcolando formalmente $c(\alpha_1, \alpha_2)$ si ottiene

$$c(\alpha_1, \alpha_2) = \frac{16}{27}\left(5 - i\sqrt{2}\right)^2 - \frac{4}{15}\left(5 - i\sqrt{2}\right)\left(5 + i\sqrt{2}\right) + \frac{16}{27}\left(5 + i\sqrt{2}\right)^2$$

e semplificando si ha

$$c(\alpha_1, \alpha_2) = \frac{2708}{135}$$

che è un numero razionale. Questo si spiega perché, da un lato si può esprimere $c(X, Y)$ come polinomio a coefficienti razionali nelle variabili *somma* e *prodotto* delle variabili: infatti

$$c(X, Y) = \frac{4}{3}(X + Y)^2 - \frac{49}{15}\, XY$$

e, dall'altro, per il fatto che (come si impara a scuola) la *somma* $S = \alpha_1 + \alpha_2$ ed il *prodotto* $P = \alpha_1\alpha_2$ delle radici di un polinomio monico di secondo grado coincidono rispettivamente, a meno del segno, con il coefficiente del termine di primo grado e con il termine noto. Infatti,

$$\begin{cases} f(z) &= (z - \alpha_1)(z - \alpha_2) &= z^2 - (\alpha_1 + \alpha_2)z + \alpha_1\alpha_2 \\ f(z) & & = z^2 - \frac{20}{3}\, z + 12 \end{cases}$$

implica che $S = \alpha_1 + \alpha_2 = \frac{20}{3}$ e che $P = \alpha_1\alpha_2 = 12$. Quindi possiamo verificare direttamente il valore di

$$c(\alpha_1, \alpha_2) = \frac{4}{3}(\alpha_1 + \alpha_2)^2 - \frac{49}{15}\,(\alpha_1\alpha_2) = \frac{4}{3}(\frac{20}{3})^2 - \frac{49}{15}\,(12) = \frac{2708}{135}$$

▲ ■

Come accennato nell'introduzione, la dimostrazione del teorema di Lindemann si svilupperà in $\mathbb{C}$; in particolare, al "normale" integrale $\int_a^b f(x)dx$ di variabile reale delle scuole superiori o del primo anno dell'università, finora sufficiente per le applicazioni fin qui mostrate del metodo di Hermite, dovrà

essere sostituito un "integrale di linea" in $\mathbb{C}$. Peraltro, per tali integrali di variabile complessa il fatto essenziale che verrà utilizzato è che il loro valore è, nelle situazioni più comuni, del tutto indipendente dal cammino di integrazione. Vale infatti il seguente teorema di Cauchy, per la cui dimostrazione può essere consultato un qualunque testo sulla teoria delle funzioni analitiche di variabile complessa, in particolare Courant (1937, Vol. II, p. 538) oppure Cartan (1961, p. 60):

(F) **Teorema di Cauchy**. *Sia $f(z)$ una funzione complessa di variabile complessa, analitica in un aperto semplicemente connesso $\Omega \subseteq \mathbb{C}$. Siano γ e γ' due cammini di integrazione, entrambi da z_0 a z, contenuti in Ω. Allora*

$$\int_{\gamma} f(u)du = \int_{\gamma'} f(u)du$$

Quindi, fissato $z_0 \in \Omega$, pr ogni $z \in \Omega$ si può definire una funzione $F : \Omega \to \mathbb{C}$

$$F(z) = \int_{z_0}^{z} f(u)du$$

intendendo che l'integrale è calcolato lungo un qualunque cammino in Ω da z_0 a z. Inoltre $F(z)$ è analitica e si ha

$$\frac{d}{dz} F(z) = \frac{d}{dz} \left(\int_{z_0}^{z} f(u)du \right) = f(z).$$

(G) **Esistenza di infiniti numeri primi (Euclide)**. *Per ogni intero $N > 0$ esiste un numero primo $p > N$.*

Questo risultato, generalmente attribuito ad Euclide, ha molte dimostrazioni. Aigner e Ziegler (2003, pp. 3–6) ne riportano ben sei. La prima è quella notissima degli *Elementi* (IX, 20): per ogni insieme finito $P = \{p_1, p_2, \ldots, p_n\}$ di numeri primi, sia $M = p_1 p_2 \cdots p_n + 1$. L'intero M ha un divisore primo p. Tuttavia $p \notin P$: altrimenti, p sarebbe un divisore comune di M, del prodotto $p_1 p_2 \cdots p_n$, e quindi della differenza $N - p_1 p_2 \cdots p_n = 1$, il che è impossibile. La quarta dimostrazione è di Eulero, ed è connessa alla formula scoperta da Eulero stesso:[5]

$$\frac{\pi^2}{6} = \prod_{p \text{ primo}} \frac{1}{1 - p^{-2}}$$

[5] Eulero (1740, p. 129) dimostrò dapprima che $\pi^2/6 = \sum_{k=1}^{\infty} 1/k^2$ e successivamente (1744b, *Theorema* 8, pp. 175) che: $\sum_{k=1}^{\infty} 1/k^n = \prod_{p \text{ primo}} 1/(1 - p^{-n})$, sottintendendo probabilmente n intero positivo. Per $n = 2$ si ha la formula citata.

dove il prodotto è esteso a tutti i numeri primi p, ed è un prodotto di un numero finito di termini se i numeri primi sono finiti, mentre è un prodotto infinito, del tipo (A.2.2), se i numeri primi sono infiniti. Per tale formula di Eulero, se i numeri primi fossero finiti, π^2 sarebbe razionale, contro il Teorema 4.3.1. Si osservi inoltre che, sempre se i numeri primi fossero finiti, sia π che $\sqrt{\pi}$ sarebbero numeri costruibili con riga e compasso (Teorema B.4.4) e conseguentemente il problema della quadratura del cerchio sarebbe risolubile con riga e compasso. Si potrebbe rilevare un'inutile sovraccarico tecnico nella dimostrazione di Eulero rispetto a quella euclidea. L'abbiamo qui segnalata, non solo per la connessione con l'irrisolubiltà della quadratura del circolo, ma anche perché questa tecnica di Eulero consentì a Dirichlet di dimostrare nel 1837 che, *se a, b sono interi, $a > 0$, e* $\text{MCD}(a, b) = 1$*, allora la progressione aritmetica* $\{na + b \mid n = 0, 1, 2, \ldots\}$ *contiene infiniti numeri primi*,[6] un risultato che fa parte della base teorica fondamentale della crittografia RSA a chiave pubblica (Barozzi, 1996).

Il teorema di Lindemann

Presentiamo ora la celebre dimostrazione di Lindemann della trascendenza di π. Rispetto alle precedenti applicazioni del metodo di Hermite, questa dimostrazione si svolge in $\mathbb{C}$.

Nel corso della dimostrazione inseriremo alcuni esempi espliciti dei passaggi più importanti in modo da renderla più "comprensibile".

Teorema 4.6.2 (Lindemann, 1882) *Il numero $i\pi \in \mathbb{C}$ è trascendente (sul campo $\mathbb{Q}$).*

Dimostrazione. Supponiamo per assurdo che $i\pi$ sia algebrico su $\mathbb{Q}$. Sia m il suo grado, e siano $\alpha_1, \alpha_2, \ldots, \alpha_m$ le radici complesse del suo *polinomio minimo* $p(z)$ che, ricordiamo, ha coefficienti in $\mathbb{Q}$, è irriducibile su $\mathbb{Q}$ e può essere assunto monico. La irriducibilità di $p(z)$ implica, per risultati algebrici elementari, che tali $\alpha_1, \alpha_2, \ldots, \alpha_m$ sono $m \geq 2$ numeri complessi tutti distinti

[6] *Werke*, 1889, pp. 313–342. Vedasi anche Hardy e Wright (1964), pp. 13–14, che però ritengono che "*... The proof of this theorem is too difficult for insertion in this book*". In effetti si può dire che il teorema di Dirichlet sulle progressioni aritmetiche segni il passaggio dalla teoria elementare dei numeri, alla teoria *analitica* dei numeri, nella quale si studiano i numeri interi con metodi, spesso molto profondi, tratti dell'analisi matematica ed in particolare dall'analisi complessa. In un certo senso si può dire che anche i teoremi sulla trascendenza di e e di π, che a prima vista sembrerebbero non riguardare i numeri interi, siano classificabili come teoria analitica dei numeri, in quanto essi dimostrano – nei due casi in questione – l'impossibilità che numeri interi siano coefficienti di polinomi aventi una radice uguale ad e oppure a π.

(Gabelli, 2008, p. 57, Proposizione 2.4.3; Birkhoff e Mac Lane, 1965, p. 403, Corollary 2). Notiamo che se una delle α è $i\pi$, un'altra è $-i\pi$. Abbiamo quindi banalmente che

$$0 = (e^{\alpha_1} + 1)(e^{\alpha_2} + 1) \cdots (e^{\alpha_m} + 1) \tag{4.7}$$

dato che uno dei fattori è $e^{i\pi} + 1 = 0$, ed in più è anche $e^{-i\pi} + 1 = 0$. Sviluppando il prodotto nella (4.7) otteniamo una somma di 2^m addendi del tipo e^{β_S}, dove i 2^m esponenti

$$\beta_S = \sum_{k \in S} \alpha_k$$

sono ottenuti al variare del sottoinsieme $S \subseteq \{1, 2, \ldots . m\}$ nei 2^m modi possibili.

▼ Ricordiamo che lo sviluppo del prodotto in (4.7) è la somma di tutti i possibili prodotti ottenuti scegliendo un termine in ciascun fattore. Ad esempio, se $m = 4$, possiamo scegliere 1 in tutti i fattori ottenendo 1, oppure e^{α_1} nel primo fattore e 1 negli altri tre ottenendo e^{α_1}, oppure e^{α_1} nel primo fattore, e^{α_2} nel secondo fattore e 1 negli altri due ottenendo $e^{\alpha_1+\alpha_2}$, ecc. Dunque la (4.7) diventa

$$\begin{aligned}
0 &= (1 + e^{\alpha_1})(1 + e^{\alpha_2})(1 + e^{\alpha_3})(1 + e^{\alpha_4}) \\
&= 1 \\
&+ e^{\alpha_1} + e^{\alpha_2} + e^{\alpha_3} + e^{\alpha_4} \\
&+ e^{\alpha_1+\alpha_2} + e^{\alpha_1+\alpha_3} + e^{\alpha_1+\alpha_4} + e^{\alpha_2+\alpha_3} + e^{\alpha_2+\alpha_4} + e^{\alpha_3+\alpha_4} \\
&+ e^{\alpha_1+\alpha_2+\alpha_3} + e^{\alpha_1+\alpha_2+\alpha_4} + e^{\alpha_1+\alpha_3+\alpha_4} + e^{\alpha_2+\alpha_3+\alpha_4} \\
&+ e^{\alpha_1+\alpha_2+\alpha_3+\alpha_4}
\end{aligned}$$

i cui $2^4 = 16$ addendi corrispondono nell'ordine ai 2^4 sottoinsiemi

$$\begin{aligned}
S = \ & \emptyset, \\
& \{1\}, \{2\}, \{3\}, \{4\}, \\
& \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\}, \\
& \{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \\
& \{1,2,3,4\}.
\end{aligned}$$

Notiamo che il caso $S = \emptyset$ corrisponde alla "somma vuota" $\beta_\emptyset = 0$ e quindi all'addendo $e^0 = 1$. ▲

Consideriamo ora il polinomio complesso

$$g(z) = \prod_{S \subseteq \{1,2,....m\}} (z - \beta_S) \tag{4.8}$$

▼ Nel caso $m = 4$ il polinomio $g(z)$ è:

$$\begin{aligned}
&g(z) = \\
&z\ (z-\alpha_1)(z-\alpha_2)(z-\alpha_3)(z-\alpha_4) \\
&(z-\alpha_1-\alpha_2)(z-\alpha_1-\alpha_3)(z-\alpha_1-\alpha_4)(z-\alpha_2-\alpha_3)(z-\alpha_2-\alpha_4)(z-\alpha_3-\alpha_4) \\
&(z-\alpha_1-\alpha_2-\alpha_3)(z-\alpha_1-\alpha_2-\alpha_4)(z-\alpha_1-\alpha_3-\alpha_4)(z-\alpha_2-\alpha_3-\alpha_4) \\
&(z-\alpha_1-\alpha_2-\alpha_3-\alpha_4) \\
&= z^{16} \\
&+z^{15}\ (-8\alpha_1 - 8\alpha_2 - 8\alpha_3 - 8\alpha_4) \\
&+z^{14}\ (28\alpha_1^2 + 60\alpha_1\alpha_2 + 28\alpha_2^2 + \ldots + 60\alpha_1\alpha_4 + 60\alpha_2\alpha_4 + 60\alpha_3\alpha_4 + 28\alpha_4^2) \\
&+z^{13}\ (-56\alpha_1^3 - 196\alpha_1^2\alpha_2 - 196\alpha_1\alpha_2^2 - 56\alpha_2^3 - 196\alpha_1^2\alpha_3 - 420\alpha_1\alpha_2\alpha_3 \\
&\qquad -196\alpha_2^2\alpha_3 - 196\alpha_1\alpha_3^2 - 196\alpha_2\alpha_3^2 - 56\alpha_3^3 - 196\alpha_1^2\alpha_4 - 420\alpha_1\alpha_2\alpha_4 \\
&\qquad -196\alpha_2^2\alpha_4 - 420\alpha_1\alpha_3\alpha_4 - 420\alpha_2\alpha_3\alpha_4 - 196\alpha_3^2\alpha_4 - 196\alpha_1\alpha_4^2 - 196\alpha_2\alpha_4^2 \\
&\qquad -196\alpha_3\alpha_4^2 - 56\alpha_4^3) + \quad \ldots\ldots \\
&+z^2\ (\alpha_1^8\alpha_2^4\alpha_3^2 + 4\alpha_1^7\alpha_2^5\alpha_3^2 + 6\alpha_1^6\alpha_2^6\alpha_3^2 + 4\alpha_1^5\alpha_2^7\alpha_3^2 + \alpha_1^4\alpha_2^8\alpha_3^2 + 2\alpha_1^8\alpha_2^3\alpha_3^3 \\
&\qquad +12\alpha_1^7\alpha_2^4\alpha_3^3 + 26\alpha_1^6\alpha_2^5\alpha_3^3 + 26\alpha_1^5\alpha_2^6\alpha_3^3 + \ldots\ldots + 12\alpha_1\alpha_2^3\alpha_3^2\alpha_4^8 + \alpha_2^4\alpha_3^2\alpha_4^8 \\
&\qquad +2\alpha_1^3\alpha_3^3\alpha_4^8 + 12\alpha_1^2\alpha_2\alpha_3^3\alpha_4^8 + 12\alpha_1\alpha_2^2\alpha_3^3\alpha_4^8 + 2\alpha_2^3\alpha_3^3\alpha_4^8 + \alpha_1^2\alpha_3^4\alpha_4^8 \\
&\qquad +3\alpha_1\alpha_2\alpha_3^4\alpha_4^8 + \alpha_2^2\alpha_3^4\alpha_4^8) \\
&+z\ (\ldots\ldots)
\end{aligned}$$

Per ispezione diretta, si può verificare che i coefficienti di $g(z)$ sono polinomi simmetrici nelle variabili $\alpha_1, \alpha_2, \alpha_3, \alpha_4$: chi studia faccia la verifica "visuale" per il coefficiente c_{13} di z^{13} che è stato riportato integralmente. Pertanto, per il teorema fondamentale sui polinomi simmetrici, il coefficiente c_{13} di z^{13} è rappresentabile come un polinomio nei polinomi simmetrici elementari delle

variabili $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, che sono:

$$\begin{aligned}
\sigma_0 &= 1 \\
\sigma_1 &= \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 \\
\sigma_2 &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4 \\
\sigma_3 &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 \\
\sigma_4 &= \alpha_1\alpha_2\alpha_3\alpha_4
\end{aligned}$$

Infatti, si ha[7]

$$\begin{aligned}
c_{13} = c_{13}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= -56\alpha_1^3 - 196\alpha_1^2\alpha_2 - 196\alpha_1\alpha_2^2 - \ldots - 56\alpha_4^3 \\
&= -56\,(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^3 \\
&\quad -28\,(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)\,(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4) \\
&= -56\,\sigma_1^3 - 28\,\sigma_1\sigma_2
\end{aligned}$$

Restiamo nella nostra ipotesi di lavoro $m = 4$. Consideriamo il polinomio

$$q(z) = (z - \alpha_1)(z - \alpha_2)(z - \alpha_3)(z - \alpha_4)$$

Esso ha $i\pi$ come radice, è monico ed ha il grado uguale al grado m del polinomio minimo $p(z)$ di $i\pi$; per la unicità di quest'ultimo necessariamente si ha $q(z) = p(z)$. Quindi, se calcoliamo i coefficienti di $q(z)$ troviamo:

$$\begin{aligned}
q(z) &= z^4 \\
&+ z^3\,(-\alpha_1 - \alpha_2 - \alpha_3 - \alpha_4) \\
&+ z^2\,(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_3\alpha_4) \\
&+ z\,(-\alpha_1\alpha_2\alpha_3 - \alpha_1\alpha_2\alpha_4 - \alpha_1\alpha_3\alpha_4 - \alpha_2\alpha_3\alpha_4) \\
&+ \alpha_1\alpha_2\alpha_3\alpha_4 \\
&= z^4 - \sigma_1 z^3 + \sigma_2 z^2 - \sigma_3 z + \sigma_4
\end{aligned}$$

abbiamo che $1 = \sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4$ sono numeri razionali, poiché coincidono (a meno del segno) con i cofficienti razionali di $p(z)$. Per conseguenza, abbiamo, ad esempio, che il coefficiente $c_{13} = -56\,\sigma_1^3 - 28\,\sigma_1\sigma_2$ di z^{13} nel polinomio $g(z)$ è un numero razionale. Nella nostra ipotesi di lavoro $m = 4$, si può verificare direttamente con la stessa tecnica computazionale che tutti i coefficienti di $g(z)$ sono numeri razionali. ▲

[7] Utilizzando per comodità il comando `SymmetricReduction` di *Mathematica*.

- Proviamo che i coefficienti di g sono numeri razionali.

Sostituendo nella definizione (4.8) di $g(z)$ le varie β_S con $\sum_{k\in S}\alpha_k$, vediamo che i coefficienti di $g(z)$ sono polinomi (a coefficienti interi) nelle α_k $(k = 1, \ldots, m)$. Tali polinomi sono *simmetrici*: infatti, una permutazione delle α_k non modifica *l'insieme* delle β_S ottenute al variare di S nei sottoinsiemi di $\{1, \ldots, m\}$. Per il *teorema fondamentale sui polinomi simmetrici* un generico coefficiente $c = c(\alpha_1, \alpha_2, \ldots, \alpha_m)$ di g può essere espresso come polinomio a coefficienti in $\mathbb{Q}$ nei polinomi simmetrici elementari delle variabili $\alpha_1, \alpha_2, \ldots, \alpha_m$. Ma questi polinomi simmetrici elementari sono, a meno del segno, i coefficienti del polinomio minimo di $i\pi$ diviso per il coefficiente direttore, e quindi sono in $\mathbb{Q}$. Quindi è chiaro che se c può essere espresso come un polinomio a coefficienti razionali calcolato in numeri razionali, è esso stesso razionale.

- Definizione del polinomio h a cofficienti in $\mathbb{Z}$.

Essendo $\beta_\emptyset = 0$, il polinomio $g(z)$ è divisibile per z. In effetti, si ha $\beta_S = 0$ anche per il sottoinsieme $S = \{r, s\}$ di 2 indici r ed s tali che $\alpha_r = i\pi$ ed $\alpha_s = -i\pi$, dato che in questo caso $\beta_S = \alpha_r + \alpha_s = i\pi - i\pi = 0$. Supponiamo allora che $g(z)$ sia divisibile per z^s e non per z^{s+1}. Ovviamente $s \geq 2$. Dividiamo $g(z)$ per z^s e moltiplichiamolo per un multiplo dei denominatori dei coefficienti, in modo da ottenere un polinomio

$$h(z) = h_t z^t + h_{t-1} z^{t-1} + \ldots + h_1 z + h_0$$

di grado $t = 2^m - s$ con coefficienti in $\mathbb{Z}$, e con $h_t \neq 0$, $h_0 \neq 0$ (questi due coefficienti interi avranno nel seguito un ruolo importante, specialmente h_t). Rinumeriamo i valori non–nulli dei β_S, incluse le ripetizioni, come $\beta_1, \beta_2, \ldots, \beta_t$: questi numeri complessi sono quindi le radici di h. Inoltre, dato che esattamente s dei β_S sono uguali a 0, abbiamo che esattamente s degli esponenziali e^{β_S} sono uguali a 1. Possiamo allora precisare meglio lo sviluppo dei prodotti della (4.7), ottenendo:

$$0 = e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_t} + s \tag{4.9}$$

- Impostazione del metodo di Hermite.

Per ogni intero $n \geq 0$ (da fissarsi opportunamente alla fine della dimostrazione) definiamo una funzione $\mathbb{C} \to \mathbb{C}$

$$f(z) = z^n h(z)^{n+1}$$

che è un *polinomio a coefficienti in* $\mathbb{Z}$ di grado $\deg(f) = t(n+1)+n$.[8]

Sia poi per ogni $\beta \in \mathbb{C}$:

$$I_\beta = \int_0^\beta f(z)e^{\beta-z}\,dz$$

Osserviamo che l'integrando è una funzione analitica, e quindi l'integrale non dipende dal cammino di integrazione, che può essere assunto sempre il segmento che unisce 0 a β. Sommiamo ora tutte le derivate di $f(z)$ fino a quella di ordine uguale al grado di $f(z)$ (quelle successive sono nulle); definiamo:

$$F(z) = f(z) + f'(z) + f''(z) + f'''(z) + \ldots + f^{(\deg(f))}(z) = \sum_{j=0}^{\deg(f)} f^{(j)}(z)$$

Si ha

$$\begin{aligned} \tfrac{d}{dz}\left(F(z)e^{\beta-z}\right) &= F'(z)e^{\beta-z} + F(z)e^{\beta-z}(-1) \\ &= e^{\beta-z}\{F'(z) - F(z)\} \\ &= -f(z)e^{\beta-z} \end{aligned}$$

Quindi

$$I_\beta = \int_0^\beta f(z)e^{\beta-z}\,dz = [-F(z)e^{\beta-z}]_0^\beta = F(0)\,e^\beta - F(\beta)$$

Ora, utilizzando (4.7) ed (4.9) abbiamo:

$$\begin{aligned} J := \sum_{k=1}^{t}\int_0^{\beta_k} f(z)e^{\beta_k-z}\,dz &= \sum_{k=1}^{t} I_{\beta_k} \\ &= F(0)\underbrace{\sum_{k=1}^{t} e^{\beta_k}}_{=-s} - \sum_{k=1}^{t} F(\beta_k) \\ &= -sF(0) - \sum_{k=1}^{t}\sum_{j=0}^{\deg(f)} f^{(j)}(\beta_k) \qquad (4.10) \end{aligned}$$

Stimiano ora i termini nella (4.10): la doppia somma, $F(0)$ e l'integrale J.

[8] Si noti la somiglianza con la funzione $f(x)$ utilizzata nella dimostrazione del teorema di Hermite sulla trascendenza di e. Qui l'intero $n+1$ fa le veci del numero primo p là utilizzato. Qui non dividiamo subito per $n!$ perché ci complicherebbe i calcoli.

- Stima della doppia somma.

Consideriamo la somma $\sum_{k=1}^{t} f^{(j)}(\beta_k)$ come un polinomio a coefficienti in $\mathbb{Z}$ nelle $\beta_1, \beta_2, \ldots, \beta_t$. Il polinomio g e quindi h è divisibile per $z - \beta_k$ (abbiamo selezionato i $\beta_k \neq 0$), e quindi f è divisibile per $(z - \beta_k)^{n+1}$. Quindi

$$\text{per } j \leq n, \quad f^{(j)}(\beta_k) = 0$$

Consideriamo gli altri indici $j \geq n + 1$. Allora $f^{(j)}(z)$ è un polinomio che ha coefficienti in $\mathbb{Z}$ che sono tutti divisibili per $j!$, e quindi, a maggior ragione, per $(n + 1)!$. Allora $\sum_{k=1}^{t} f^{(j)}(\beta_k)$ è un polinomio nelle $\beta_1, \beta_2, \ldots, \beta_t$ che è simmetrico per costruzione ed ha i coefficienti interi divisibili per $(n+1)!$. Siamo allora per la seconda volta in questa dimostrazione nel quadro del *teorema fondamentale sui polinomi simmetrici*, stavolta considerando i coefficienti nel gruppo additivo $G = (n + 1)!\mathbb{Z}$ degli interi divisibili per $(n + 1)!$. La somma $\sum_{k=1}^{t} f^{(j)}(\beta_k)$ può essere espressa come un polinomio p a coefficienti in G nei polinomi simmetrici elementari $\sigma_k = \sigma_k(\beta_1, \beta_2, \ldots, \beta_t)$ della variabili $\beta_1, \beta_2, \ldots, \beta_t$. Ma questi polinomi simmetrici elementari sono, a meno del segno, i coefficienti del polinomio h divisi per il coefficiente direttore, ovvero sono i numeri razionali $\pm h_{t-k}/h_t$:

$$\sum_{k=1}^{t} f^{(j)}(\beta_k) = p(\sigma_1, \sigma_2, \ldots, \sigma_t) = p\left(-\frac{h_{t-1}}{h_t}, \frac{h_{t-2}}{h_t}, \ldots, \pm\frac{h_0}{h_t}\right) \tag{4.11}$$

Sempre per il teorema fondamentale si ha che $\deg p \leq \deg f^{(j)}$, e quindi (usando anche la assunzione che sia $j \geq n + 1$):

$$\deg p \leq \deg f^{(j)} \leq \deg f - j < t(n + 1) + (n + 1) - j \leq t(n + 1)$$

Moltiplicando la (4.11) per $h_t^{t(n+1)}$ "eliminiamo" tutti i denominatori, e quindi

$$h_t^{t(n+1)} \sum_{k=1}^{t} f^{(j)}(\beta_k)$$

è un intero divisibile per $(n + 1)!$ e conseguentemente

$$h_t^{t(n+1)} \sum_{k=1}^{t} F(\beta_k) = h_t^{t(n+1)} \sum_{j=0}^{\deg(f)} \sum_{k=1}^{t} f^{(j)}(\beta_k) \tag{4.12}$$

è un intero divisibile per $(n + 1)!$.

- Stima di $F(0)$.

Applicando il Lemma 4.4.3 del Teorema 4.4.2 ad $f(z)$ nella forma

$$f(z) = \frac{z^n \cdot \overbrace{n!\, h(z)^{n+1}}^{w(z)}}{n!}$$

otteniamo che per $j \geq 0$ le derivate $f^{(j)}(0)$ sono numeri interi, uguali a:

$$f^{(j)}(0) = \begin{cases} 0 & \text{se } j < n \\ w(0) = h_0^{n+1}\, n! & \text{se } j = n \\ \text{un multiplo di } (n+1)! & \text{se } j > n \end{cases}$$

Precisiamo il ragionamento nel caso $j > n$: il Lemma 4.4.3 ci dice che in questo caso $f^{(j)}(0) = j!(c_j/n!)$ dove c_j è il coefficiente di z^j in $w(z)$; questo coefficiente è $n! \cdot \{\text{coeff. di } z^j \text{ in } h(z)^{n+1}\}$; semplificando $n!$ si ha per $j > n$ che

$$f^{(j)}(0) = j! \cdot \{\text{un numero intero}\} = (n+1)! \cdot \{\text{un numero intero}\}$$

Sommando tutti i casi per $0 \leq j \leq \deg(f)$ (range di indici che include tutti i tre casi) otteniamo che

$$F(0) = \sum_{j=0}^{\deg(f)} f^{(j)}(0) = 0 + h_0^{n+1}\, n! + \text{un multiplo di } (n+1)!$$

- Riscriviamo la (4.10) moltiplicandola membro a membro per $h_t^{t(n+1)} \neq 0$:

$$h_t^{t(n+1)}\, J = -\, h_t^{t(n+1)}\, s\, \overbrace{h_0^{n+1}\, n! + \{\text{un } \underbrace{\text{multiplo}}_{\text{doppia somma}} \text{ di } (n+1)!\}}^{F(0)} \tag{4.13}$$

dove la parentesi $\{\ldots\}$ raccoglie termini sia da $F(0)$ che dalla doppia somma.

La (4.13) è il passo cruciale nella dimostrazione del teorema. La (4.13) ci dice banalmente che il numero $|h_t^{t(n+1)}\, J|$ è divisibile per $n!$, ma tale numero potrebbe essere 0, in quanto J potrebbe essere 0.[9] Ma l'ostacolo si supera facilmente scegliendo $n+1$ un numero *primo* tale che:

$$n + 1 > \max\{\, s,\ |h_0|\,,\ |h_t|\,\}$$

[9] Nelle precedenti applicazioni del metodo di Hermite abbiamo utilizzato il fatto che se una funzione reale f è definita, continua e positiva su un intervallo $[a, b]$, allora $\int_a^b f(x)dx > 0$, un risultato che non aiuta nel caso presente, visto che $\mathbb{C}$ non è un campo ordinato.

Tale scelta di $n+1$ assicura che $|h_t^{t(n+1)}\, J| \neq 0$. Infatti, il numero primo $n+1$ è fra i fattori primi del termine nella parentesi $\{\ldots\}$, ma non può comparire nella scomposizione in fattori primi di $h_t^{t(n+1)}\, s\, h_0^{n+1}\, n!$, essendo maggiore di ciascuno dei fattori di questo prodotto. Quindi:

$$1 \leq \frac{|h_t^{t(n+1)}\, J|}{n!}$$

- Stima di J.

Per un generico $\beta \in \mathbb{C}$ abbiamo

$$I_\beta = \int_0^\beta \underbrace{z^n h(z)^{n+1}}_{=f(z)} e^{\beta - z}\, dz$$

dove il cammino di integrazione è il segmento γ da 0 a β. Per $z \in \gamma$ valgono le ovvie disuguaglianze

$$|h(z)| \leq \sum_{j=0}^{t} |h_j| \cdot |z|^j \leq \underbrace{\sum_{j=0}^{t} |h_j|}_{:=\|h\|} \cdot (1+|\beta|)^t, \qquad \left|e^{\beta - z}\right| = e^{\Re(\beta - z)} \leq e^{|\Re\beta|}$$

(abbiamo usato la maggiorazione $|z| \leq 1 + |\beta|$ e non la $|z| \leq |\beta|$ perché dobbiamo elevare ambo i membri ad un esponente intero ≥ 0). Quindi

$$\begin{aligned}
|I_\beta| &\leq \left| \int_0^\beta \left| z^n h(z)^{n+1} e^{\beta - z} \right| \, dz \right| \\
&\leq |\beta|\ |\beta|^n \left(\max_{z \in \gamma} |h(z)| \right)^{n+1} \left(\max_{z \in \gamma} \left| e^{\beta - z} \right| \right) \\
&\leq |\beta|\ |\beta|^n \left(\|h\| (1+|\beta|)^t \right)^{n+1}\ e^{|\Re\beta|} \\
&= \underbrace{|\beta|\ \|h\|\, (1+|\beta|)^t\, e^{|\Re\beta|}}_{a} \cdot \left(\underbrace{|\beta|\ \|h\|\, (1+|\beta|)^t}_{b} \right)^n = a\, b^n
\end{aligned}$$

dove le costanti a e b dipendono da β ma non da n.

Siano ora A il massimo delle costanti a e B il massimo delle costanti b al variare di β fra le $\beta_1, \beta_2, \ldots, \beta_t$. Abbiamo:

$$\begin{aligned}\left|h_t^{t(n+1)}\, J\right| &\leq \left|h_t^{t(n+1)}\right| \cdot \sum_{k=1}^{t} |I_{\beta_k}| \leq \left|h_t^{t(n+1)}\right| \cdot t\, A\, B^n \\ &= \underbrace{|h_t^t|\; t\, A}_{c} \cdot \left(\underbrace{|h_t^t|\; B}_{d}\right)^n = c\, d^n\end{aligned}$$

e in definitiva esistono due costanti c e d indipendenti da n tali che:

$$\left|h_t^{t(n+1)}\, J\right| \leq c\, d^n \tag{4.14}$$

- Conclusione della dimostrazione.

In definitiva possiamo scegliere il numero primo $n+1$ così grande da ottenere la contraddizione

$$1 \leq \frac{|h_t^{t(n+1)}\, J|}{n!} \leq \frac{c\, d^n}{n!} \to 0 \quad \text{per } n \to \infty$$

che dimostra il teorema. ■

Esempio numerico 4.6.3 Un'esemplificazione numerica del teorema di Lindemann è particolarmente complicata dall'ordine di grandezza degli interi in gioco. Supponiamo ad esempio che si assuma per assurdo che $i\pi$ sia uguale al numero algebrico ib di grado $m = 4$ con coefficiente immaginario

$$b = \frac{1}{12}\sqrt{\frac{-1 + \sqrt{3143812232245043259073}}{39451730}}$$

Si osservi, numericamente, che $b \approx 3.1415926\ldots$. Il polinomio minimo di $i\pi = ib$ è allora calcolabile senza troppe difficoltà:

$$p(z) = -\frac{642118511487958182}{6591976941146400} - \frac{z^2}{2840524560} + z^4$$

Le radici sono $(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (a, -a, ib, -ib)$ dove

$$a = \frac{1}{12}\sqrt{\frac{1 + \sqrt{3143812232245043259073}}{39451730}}$$

Sono allora calcolabili, ma utilizzando un software di computer algebra, i 16 valori β_S, ed è calcolabile il polinomio

$$
\begin{aligned}
g(z) = & \frac{4000755120447873459835106382776368722466032154333683673}{10821399891907668709109091193422573079357440000000}\, z^4 \\
& + \frac{16822500258056852217020076058462045039}{8393417391135310479381720155712581836800000}\, z^6 \\
& - \frac{43240554663309332938625783657143969698863 03}{65101979601082259426666621911080960000}\, z^8 \\
& - \frac{78595305806126081477}{11459499508971374538417408 00}\, z^{10} \\
& + \frac{261984352687086938257}{1344763295993865600}\, z^{12} \\
& - \frac{1}{710131140}\, z^{14} \\
& + z^{16}
\end{aligned}
$$

che effettivamente ha coefficienti razionali come previsto dalla dimostrazione. Si noti che in questo caso $s = 4$. Dividendo quindi $g(z)$ per z^4, moltiplicando per il m.c.m. dei denominatori dei coefficienti razionali di $g(z)$ e semplificando si ottiene infine l'espressione per $h(z)$:

$$
\begin{aligned}
h(z) = & \, 324061164756277750246643617004885866519748604501028377513 \\
& + 17567913655741480367182344138650527485700609 50\, z^2 \\
& - 58219105241608569992692283586226003451698056544384145 75\, z^4 \\
& - 60117293848837309699985192840253395331600 00\, z^6 \\
& + 17076464965835930564735144269903895530444587526080000\, z^8 \\
& - 12343260869316633057914294346636149760000 0\, z^{10} \\
& + 87653339124452116543783638666722841942795264000000\, z^{12}
\end{aligned}
$$

che è un polinomio a coefficienti interi di grado $t = 2^m - s = 12$, con coefficiente direttore e termine noto rispettivamente:

$$
\begin{aligned}
h_t &= 87653339124452116543783638666722841942795264000000 \\
h_0 &= 324061164756277750246643617004885866519748604501028377513
\end{aligned}
$$

Con un buon software di computer algebra si potrebbe proseguire in questa illustrazione numerica del teorema di Lindemann, ma si tenga conto che alla

fine si dovrà scegliere un numero primo $> h_0$. Quindi chiudiamo qui questo esempio.

Corollario 4.6.4 *π e $\sqrt{\pi}$ sono trascendenti.*

DIMOSTRAZIONE. Basta usare il fatto che il prodotto di numeri algebrici è un numero algebrico (Teorema B.3.27). ■

Corollario 4.6.5 *Non è possibile "costruire con riga e compasso" un lato L di un quadrato di area pari all'area del cerchio di raggio* 1.

DIMOSTRAZIONE. I numeri "costruibili con riga e compasso" sono particolari numeri algebrici (Teorema B.4.7), ed $L = \sqrt{\pi}$ non lo è. ■

Osservazione 4.6.6 Come vedremo in seguito, nel nota a p. 195, il problema delle costruzioni con riga e compasso è stato spesso connesso ad esigenze pratiche di natura militare. Ad esempio, il problema della duplicazione del cubo (ossia del calcolo grafico della radice cubica) trovava applicazione già ai tempi di Archimede nel caricamento ottimale delle catapulte (Russo, 1996, p. 138).

Per quanto riguarda invece la quadratura del cerchio non è evidente una sua "applicazione pratica" immediata. La sua origine è probabilmente puramente speculativa. Sappiamo infatti che Euclide (nel I Libro degli *Elementi* Prop. XLV) aveva sostanzialmente risolto il problema di costruire un quadrato di area uguale a quella di una figura a più lati (in numero finito) rettilinei: Probl. XIII: *In un angolo rettilineo dato costruire un parallelogrammo eguale ad una figura rettilinea data.* Proclo (412–485), nel suo *Commento* (Timpanaro Cardini, 1978, p. 337) scrive:

> Io son d'avviso che gli antichi furono indotti da questo problema a ricercare la quadratura del circolo.[10] Se infatti si è trovato un parallelogrammo equale ad ogni figura rettilinea, meritava di cercare se non fosse possibile dimostrare parellelogrammi uguali a figure curvilinee; e Archimede ha dimostrato che ogni circolo è uguale a un triangolo rettangolo, di cui uno dei lati che comprende l'angolo retto è uguale al raggio, e la base è uguale al perimetro.

[10] Ἐκ τούτον δὲ οἶμαι τοῦ προβλήματος ἐπα | χθέντες οἱ παλαιοὶ καὶ τὸν τοῦ κύκλου τετραγωνισμὸν ἐζήτησαν.

Epilogo

Nessuna trattazione sulla trascendenza di π collegata al problema classico della quadratura del cerchio risulterebbe completa senza la citazione dei versi conclusivi della *Divina Commedia* di Dante Alighieri (*Paradiso*, XXXIII, 133 e segg.):

> Qual è 'l geomètra che tutto s'affige
> per misurar lo cerchio, e non ritrova,
> pensando, quel principio ond'elli indige,
> tal era io a quella vista nova:
> veder voleva come si convenne
> l'imago al cerchio e come vi s'indova;
> ma non eran da ciò le proprie penne:
> se non che la mia mente fu percossa
> da un fulgore in che sua voglia venne.
> A l'alta fantasia qui mancò possa;
> ma già volgeva il mio disio e 'l velle,
> sì come rota ch'igualmente è mossa,
> l'amor che move il sole e l'altre stelle.

Per un'analisi dettagliata del famosissimo *misurar lo cerchio* si veda D'Amore (2011, pp. 198–203).

Appendice A

Complementi di Analisi matematica

In questo libro si è parlato dei numeri e e π, della loro irrazionalità, della loro trascendenza e delle loro rappresentazioni ed approsimazioni: ma quando e come questi numeri fecero la loro comparsa nella matematica?

Nell'insegnamento dell'analisi matematica sia nelle classi della scuola superiore che nei corsi universitari di matematica di base[1] ci si trova a dover affrontare il problema di come definire la funzione esponenziale, il logaritmo e le funzioni trigonometriche, ed i numeri e e π sono indissolubilmente legati a queste funzioni. Ad esempio, il rigore suggerirebbe di rimandare l'introduzione delle funzioni logaritmo ed esponenziale dopo aver trattato l'integrale, d'altra parte l'importanza di queste funzioni e la necessità di utilizzarle per illustrare alcuni aspetti del calcolo integrale stesso, come ad esempio alcune regole di integrazione, farebbe propendere per una loro precoce introduzione.

Vediamo per cominciare il caso di e e delle funzioni esponenziale e logaritmo, mentre rinviamo ad una sezione successiva le considerazioni sulle funzioni trigonometriche.

A.1 Il numero e di Nepero

Il numero e, a tutti noto come *numero di Nepero*, ha le sue origini nell'opera di Nepero (1550–1617) nel suo studio volto ad agevolare il calcoli di coloro che utilizzavano i valori delle funzioni trigonometriche. Il nome e fu intro-

[1] Un discorso a parte meriterebbe il caso dei corsi di Analisi matematica del primo anno volti a studenti dei corsi triennali di Matematica.

dotto molto più tardi (un secolo dopo) da Eulero (1707–1783), probabilmente essendo *e* la lettera iniziale della parola "esponenziale".

Il *Mirifici logarithmorum canonis descriptio* (Nepero, 1614) inizia con le seguenti parole:

> Quum nihil sit (charissimi mathematum cultores) mathematicae praxi tam molestum, quodque; Logistas magis remoretur, ac retardet, quam magnorum numerorum multiplications, partitiones, quadrataeque ac cubicae extractiones, quae praeter prolixitatis tœdium, lubricis etiam erroribus plurimum sunt obnoxiæ: Coepi igitur animo revolvere, qua arte certa & expedita, possem dicta impedimenta amoliri.[2]

Ed ancora nella prefazione del libro *Rabdologiæ* (Nepero, 1617):

> Difficultatem & prolixitate calculi (Vir illustrissime) cujus tædium plurimos à studio Mathematum deterrere solet, ego semper pro viribus, & ingenij modulo conatus sum è medio tollere.[3]

Da queste parole emerge la impellente necessità sentita da Nepero di inventare qualche nuova tecnica per snellire i calcoli, spesso molto pesanti, che si trovavano a dover affrontare i suoi contemporanei se volevano intraprendere la strada della matematica, in particolare della trigonometria, assolutamente fondamentale per lo sviluppo dell'astronomia e della navigazione.[4]

All'epoca erano note le proprietà delle potenze: si sapeva che per moltiplicare potenze intere della stessa base bastava sommarne gli esponenti, mentre non erano altrettanto ben note le potenze ad esponente razionale. Nepero spese vent'anni della sua vita nella costruzione di tavole che consentissero di agevolare questi calcoli.

Dopo anni di studio decise che poteva essere comodo rappresentare i numeri utilizzando una base vicina ad 1. Così Nepero scelse la base $1-10^{-7}$ e nella sua

[2] Poiché non vi è nulla di più fastidioso, carissimi matematici, nella pratica della matematica, delle lungaggini dovute alle moltiplicazioni, divisioni ed estrazioni di radici quadrate e cubiche e alle perdite di tempo dovute agli errori scivolosi, cominciai a dedicarmi alla ricerca di qualche idea che potesse eliminare questi ostacoli.

[3] Mi sono sempre sforzato di eliminare la difficoltà e la lunghezza del calcolo (Signore illustrissimo) che suole distogliere la maggioranza delle persone dallo studio della matematica.

[4] La *Mirifici logarithmorum canonis descriptio* venne tradotta in inglese da Edward Wright (1560–1615), matematico e cartografo in servizio presso la Compagnia delle Indie; Wright morì prima della pubblicazione della traduzione, che venne quindi affidata a suo figlio Samuel, che però morì anch'egli pochi mesi dopo; alla fine la traduzione venne completata e pubblicata nel 1618. Successivamente, l'inglese Henry Briggs (1561–1630), venuto in possesso di una copia del *Mirifici logarithmorum*, si rese conto di quanto l'idea di Nepero potesse essere utile ai calcoli nell'astronomia e nella navigazione, e propose una modifica che poi portò alla introduzione dei logaritmi in base 10. La sua idea fu proprio quella di fare in modo che il logaritmo di 10 fosse uguale 1 e così pubblicò le nuove tavole nel 1624 nel libro *Arithmetica logarithmica*. Quest'opera assunse nel secolo successivo un'importanza fondamentale nella pratica dei calcoli nautici e nella compilazione delle tabelle delle latitudini crescenti.

prima tavola scrisse i numeri nella forma $N = 10^7(1-10^{-7})^L$. Successivamente battezzò il numero L con il nome di *logaritmo* di N. Osserviamo subito che la nozione di logaritmo di Nepero differisce da quella odierna: ad esempio, il logaritmo L è uguale a 0 se $N = 10^7$ e inoltre non è vero che il logaritmo del prodotto di due numeri è la somma dei loro logaritmi. Si noti inoltre che L è funzione decrescente di N.

Esempio numerico A.1.1 Supponiamo ad esempio di dover calcolare il prodotto xy di $x = \cos(38^\circ)$ e di $y = \cos(46^\circ)$. Supponiamo di conoscere questi valori a 7 cifre decimali dopo la virgola: $x = 0.7880108$, $y = 0.6946584$. Per lavorare con interi, visto che abbiamo 7 cifre, moltiplichiamo per $M = 10^7$, ottenendo $N_1 = 7\,880\,108$ ed $N_2 = 6\,946\,584$. In questo modo la scala naturale da 0 a 1 dei coseni degli angoli del primo quadrante diventa la scala degli interi da 0 a $M = 10\,000\,000$. Per le proprietà delle potenze *ad esponente intero* si ha:

$$N_1 \times N_2 = 10^7(1-10^{-7})^{L_1} \times 10^7(1-10^{-7})^{L_2} = 10^{14}\,(1-10^{-7})^{L_1+L_2}$$

o equivalentemente:

$$\frac{N_1}{10^7} \times \frac{N_2}{10^7} = (1-10^{-7})^{L_1+L_2}$$

dove

$$L_1 = 2\,382\,435, \quad L_2 = 3\,643\,350$$

sono i "logaritmi" (secondo il *Mirifici logarithmorum canonis descriptio*) rispettivamente di N_1, N_2. La loro somma, calcolata a mano, è $L = L_1 + L_2 = 6\,025\,785$. Dovremmo ora calcolare la potenza $(1-10^{-7})^L$, ma questo ci è dato sempre dalla tavole (inverse), dove troviamo che è $N = 10^7(1-10^{-7})^L = 5\,473\,980$. Pertanto, basta spostare la virgola a sinistra di 7 posti, e si ottiene il prodotto desiderato:

$$xy = \cos(38^\circ)\,\cos(46^\circ) = 0.7880108 \times 0.6946584 = 0.5473980$$

■

Nel corso di questi studi Nepero si avvicinò comunque alla definizione del numero e, oggi chiamato numero di Nepero: infatti, se riscaliamo l'espressione $N = 10^7(1-10^{-7})^L$ dividendo sia N che L per 10^7 otteniamo

$$N^* = ((1-10^{-7})^{10^7})^{L^*}$$

dove $N^* = N/10^7$ e $L^* = L/10^7$. Ora, per $n = 10^7$, si ha

$$\left(1 - \frac{1}{n}\right)^n = (1 - 10^{-7})^{10^7} \approx e^{-1} = 1/e$$

e quindi in questo senso L^* può essere inteso come un "logaritmo approssimato" di N^* nella base $1/e$. [5]

A.1.1 Sulla definizione di *e*, delle funzioni esponenziale e logaritmo

In un'ottica che vuole vedere la matematica costruita passo passo dalle fondamenta bisognerebbe partire almeno da una buona conoscenza dei numeri reali e poi a seconda dell'approccio usato per la loro costruzione si potrebbe giungere a definire ad esempio la funzione potenza ad esponente reale. Poi da qui passando allo studio delle sue proprietà si potrebbe finalmente giungere alla definizione di esponenziale e logaritmo.

Questa strada è a nostro avviso improponibile agli studenti non matematici di elezione in quanto molto tecnica e prolissa. Essa avrebbe però il vantaggio di avere subito a disposizione delle funzioni non banali (intendo diverse dai polinomi o dai quozienti di polinomi) da impiegare negli esercizi e nelle applicazioni dei concetti di derivata e di integrale. Vediamo brevemente di seguito altri approcci che presuppongono però lo studio preliminare della teoria dei limiti, della derivata e dell'integrale oppure lo studio del limite delle succesioni e delle serie numeriche, e che quindi non sono praticabili nelle scuole secondarie.

A.1.2 Introduzione del logaritmo tramite l'integrale

Una volta che sia noto l'integrale di Riemann la funzione logaritmo in base e può essere definita ponendo per ogni $x > 0$

$$\log(x) = \int_1^x \frac{1}{t} dt$$

Questo approccio è stato adottato ad esempio da G.H. Hardy (1908, Cap. IX) e successivamente da R. Courant (1937, Vol. I, Cap. III). Seguono dalla definizione immediatamente le proprietà seguenti:

[5] Questo ha fatto osservare a taluni autori che il "numero di Nepero" dovrebbe essere $1/e = 0.367879\ldots$ e non $e = 2.71828\ldots$. È anche notevole che, se da un lato è ben noto che π compare "nel mondo reale" come un valore di probabilità del classico problema dell'ago di Buffon, è forse meno popolare il fatto che anche e è coinvolto in un antico problema combinatorio, ma nella forma $1/e$. Infatti, come dimostrato da Eulero nel 1751, proprio $1/e$ è la probabilità (asintotica) di vincita di uno dei due giocatori nel *jeu des rencontres*, un gioco di carte all'epoca molto in voga (Eulero, 1753).

1. Per il teorema fondamentale del calcolo, la funzione logaritmo è derivabile in ogni $x > 0$ e la sua derivata è $(D\log)(x) = 1/x$ (definita per $x > 0$).

2. $\log(x) > 0$ se $x > 1$, $\log(1) = 0$, $\log(x) < 0$ se $0 < x < 1$.

3. $\log(x) = -\log(1/x)$: infatti, mediante il cambio di variabili $t = 1/u$ si ottiene
$$\log(x) = \int_1^x \frac{1}{t}dt = -\int_1^{1/x} \frac{1}{u}du = -\log(1/x)$$
Alternativamente, le due funzioni $f(x) = \log(x)$ e $g(x) = -\log(1/x)$ hanno la stessa derivata: $f'(x) = 1/x$ e $g'(x) = -\frac{1}{1/x} \cdot \frac{-1}{x^2} = 1/x$, ed hanno lo stesso valore ($= 0$) in $x = 1$; quindi, per il Teorema di Lagrange, si ha $f(x) = g(x)$ per ogni $x > 0$.

4. $\log(xy) = \log(x) + \log(y)$: infatti, mediante il cambio di variabili $t = yu$ si ottiene
$$\log(xy) = \int_1^{xy} \frac{1}{t}dt = \int_{1/y}^x \frac{1}{u}du = \int_1^x \frac{1}{u}du - \int_1^{1/y} \frac{1}{u}du = \log(x) - \log(y)$$
Alternativamente, per ogni $y > 0$ dato, le due funzioni $f(x) = \log(xy)$ e $g(x) = \log(x) + \log(y)$ hanno la stessa derivata rispetto ad x: $f'(x) = 1/(xy) \cdot y = 1/x$ e $g'(x) = 1/x + 0 = 1/x$, ed hanno lo stesso valore ($= \log(y)$) in $x = 1$; quindi, per il Teorema di Lagrange, si ha $f(x) = g(x)$ per ogni $x > 0$ (e per ogni $y > 0$).

5. Siccome $(D\log)(x) > 0$ per ogni $x > 0$, la funzione logaritmo è strettamente crescente e dunque invertibile. La sua funzione inversa è per definizione la funzione esponenziale $\exp(\cdot)$, che risulta derivabile in quanto $(D\log)(x) \neq 0$ per ogni x e dalla formula di derivazione della funzione inversa
$$D\exp(x) = \frac{1}{(D\log)(\exp(x))} = \exp(x)$$

6. Per ogni a, b si ha $\exp(a) \cdot \exp(b) = \exp(a + b)$. Questo discende direttamente dalla formula $\log(xy) = \log(x) + \log(y)$, ed implica per esclusivi motivi algebrici che, se si definisce $e = \exp(1)$, si ha per $n \geq 0$ intero che $\exp(n) = e^n$, e, più in generale, che per p, q interi, $q > 0$, si ha $\exp(p/q) = \sqrt[q]{e^p}$. Questo quindi giustifica la notazione e^x per $\exp(x)$ per ogni numero reale x.

7. Si ha $\lim_{x\to+\infty}\log(x) = +\infty$: infatti, log è monotona crescente, quindi il limite suddetto esiste ed è illimitata superiormente perché

$$\log(n) = \int_1^n \frac{1}{t}dt \geq \sum_{k=2}^{n} \frac{1}{k}$$

8. Dal punto precedente segue mediante il cambio di variabile $t = 1/y$ che $\lim_{x\to 0^+}\log(x) = -\infty$.

9. Essendo derivabile, la funzione logaritmo è continua e quindi, per il teorema di esistenza del valore intermedio, la sua immagine è $\mathbb{R}$.

10. Inoltre se $1 > h > 0$ risulta, per la monotonia dell'integrale:

$$\frac{h}{1+h} < \log(1+h) < h$$

Posto $h = a/n$ si ricava che

$$\frac{a}{n+a} < \log\left(1+\frac{a}{n}\right) < \frac{a}{n}$$

Da cui

$$\lim_{n\to\infty} n\log\left(1+\frac{a}{n}\right) = a$$

e applicando la funzione exp che è continua si ha che

$$\lim_{n\to\infty} \exp\left(\log\left(1+\frac{a}{n}\right)^n\right) = \lim_{n\to\infty}\left(1+\frac{a}{n}\right)^n = \exp(a)$$

11. Pertanto si ha nel caso particolare $a = 1$ che:

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n = \exp(1)$$

12. Per definire le funzioni esponenziali in base diversa da e, scelto $a > 0$, $a \neq 1$ si pone

$$\exp_a(x) = \exp(\log(a)x)$$

13. Naturalmente la potenza ad esponente reale x^α con $x > 0$ e $\alpha \in \mathbb{R}$ si ottiene sempre da questa formula:

$$x^\alpha = \exp_x(\alpha) = \exp(\log(x)\alpha)$$

A.1.3 Introduzione dell'esponenziale tramite una serie

In alternativa, possiamo definire la funzione esponenziale mediante la serie

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \tag{A.1}$$

che converge assolutamente per ogni $x \in \mathbb{R}$ per il criterio del rapporto e totalmente (quindi uniformemente) su ogni intervallo compatto. Dunque la funzione $\exp(\cdot)$ così definita è una funzione continua su tutto $\mathbb{R}$. Questo approccio è adottato, ad esempio, da Cartan (1961, p. 28).

Teorema A.1.2 *La funzione* exp *definita da* (A.1) *verifica le seguenti proprietà:*

1. *Per ogni* $a, b \in \mathbb{R}$
$$\exp(a) \cdot \exp(b) = \exp(a + b) \tag{A.2}$$
e quindi in particolare
$$\exp(a) \cdot \exp(-a) = \exp(0) = 1$$
da cui segue che
$$\exp(-a) = \frac{1}{\exp(a)}$$
2. *Per ogni* $x \in \mathbb{R} \setminus \{0\}$ *si ha* $1 + x < \exp(x)$.
3. $\lim_{x \to +\infty} \exp(x) = +\infty$ *e* $\lim_{x \to -\infty} \exp(x) = 0$.
4. $\exp : \mathbb{R} \to (0, +\infty)$ *è continua e strettamente crescente.*
5. exp *è derivabile e* $D \exp(x) = \exp(x)$.

Dimostrazione. Dimostriamo che vale (A.2). Consideriamo le due serie convergenti

$$\exp(a) = \sum_{n=0}^{\infty} \frac{a^n}{n!} \quad e \quad \exp(b) = \sum_{n=0}^{\infty} \frac{b^n}{n!}$$

Il loro prodotto alla Cauchy (Cecconi e Stampacchia, 1974; Definizione 66.2) è la serie

$$\sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{a^k}{k!} \frac{b^{n-k}}{(n-k)!} \tag{A.3}$$

Ricordando che

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

ricaviamo che la serie (A.3) è la serie

$$\sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} = \sum_{n=0}^{\infty} \frac{(a+b)^n}{n!}$$

Poiché il prodotto alla Cauchy di due serie assolutamente convergenti converge al prodotto delle due serie (Cecconi e Stampacchia, 1974; Teorema 66.3), abbiamo dimostrato la (A.2). Dalla (A.2) segue in particolare che

$$\exp(a) \cdot \exp(-a) = \exp(0) = 1$$

Quindi $\exp(a)$ non si annulla mai e dunque è sempre positiva. Inoltre $\exp(-a) = (\exp(a))^{-1}$. Abbiamo dimostrato così il punto 1.

Dalla definizione (A.1) segue subito che se $x > 0$, allora $1 + x < \exp(x)$, quindi vale $\lim_{x\to+\infty} \exp(x) = +\infty$. Inoltre

$$\lim_{x\to-\infty} \exp(x) = \lim_{x\to+\infty} \exp(-x) = \lim_{x\to+\infty} \frac{1}{\exp(x)} = 0$$

quindi vale 3. Per definizione exp è continua e quindi $\exp(\mathbb{R}) = (0, +\infty)$.

Dal fatto che $1 + x < \exp(x)$ per $x > 0$, segue che la funzione exp è strettamente crescente. Infatti, se $x < y$, allora $y - x > 0$ e quindi $\exp(y-x) > 1 + (y - x) > 1$, che implica $\exp(y) > \exp(x)$. Abbiamo quindi dimostrato il punto 4.

Resta ancora da dimostrare che vale la 2. anche per gli x negativi. Sia $x < 0$. Se $x + 1 < 0$, la 2. vale perché $x + 1 < 0 < \exp(x)$. Se invece $-1 < x < 0$. Allora

$$\exp(x) - (1 + x) = \sum_{k=1}^{\infty} \left(\frac{x^{2k}}{(2k)!} + \frac{x^{2k+1}}{(2k+1)!} \right) = \sum_{k=1}^{\infty} \left[\frac{x^{2k}}{(2k)!} \left(1 + \frac{x}{2k+1} \right) \right]$$

e poiché $-1 < x$, si conclude che per ogni $k \geq 1$

$$\frac{x^{2k}}{(2k)!} \left(1 + \frac{x}{2k+1} \right) > 0$$

La derivabilità ed il fatto che $D \exp(x) = \exp(x)$ seguono dalle proprietà delle serie di potenze. ■

Da quanto dimostrato nel Teorema A.1.2 si ricava la invertibilità della funzione exp. Poniamo allora per definizione, per ogni x reale, $x > 0$:

$$\log(x) = \exp^{-1}(x)$$

A questo punto viene naturale chiedersi se le due funzioni exp definite una come nella Sezione A.1.2 e l'altra come nella Sezione A.1.3 sono la stessa funzione. La risposta verrà data nella Sezione A.1.4 dove si mostrerà che esiste un'unica funzione y definita su tutto $\mathbb{R}$ che soddisfa alle seguenti condizioni $y' = y,\ y(0) = 1$.

A.1.4 L'esponenziale come soluzione di un'equazione differenziale

Nel testo di *Analisi matematica* di Cecconi e Stampacchia (1974) si rinvia la definizione rigorosa delle funzioni esponenziali e trigonometriche alla fine del libro, quando già sono stati sviluppati i concetti di derivata, integrale, serie di potenze e di sviluppabilità in serie di Taylor.

Infatti, la funzione esponenziale può essere definita anche come segue (Cecconi e Stampacchia, 1974; Teoremi 94.1, 94.2 e 94.3):

Teorema A.1.3 *Esiste un'unica soluzione y del problema di Cauchy*

$$\begin{cases} y' = y \\ y(0) = 1 \end{cases}$$

definita su tutto $\mathbb{R}$. Tale funzione ammette derivate di tutti gli ordini ed è sviluppabile in serie di Taylor su $\mathbb{R}$. In particolare, risulta per ogni x reale:

$$y(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Dimostrazione. Se y è una soluzione dell'equazione $y' = y$, essa ammette derivate di tutti gli ordini coincidenti con la funzione stessa; infatti,

$$y''(x) = y'(x) = y(x),\ \ldots$$

e inoltre, se y soddisfa alla condizione iniziale $y(0) = 1$, tutte le derivate in 0 valgono 1. y è continua in quanto derivabile e quindi fissato un qualunque intervallo $[-a, a]$ e detto M il massimo di y su tale intervallo risulta per ogni $k \in \mathbb{N}$:

$$\max\left\{\left|y^{(k)}(x)\right| : x \in [-a, a]\right\} \leq M$$

Per il teorema di sviluppabilità in serie di Taylor (Cecconi e Stampacchia, 1974; Teorema 94.3) e l'unicità dello sviluppo in serie di potenze, ogni eventuale soluzione del problema di Cauchy y è sviluppabile in serie di Taylor su tutto $\mathbb{R}$ e coincide con la somma della serie

$$\sum_{n=0}^{\infty} \frac{x^n}{n!}$$

La funzione somma di tale serie è effettivamente una soluzione per ben noti teoremi sulle serie di potenze. ■

Poniamo allora per definizione

$$\exp(x) \equiv \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

A questo punto le proprietà della funzione exp e quindi anche la definizione di logaritmo possono essere dimostrate come abbiamo fatto nella sezione precedente.

A.1.5 L'approccio classico

Il percorso che potrebbe essere definito "classico" parte essenzialmente dalla definizione

$$e^x = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n \tag{A.4}$$

oppure, meno frequentemente, dalla

$$\log(x) = \lim_{n\to\infty} n\left(x^{1/n} - 1\right) \tag{A.5}$$

L'esistenza dei limiti nelle (A.4) e (A.5) non è così immediata e richiede un certo lavoro. Il fatto che le due funzioni così definite siano una l'inversa dell'altra non è neanche tanto evidente. Si può immaginare che ciò sia plausibile osservando che se $x \in \mathbb{R}$ e

$$y = \left(1 + \frac{x}{n}\right)^n$$

allora

$$x = n\left(y^{1/n} - 1\right)$$

La studio del limite (A.5) e delle sue proprietà non è usuale sui testi più recenti di analisi matematica che abbiamo consultato, ma può trovarsi ad esempio in Hardy (1908, sezione 75). Studiamo un po' più da vicino il limite (A.4).

Che esso esiste quando $x = 1$ può essere dimostrato in vari modi. Ad esempio, posto

$$a_n = \left(1 + \frac{1}{n}\right)^n \text{ e } b_n = \left(1 + \frac{1}{n}\right)^{n+1}$$

e usando la disuguaglianza di Bernoulli si fa vedere che la successione $\{a_n\}_n$ è monotona crescente e che la successione $\{b_n\}_n$ è monotona decrescente. Inoltre, si ha evidentemente

$$b_n = a_n \left(1 + \frac{1}{n}\right) > a_n \tag{A.6}$$

Quindi per il teorema sul limite delle successioni monotone, le due successioni sono entrambe convergenti e per la (A.6) convergono allo stesso limite che viene chiamato e.

Un'altro modo per dimostrare che il limite (A.4) esiste quando $x = 1$ si basa sullo sviluppo del binomio di Newton (Cecconi e Stampacchia, 1974; § 26). Dimostrare poi che il limite (A.4) esiste per ogni $x \in \mathbb{R}$ non è un esercizio da poco. La traccia di questo percorso si trova ad esempio in Cecconi, Piccinini, e Stampacchia (1979).

Se si vuole definire la funzione esponenziale tramite la (A.4), possiamo dimostrare che tale funzione coincide con la funzione definita nella Sezione A.1.3 indipendentemente dai risultati della Sezione A.1.4 mediante il seguente

Teorema A.1.4 *Per ogni $x \in \mathbb{R}$ si ha*

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n \tag{A.7}$$

Dimostrazione. Se $x = 0$, (A.7) vale. Sia ora $x > 0$. Per la formula del binomio di Newton:

$$\left(1 + \frac{x}{n}\right)^n = \sum_{k=0}^{n} \binom{n}{k} \left(\frac{x}{n}\right)^k = \sum_{k=0}^{n} \frac{n(n-1)\dots(n-k+1)}{k!} \left(\frac{x}{n}\right)^k =$$

$$= \sum_{k=0}^{n} \frac{n(n-1)\dots(n-k+1)}{n^k} \frac{x^k}{k!} =$$

$$= \sum_{k=0}^{n} 1 \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \dots \left(1 - \frac{k-1}{n}\right) \frac{x^k}{k!}$$

Dunque, se $x > 0$

$$\sum_{k=0}^{n} 1 \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \dots \left(1 - \frac{k-1}{n}\right) \frac{x^k}{k!} \leq \sum_{k=0}^{n} \frac{x^k}{k!}$$

e quindi passando al limite per $n \to \infty$ si ottiene

$$\lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n \leq \sum_{k=0}^{\infty} \frac{x^k}{k!} \tag{A.8}$$

Fissiamo ora un intero positivo m e sia $m < n$: allora

$$\begin{aligned} \left(1 + \frac{x}{n}\right)^n &\geq \sum_{k=0}^{m} 1 \left(1 - \frac{1}{n}\right) \left(1 - \frac{2}{n}\right) \dots \left(1 - \frac{k-1}{n}\right) \frac{x^k}{k!} \geq \\ &\geq \left(1 - \frac{m-1}{n}\right)^m \sum_{k=0}^{n} \frac{x^k}{k!} \end{aligned}$$

Passando al limite per $n \to \infty$ si ottiene

$$\lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n \geq \sum_{k=0}^{\infty} \frac{x^k}{k!} \tag{A.9}$$

Quindi da (A.8) e (A.9) segue che per ogni $x > 0$ vale la (A.7). In particolare

$$\lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = \sum_{k=0}^{\infty} \frac{1}{k!}$$

Per dimostrare che vale anche per $x < 0$ verifichiamo prima che

$$\lim_{n\to\infty} \left(\frac{1}{1 - \frac{x}{n}}\right)^n = \lim_{n\to\infty} \left(1 + \frac{x}{n}\right)^n \tag{A.10}$$

Ciò segue dal fatto che dato $x > \epsilon > 0$ esiste $\overline{n} > 0$ tale che per ogni $n > \overline{n}$ vale la seguente disuguaglianza

$$1 + \frac{x - \epsilon}{n} < \frac{1}{1 - \frac{x}{n}} < 1 + \frac{x + \epsilon}{n}$$

e quindi elevando alla n anche la

$$\left(1 + \frac{x - \epsilon}{n}\right)^n < \frac{1}{\left(1 - \frac{x}{n}\right)^n} < \left(1 + \frac{x + \epsilon}{n}\right)^n$$

Ora avendo definito la funzione e^x mediante il limite (A.4) e avendo dimostrato il fatto che $e^{a+b} = e^a \cdot e^b$, passando al limite nella disuguaglianza per $n \to \infty$ si conclude che per ogni $x > \epsilon > 0$

$$e^x \cdot e^{-\epsilon} \leq \lim_{n\to\infty} \left(\frac{1}{1-\frac{x}{n}}\right)^n \leq e^x \cdot e^{\epsilon}$$

Passando al limite per $\epsilon \to 0$ ricaviamo che vale (A.10) e quindi

$$\lim_{n\to\infty} \left(1-\frac{x}{n}\right)^n = \frac{1}{e^x} = \frac{1}{\sum_{n=0}^{\infty} \frac{x^n}{n!}}$$

Dalla 1. del Teorema A.1.2 concludiamo che per ogni $x > 0$

$$\lim_{n\to\infty} \left(1-\frac{x}{n}\right)^n = \sum_{n=0}^{\infty} \frac{(-x)^n}{n!}$$

che è quanto volevamo dimostrare. ■

Il numero *e* è irrazionale

Concludiamo questa parte dedicata alla funzione esponenziale con due risultati di irrazionalità la cui dimostrazione è abbastanza elementare e che possono essere considerati due interessanti esercizi. Presupponendo una qualunque delle definizioni equivalenti di e e e^x valgono i seguenti teoremi.

Teorema A.1.5 *Il numero e è irrazionale.*

DIMOSTRAZIONE. Supponiamo per assurdo che $e = N/M$ dove M e N sono interi positivi. Quindi

$$\frac{M}{N} = \sum_{n=0}^{\infty} \frac{(-1)^n}{n!}$$

Moltiplichiamo ambo i membri per $N!$, e otteniamo:

$$(N-1)!M = \sum_{n=0}^{\infty} (-1)^n \frac{N!}{n!}$$

Ora si ha

$$\sum_{n=0}^{\infty} (-1)^n \frac{N!}{n!} = \sum_{n=0}^{N} (-1)^n \frac{N!}{n!} + \sum_{n=N+1}^{\infty} (-1)^n \frac{N!}{n!} =$$

$$= N! - N! + \frac{N!}{2} + \cdots + N + (-1)^N + \sum_{n=N+1}^{\infty} (-1)^n \frac{N!}{n!}$$

La serie

$$\sum_{n=N+1}^{\infty} (-1)^n \frac{N!}{n!}$$

è una serie a serie alternati convergente, la cui somma σ è strettamente compresa fra le prime due ridotte, cioè ad esempio se N è dispari:

$$\frac{1}{N+1} > \sigma > (-1)^{N+1} \frac{1}{N+1} + (-1)^{N+2} \frac{1}{(N+1)(N+2)} =$$

$$= \left(\frac{1}{N+1} - \frac{1}{(N+1)(N+2)} \right) = \frac{1}{N+2}$$

Quindi partendo dall'ipotesi che e sia razionale abbiamo dimostrato che

$$(N-1)!M - \left(N! - N! + \frac{N!}{2} + \cdots + (-1)^N \right) = \sigma$$

dove $0 < \sigma < 1$, cioè che un numero intero è uguale a un numero strettamente compreso fra 0 e 1. Siamo giunti quindi ad un assurdo. ■

Possiamo anche dimostrare indipendentemente dal risultato precedente che

Teorema A.1.6 *Il numero $e^{1/b}$ è irrazionale per ogni $b \in \mathbb{N}$, $b > 0$.*

DIMOSTRAZIONE. Potremmo modificare leggermente la dimostrazione del Teorema precedente, ma possiamo anche procedere così.

Scriviamo la formula di Taylor con il resto di Lagrange:

$$e^{1/b} = \sum_{k=0}^{n} \frac{1}{b^k k!} + e^{\xi} \frac{1}{b^{n+1}(n+1)!}$$

dove $0 < \xi < 1/b$ e quindi $1 < e^{\xi} < e^{1/b}$. Supponiamo ora che $e^{1/b} = M/N$. Moltiplicando per $Nb^n n!$ ambo i membri della formula, troviamo che

$$Mb^n n! = \sigma + \frac{M\, e^{\xi}}{b(n+1)} \tag{A.11}$$

dove σ è un numero intero positivo. Poiché

$$\lim_{n \to 0} \frac{M}{b(n+1)} = 0$$

per n abbastanza grande sarà

$$0 < Mb^n n! - \sigma = \frac{M\, e^{\xi}}{b(n+1)} < \frac{M\, e^{1/b}}{b(n+1)} < 1$$

il che è assurdo. ■

A.2 Pi greco

La questione della definizione di π (pi greco)[6] è molto più antica di quella della definizione di e. Se per il numero e possiamo indicare nell'opera di Nepero gli inizi della sua storia, per π dobbiamo addirittura risalire a migliaia di anni fa. Ciò è dovuto al fatto che π è legato ad un problema (apparentemente) ben più elementare che è il problema di calcolare l'area del cerchio o la lunghezza della circonferenza in funzione del diametro.

Nel seguito non intendiamo presentare una storia della definizione e del calcolo di π, compito che esula dagli scopi di questo libro e che è stato egregiamente svolto da altri autori,[7] ma vogliamo ricordare soltanto alcuni contributi che per la loro semplicità potrebbero essere discussi anche con gli studenti delle scuole secondarie o dei corsi universitari del primo anno anche per esercizio, curiosità, e per cultura generale.

È ben noto che nel papiro Rhind[8] si afferma che il cerchio ha la stessa area del quadrato avente il lato uguale agli 8/9 del diametro del cerchio, ottenendo

[6] Il simbolo π fu introdotto nel 1706 da William Jones (1675–1749) nel suo libro di testo *Synopsis palmariorum mathesios* (Berggren, Borwein e Borwein, 1997, p. 108), probabilmente perché è la lettera iniziale della parola greca περίμετρος che significa "perimetro", o piuttosto l'iniziale di περιφέρεια, sostantivo derivato dal verbo περιφέρω, che significa "portare, girare intorno". Lo stesso Aristotele usa περιφερόγραμμος per dire "circondato da linea circolare", come noi usiamo tuttora "parallelogramma" per dire "racchiuso da linee parallele". All'inizio, Eulero utilizzò la lettera latina p per il termine esplicito "periferia" (*... denotante p totam circuli peripheriam cuius diameter* = 1 (Eulero, 1740)), ma successivamente optò definitivamente per la lettera greca (*Posito* π *pro peripheria circuli cuius diameter est* 1 ... (Eulero, 1744b)). L'uso di π divenne sostanzialmente universale dopo la pubblicazione dell'*Introductio in Analysin Infinitorum* (Eulero, 1797).

[7] Si veda ad esempio Berggren, Borwein e Borwein (1997) che contiene una collezione di articoli, alcuni anche in lingua originale, a partire da un commento al papiro Rhind fino ad articoli relativi agli anni '90 del Novecento passando per i testi di Archimede, Viète, Wallis, Gregory, Newton, Eulero, Lambert, Lindemann, solo per citarne alcuni.

[8] Si tratta di un papiro egizio contenente vari problemi aritmetici e geometrici risalente al 1650 a.C. acquistato dall'antiquario Henry Rhind nel 1858 a Luxor e oggi conservato al British Museum. Il papiro, lungo 3 metri e altro circa 33 centimetri, è probabilmente una copia di testi precedenti, risalenti forse al periodo fra il 1800 e il 2000 a.C.

l'approssimazione

$$\pi \approx \left(\frac{4}{3}\right)^4 = 3.\overline{160493827}$$

con un errore inferiore a 2 centesimi, un risultato veramente sorprendente se si pensa a quando è stato ottenuto.

A.2.1 Archimede e π

La storia di π è dunque molto lunga, ma una svolta, decisiva sotto molti punti di vista, si trova nell'opera *Sulla misura del cerchio* di Archimede di Siracusa (287–212 a.C.). Qui sono contenute le seguenti tre proposizioni

1. L'area di un cerchio è uguale a quella di un triangolo rettangolo avente un cateto uguale al raggio e l'altro uguale alla lunghezza della circonferenza del cerchio.

2. Il rapporto fra l'area di un cerchio e quella di un quadrato di lato uguale al diametro del cerchio è circa uguale a 11:14.

3. Il rapporto fra la lunghezza della circonferenza di un cerchio ed il suo diametro è minore di $3 + 1/7$ e maggiore di $3 + 10/71$.

Da quest'ultima considerazione si evince che Archimede ritenesse che il rapporto fra l'area di un cerchio ed il quadrato del diametro e la lunghezza della circonferenza di un cerchio ed il suo diametro non dipende dal raggio del cerchio stesso.

Archimede giunse a queste conclusioni attraverso considerazioni di geometria elementare usando dei poligoni regolari inscritti e circoscritti, in modo che di essere in grado di calcolarne l'area ed il perimetro.

Ad esempio, vediamo come Archimede pensò di calcolare il rapporto della lunghezza della circonferenza di un cerchio ed il suo diametro, cioè π. Archimede partendo dagli esagoni regolari inscritti e circoscritti ad un cerchio di raggio unitario e poi raddoppiando successivamente il numero dei lati, misurò il perimetro di tutti questi poligoni fino a quelli di 96 lati ottenendo infine la famosissima stima:[9]

$$3.14085 \approx 3 + \frac{10}{71} < \pi < 3 + \frac{1}{7} = \frac{22}{7} \approx 3.14286$$

[9] Per curiosità, gli sviluppi decimali (periodici) delle stime di Archimede sono: $22/7 = 3.\overline{1428571}$ e $3 + 10/71 = 3.\overline{140845070422535211267605633802816 90}$.

Una descrizione chiara e dettagliata del calcolo di π in Archimede, che include il commento al *Sulla misura del cerchio* di Eutocio,[10] ancora oggi più che valida, si trova in Audisio (1930).

Sotto quanto espresso da Archimede c'è l'idea che il calcolo di π si può ottenere attraverso il limite di due successioni "adiacenti", idea che verrà resa rigorosa soltanto molti secoli dopo nell'opera di Dedekind e Cantor (Fiori e Invernizzi, 2009). Per apprezzare fino in tutti i suoi aspetti l'opera di Archimede, non si deve trascurare neanche il fatto che il sistema di numerazione nella Grecia antica era piuttosto complesso e non agevolava i calcoli né permetteva di esprimere facilmente numeri molto grandi o molto piccoli. Archimede stesso cercò di risolvere questo problema in un'altra opera famosa: l'*Arenario*.

Volendo formulare e interpretare la definizione di π di Archimede in termini moderni potremmo enunciare il seguente teorema:

Teorema A.2.1 *Per ogni intero $n > 0$ indichiamo con p_n il semiperimetro del poligono regolare di $6 \cdot 2^n$ lati inscritto e con P_n il semiperimetro del poligono regolare di $6 \cdot 2^n$ lati circoscritto nel cerchio di raggio unitario.*

Allora

$$p_n \leq P_n \text{ e } p_n \leq p_{n+1} \leq P_{n+1} \leq P_n$$

$$\lim_{n\to\infty} P_n - p_n = 0 \quad e \quad \lim_{n\to\infty} P_n = \lim_{n\to\infty} p_n$$

A.2.2 Il prodotto infinito di Viète

Facciamo ora un volo di qualche secolo e arriviamo al XV secolo dopo Cristo quando François Viète[11] nel 1593 propose la prima rappresentazione "esatta" giunta sino a noi di π come il prodotto infinito:

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}}\cdots \tag{A.12}$$

Ricordiamo che

Definizione A.2.2 *Con il prodotto infinito*

$$\prod_{n=1}^{\infty} b_n, \tag{A.13}$$

[10] Eutocio di Ascalona, matematico bizantino (480 ca. – 540 ca.).

[11] François Viète (1540–1603) non era un matematico di professione, ma si occupò di astronomia e di trigonometria per *hobby*. Egli infatti era un avvocato dedito alla politica.

si intende la successione definita per ricorrenza

$$x_1 = b_1, \quad x_n = x_{n-1} \cdot b_n$$

Si dice che il prodotto infinito (A.13) *è convergente a ℓ, se la successione $\{x_n\}_n$ così definita è convergente a ℓ e si scrive*

$$\ell = \prod_{n=1}^{\infty} b_n$$

In analogia con quanto ben noto per le serie si ha che

Lemma A.2.3 *Condizione necessaria affinché il prodotto* (A.13) *sia convergente è che*

$$\lim_{n\to\infty} b_n = 1$$

In base alla definizione con (A.12) si deve intendere che la successione definita per ricorrenza

$$x_1 = \sqrt{\frac{1}{2}}, \; x_n = \sqrt{\frac{1}{2}(1 + x_{n-1})}$$

è convergente e che

$$\lim_{n\to\infty} x_n = \frac{2}{\pi}$$

Viète giunse alla formula (A.12) seguendo un'idea simile a quella di Archimede: partì dal fatto che π è il limite della successione delle aree A_n dei poligoni regolari di $N = 2^n$ lati inscritti nel cerchio unitario. Congiungendo i vertici del poligono di 2^n lati inscritto nel cerchio unitario con il centro osserviamo (aiutandoci con un po' di trigonometria) che A_n è uguale alla somma delle aree di N triangoli uguali fra loro aventi al centro un angolo pari a 2θ. Quindi

$$A_n = 2^n \cos(\theta) \sin(\theta)$$

Raddoppiando il numero di lati si ha che

$$A_{n+1} = 2^{n+1} \cos\left(\frac{\theta}{2}\right) \sin\left(\frac{\theta}{2}\right) = 2^n \sin(\theta)$$

da cui segue che

$$A_n = A_{n+1} \cos(\theta)$$

Allora partendo da $n = 2$ si ha

$$\begin{aligned} 2 &= A_2 = A_3 \cos\left(\frac{\pi}{4}\right) = A_4 \cos\left(\frac{\pi}{4}\right) \cos\left(\frac{\pi}{8}\right) = \dots \\ &= A_{n+1} \cos\left(\frac{\pi}{4}\right) \cos\left(\frac{\pi}{8}\right) \dots \cos\left(\frac{\pi}{2^n}\right). \end{aligned}$$

Per esprimere i valori $\cos\left(\frac{\pi}{2^k}\right)$ $(k = 2, \ldots, n)$ si deve usare la formula

$$\cos\left(\frac{\theta}{2}\right) = \sqrt{\frac{1+\cos(\theta)}{2}} = \sqrt{\frac{1}{2} + \frac{1}{2}\cos(\theta)}$$

Per cui

$$\cos\left(\frac{\theta}{2^2}\right) = \sqrt{\frac{1+\cos(\theta/2)}{2}} = \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\cos(\theta)}}$$

infine, posto $\theta = \pi$ e in base all'ipotesi che $\lim_{n\to\infty} A_n = \pi$, passando al limite per $n \to \infty$ si trova (A.12). ■

Senza seguire il ragionamento geometrico di Viète ma partendo da una definizione astratta di seno e coseno mediante le serie di potenze, cioè ponendo

$$\sin(x) = \sum_{n=1}^{\infty}(-1)^n \frac{x^{2n+1}}{(2n+1)!} \;\; e \;\; \cos(x) = \sum_{n=0}^{\infty}(-1)^n \frac{x^{2n}}{(2n)!}$$

e dimostrando a partire da queste la formula di duplicazione si può giungere ugualmente a (A.12) al modo seguente.

Da $\sin(\theta) = 2\sin(\theta/2)\cos(\theta/2)$, si ottiene

$$\frac{\sin(\theta)}{\theta} = \frac{\sin(\theta/2)}{\theta/2}\cos(\theta/2)$$

Sostituendo $\theta/2$ al posto di θ si trova:

$$\frac{\sin(\theta)}{\theta} = \frac{\sin(\theta/2^2)}{\theta/2^2}\cos(\theta/2)\cos(\theta/2^2)$$

Iterando il procedimento si giunge quindi a

$$\frac{\sin(\theta)}{\theta} = \frac{\sin(\theta/2^n)}{\theta/2^n}\cos(\theta/2)\cos(\theta/2^2)\ldots\cos(\theta/2^n)$$

ovvero a

$$\prod_{k=1}^{n}\cos(\theta/2^k) = \frac{\sin(\theta)}{\theta}\frac{\theta/2^n}{\sin(\theta/2^n)}$$

Passando al limite per $n \to \infty$ e sapendo che

$$\lim_{x\to 0}\frac{\sin(x)}{x} = 1$$

e infine ponendo $\theta = \pi/2$ si ottiene la (A.12). ■

A.2.3 Il prodotto infinito di Wallis

Nel 1655 John Wallis dimostrò nel suo libro *Arithmetica infinitorum* che

$$\frac{\pi}{2} = \frac{2 \cdot 2}{1 \cdot 3} \cdot \frac{4 \cdot 4}{3 \cdot 5} \cdots = \prod_{n=1}^{\infty} \frac{4n^2}{4n^2 - 1} \tag{A.14}$$

Poiché

$$\frac{4n^2}{4n^2 - 1} = 1 + \frac{1}{4n^2 - 1}$$

la convergenza del prodotto a destra della (A.14) discende dal seguente lemma (Courant, 1937; Appendix to Cap. VIII, § 3):

Lemma A.2.4 *Dato il prodotto infinito*

$$\prod_{n=1}^{\infty} b_n, \tag{A.15}$$

poniamo $b_n = 1 + a_n$. *Se la serie* $\sum_{n=1}^{\infty} |a_n|$ *è convergente allora il prodotto* (A.15) *e il prodotto*

$$\prod_{n=1}^{\infty} (1 + |a_n|)$$

sono convergenti.

Il prodotto di Wallis fu la prima rappresentazione di π come limite di una successione di numeri razionali.

Non seguiremo qui la dimostrazione originale di Wallis, ma partiremo dai cosiddetti *integrali di Wallis*, seguendo ad esempio Courant (1937) o Cecconi e Stampacchia (1974, § 80)

$$I_{2n} = \int_0^{\frac{\pi}{2}} \sin^{2n}(x) dx = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1)}{2 \cdot 4 \cdot 6 \cdot \cdots \cdot (2n)} \frac{\pi}{2}$$

$$I_{2n+1} = \int_0^{\frac{\pi}{2}} \sin^{2n+1}(x) dx = \frac{2 \cdot 4 \cdot 6 \cdot \cdots \cdot (2n)}{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n+1)}$$

Tali formule possono essere dimostrate applicando ripetutamente la formula di integrazione per parti e sono legati alla formula (A.14) dalla relazione

$$\frac{\pi}{2} = x_n \frac{I_{2n}}{I_{2n+1}}$$

dove

$$x_n = \prod_{k=1}^{n} \frac{4k^2}{4k^2 - 1}$$

Quindi sapendo che $\{x_n\}_n$ è convergente, se riusciamo a dimostrare che

$$\lim_{n\to\infty} \frac{I_{2n}}{I_{2n+1}} = 1 \tag{A.16}$$

avremo dimostrato la (A.14). Ora nell'intervallo $(0, \pi/2)$ il seno è positivo e minore di 1, perciò

$$0 < \sin^{2n+1}(x) \leq \sin^{2n}(x) \leq \sin^{2n-1}(x)$$

da cui segue che

$$0 < I_{2n+1} \leq I_{2n} \leq I_{2n-1}$$

Quindi dividendo per I_{2n+1} si ricava che

$$1 \leq \frac{I_{2n}}{I_{2n+1}} \leq \frac{I_{2n-1}}{I_{2n+1}} = 1 + \frac{1}{2m}$$

e quindi si ha (A.16). ■

A.2.4 Altri modi di definire π

La "definizione" popolare delle funzioni circolari coseno e seno è difettosa nel punto in cui non prende in considerazione il problema della *suriettività* della misura degli angoli (o degli archi). Ad esempio, ripetiamo quella definizione e chiediamoci subito dopo se e perché esiste un arco di lunghezza pari al raggio della circonferenza. In mancanza di questa dimostrazione di esistenza, non possiamo affermare che esiste l'angolo di 1 radiante, cioè proprio l'unità di misura "matematica" degli angoli, e quindi neppure che esistono i valori cos(1) e sin(1).

Di definizioni rigorose di coseno e seno ne esistono molte, ad esempio ce n'è una basata sulle serie di potenze (Cartan, 1961, p. 30):

$$\begin{cases} \cos(x) = 1 - \dfrac{x^2}{2!} + \dfrac{x^4}{4!} - \dfrac{x^6}{6!} + \dfrac{x^8}{8!} \mp \dots \\ \sin(x) = x - \dfrac{x^3}{3!} + \dfrac{x^5}{5!} - \dfrac{x^7}{7!} + \dfrac{x^9}{9!} \mp \dots \end{cases} \tag{A.17}$$

ed un'altra basata sullo studio dei problemi di Cauchy:

$$\begin{cases} y'' + y = 0 \\ y'(0) = 0,\ y'(0) = 1 \end{cases}$$

$$\begin{cases} y'' + y = 0 \\ y'(0) = 1,\ y'(0) = 0 \end{cases}$$

per la quale rinviamo a Cecconi e Stampacchia (1974, § 96).

Cerchiamo qui di "mettere a posto" la definizione popolare di coseno e seno[12] seguendo una strada che presuppone la nozione di lunghezza di una curva regolare. Consideriamo la funzione

$$f : [-1, 1] \to \mathbb{R}, \quad f(x) = \sqrt{1 - x^2}$$

il cui grafico è la semicirconferenza nel semipiano superiore. Fissiamo $x \in [-1, 1]$ e consideriamo la lunghezza della curva fra le ascisse x ed 1:

$$L(x) = \int_x^1 \sqrt{1 + f'(u)^2}du = \int_x^1 \sqrt{1 + \frac{u^2}{1 - u^2}}du = \int_x^1 \frac{1}{\sqrt{1 - u^2}}du$$

Poniamo ***per definizione***

$$\pi = \int_{-1}^1 \frac{1}{\sqrt{1 - u^2}}du$$

[12] La definizione cui alludiamo è quella secondo la quale, assumendo $0 \leq x < 2\pi$, $(\cos(x), \sin(x))$ sono le coordinate cartesiane del punto P della circonferenza di centro $O = (0, 0)$ e raggio 1 tale che, posto $U = (1, 0)$, l'angolo $\widehat{UOP}$ misuri x radianti. È da osservare che nel mentre alcuni autori considerano inaccettabile per il loro livello di rigore la definizione in base alla quale "il logaritmo di un dato numero x è l'esponente da dare alla base per ottenere che la potenza sia uguale ad x", valutano invece didatticamente accettabile la "definzione" di coseno e seno precedentemente enunciata, che ricalca sintatticamente quasi *verbatim* quella "rifiutata" di logaritmo. Infatti tale definizione "popolare" di coseno e seno altro non dice che "il coseno ed il seno di un dato numero x sono le coordinate da dare al punto P del cerchio unitario per ottenere che la lunghezza dell'arco di circonferenza $\overset{\frown}{UOP}$ sia uguale ad x". Nei due casi, il problema non è quindi quello di definire "rigorosamente" la potenza ad esponente reale o la lunghezza degli archi (equivalentemente la misura degli angoli in radianti), quanto quello di mettere in evidenza il problema della *suriettività*. Come mai siamo certi che esiste un reale a tale che $10^a = 2$? Ed analogamente, come mai siamo certi che esiste un punto P sulla circonferenza unitaria tale che l'arco $\overset{\frown}{UOP}$ sia lungo 2, cioè esattamente il doppio del raggio? Come si è visto in quest'appendice, queste problematiche non sono affatto banali, ma quello che sarebbe forse da evitare è di trattare didatticamente i due casi (logaritmo e funzioni trigonometriche) a diversi livelli di rigore senza dichiararlo esplicitamente.

L'integrale improprio (alla Riemann) è convergente. Infatti per $0 < u < 1$

$$0 < \frac{1}{\sqrt{1-u^2}} = \frac{1}{\sqrt{1-u}\sqrt{1+u}} \leq \frac{1}{\sqrt{1-u}\cdot 1}$$

e quindi

$$\int_0^1 \frac{1}{\sqrt{1-u^2}}du \leq \int_0^1 \frac{1}{\sqrt{1-u}}du = \lim_{b\to 1}\int_0^b \frac{1}{\sqrt{1-u}}du$$

$$= \lim_{b\to 1}\left[-2\sqrt{1-u}\right]_0^b = \lim_{b\to 1}(2-2\sqrt{1-b}) = 2$$

Quindi l'integrale da 0 a 1 converge per il criterio del confronto. Analogamente converge da -1 a 1. In particolare $\pi < 4$.

Per il teorema fondamentale del calcolo, la funzione L è derivabile in $(-1,1)$ ed è continua su $[-1,1]$ ***per costruzione***.[13] Inoltre L è strettamente decrescente e (per il teorema di esistenza del valore intermedio) è suriettiva su $[0,\pi]$. Quindi L è invertibile. Poniamo per definizione

$$\arccos : [-1,1] \to [0,\pi], \quad \arccos(x) = \int_1^x \frac{-1}{\sqrt{1-u^2}}du \quad (= L(x))$$

Poniamo poi per definizione

$$\cos : [0,\pi] \to [-1,1], \quad \cos = \text{funzione inversa di } \arccos$$

quindi effettivamente $\cos(x)$ è l'ascissa del punto P della (semi)circonferenza unitaria tale che la lunghezza dell'arco dal punto $(1,0)$ al punto P è uguale a $L(\cos(x)) = x$. L'ordinata di P viene chiamata per definizione

$$\sin(x) = f(\cos(x)) = \sqrt{1-\cos^2(x)}$$

[13] In generale: supponiamo che $f : [0,1) \to \mathbb{R}$ sia continua, e supponiamo che esista l'integrale improprio (alla Riemann) $\int_0^1 f(u)du$. Definiamo $F : [0,1] \to \mathbb{R}$ ponendo

$$\begin{cases} F(x) = \int_0^x f(u)du & \text{per } 0 \leq x < 1 \\ F(1) = \int_0^1 f(u)du & \text{(integrale improprio)} \end{cases} \tag{A.18}$$

Proprio per definizione di integrale improprio si ha

$$\lim_{x\to 1} F(x) = F(1)$$

ossia F è continua in 1 (e lo è negli altri punti dove f esiste continua per il teorema fondamentale del calcolo).

Abbiamo

$$\frac{d}{dx}\arccos(x) = \frac{-1}{\sqrt{1-x^2}}$$

$$\frac{d}{dx}\cos(x) = \frac{1}{\frac{-1}{\sqrt{1-\cos^2(x)}}} = -\sin(x)$$

$$\frac{d}{dx}\sin(x) = \frac{1}{2\sqrt{1-\cos^2(x)}} \cdot (-2\cos(x)) \cdot (-\sin(x)) = \cos(x)$$

Prolunghiamo poi cos a $[-\pi, \pi]$ per simmetria pari e sin a $[-\pi, \pi]$ per simmetria dispari, e prolunghiamo entrambe a $\mathbb{R}$ per $2\pi-$periodicità. Queste estensioni conservano le formule delle derivate. Per dimostrare le formule di addizione, definiamo, per α fissato, le funzioni:

$$\begin{aligned}
\phi(x) &= \sin(\alpha + x) - \{\sin(\alpha)\cos(x) + \cos(\alpha)\sin(x)\} \\
\phi'(x) &= \cos(\alpha + x) - \{-\sin(\alpha)\sin(x) + \cos(\alpha)\cos(x)\} \\
\phi''(x) &= -\sin(\alpha + x) + \{\sin(\alpha)\cos(x) + \cos(\alpha)\sin(x)\}
\end{aligned}$$

Quindi $\phi(x)$ è soluzione del problema di Cauchy $\phi'' + \phi = 0$, $\phi(0) = \phi'(0) = 0$, e per la unicità della soluzione di questo problema di Cauchy deve essere, per ogni $x \in \mathbb{R}$, $\phi(x) = 0$, cioè deve valere la formula di addizione del seno e quindi anche $\phi'(x) = 0$, cioè la formula di addizione del coseno.

Infine, non possiamo trascurare di ricordare che si incontrano, nel corso degli studi, delle serie di potenze che convergono a multipli razionali di π. Ad esempio, dalla serie dell'arcotangente

$$\arctan(x) = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{2k+1}$$

si trova la *formula di Leibnitz*:

$$\frac{\pi}{4} = \arctan(1) = \sum_{k=0}^{\infty} (-1)^k \frac{1}{2k+1}$$

A.2.5 L'esponenziale in campo complesso

Esula gli scopi di questo libro la trattazione delle proprietà fondamentali dell'esponenziale in campo complesso, ma dal momento che esso viene utilizzato nella dimostrazione del teorema di Lindemann ci sembra utile per il lettore di inserire un breve cenno a riguardo.

L'esponenziale in campo complesso può essere definito a partire dalla serie

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} \tag{A.19}$$

dove $z \in \mathbb{C}$. La serie in (A.19) risulta assolutamente convergente per ogni $z \in \mathbb{C}$ per quanto detto nella Sezione A.1.3 e per le proprietà delle serie di potenze in campo complesso, la funzione $\exp(z)$ (che viene anche indicata con il simbolo e^z) risulta derivabile in senso complesso con $D\exp(z) = \exp(z)$, per ogni $z \in \mathbb{C}$. Ora se il numero complesso z è immaginario puro, cioè se $z = i\beta$, ricordando che le serie assolutamente convergenti sono permutabili, si osserva che da (A.19) segue che

$$\exp(i\beta) = \sum_{n=0}^{\infty} \frac{(i\beta)^n}{n!} = \sum_{k=0}^{\infty} (-1)^k \frac{\beta^{2k}}{(2k)!} + i \sum_{k=0}^{\infty} (-1)^k \frac{\beta^{2k+1}}{(2k+1)!}$$

per cui (ricordando gli sviluppi (A.17) in serie di potenze di seno e coseno) si perviene alla ben nota formula

$$\exp(i\beta) = \cos(\beta) + i\sin(\beta)$$

da cui seguono le *formule di Eulero* $\exp(i\pi) = \cos(\pi) = -1$ e $\exp(-i\pi) = \cos(-\pi) = -1$ che rivestono un ruolo essenziale nella dimostrazione del teorema di Lindemann.

Appendice B

Compendio di Algebra

Con quest'appendice abbiamo inteso rendere il più possibile autosufficiente la trattazione per quel che concerne le nozioni basilari di algebra e in particolare familiarizzare con le strutture algebriche. Particolare attenzione è riservata alla struttura di campo e alle relative estensioni algebriche. Si considerano, in particolare, i campi di caratteristica zero perché questa è la caratteristica dei campi numerici. Vengono richiamate le definizioni e le proprietà inerenti alla algebricità e/o trascendenza di un numero reale. Definizioni e teoremi sono illustrati con esempi e osservazioni di tipo anche didattico. Infine, per rimarcare lo stretto legame fra l'algebra e la geometria e il legame con l'algebricità o trascendenza di un numero reale, si caratterizzano algebricamente i punti del piano reale costruibili con riga e compasso (costruzioni euclidee).

B.1 La divisione euclidea. MCD di due interi

Ricordiamo una proprietà dei numeri interi di cui si fa uso in varie parti del testo. Grazie a questa proprietà, nell'insieme $\mathbb{Z}$ dei numeri interi è possibile eseguire la *divisione con resto* detta anche *divisione euclidea* (Teorema B.1.1). Questa proprietà, così importante per gli interi, non lo è per i numeri razionali, reali, complessi perché in questi ambienti numerici la divisibilità $b|a$ (b divide a) c'è sempre ogniqualvolta $b \neq 0$. Qualunque siano $a, b \in \mathbb{Z}$ non entrambi nulli, la divisione euclidea assicura due proprietà fondamentali:

1. Esiste il $\text{MCD}(a, b)$ (Teorema B.1.3),
2. Fornisce un algoritmo per calcolare il $\text{MCD}(a, b)$ (Corollario B.1.4).

Teorema B.1.1 *Se $a, b \in \mathbb{Z}$ e $b \neq 0$ allora esistono e sono unici $q, r \in \mathbb{Z}$ tali che $a = bq + r$ e $0 \leq r < |b|$.*

Di questo teorema daremo due dimostrazioni, la prima di carattere geometricamente più intuitiva (Villani, 2003, nota a pie' di p. 28), la seconda più algoritmica, basata sul principio di induzione.

DIMOSTRAZIONE. Consideriamo l'insieme

$$T = \{bk \mid k \in \mathbb{Z},\ bk \leq a\}$$

dei multipli di b minori od uguali ad a. Poniamo $m = \max T$. Essendo m multiplo di b, esiste $q \in \mathbb{Z}$ tale che $m = bq$, e definiamo $r = a - bq$, in modo che sia $a = bq + r$. Dato che $m = bq = \max T \in T$ si ha $m = bq \leq a$, ossia $r = a - bq \geq 0$. Se fosse per assurdo $r \geq |b|$, avremmo $a - m = a - bq = r \geq |b|$ e quindi $m + |b| = bq + |b|$ sarebbe un multiplo di b minore o uguale ad a, e quindi un elemento di T, però maggiore di $m = \max T$. Dimostriamo infine l'unicità di q ed r. Supponiamo esistano anche q' ed r' interi tali che $a = q'b + r'$ con $0 \leq r' < |b|$ e con $r' \geq r$ (analogamente se fosse $r' \leq r$). Si ottiene $(q - q')b = r' - r$ con $0 \leq r' - r < |b|$ da cui segue dapprima $q = q'$ e poi $r = r'$. ■

DIMOSTRAZIONE. Supponiamo dapprima $a \in \mathbb{N}$ e $b \in \mathbb{N}^*$ e proviamo

$$P_a : \text{ ″ esistono } q, r \in \mathbb{N} \text{ tali che } a = bq + r \text{ con } 0 \leq r < b \text{ ″}.$$

Per $a = 0$ la proposizione P_0 è vera (basta prendere $q = 0$ e $r = a$). Sia ora $a > 0$; se è $a \leq b$ la P_a è sempre vera (nel caso $a = b$ si ha $q = 1$, $r = 0$; nel caso $a < b$ si ha $q = 0, r = a$); se è $b < a$ procediamo per induzione su a.
Per $a = 1$ la proposizione è banalmente vera. Supponiamo vera P_a e dimostriamo che vale P_{a+1}. Si ha $a = bq + r$ con $0 \leq r < b$. Se è $r = b - 1$ risulta $a + 1 = bq + r + 1 = bq + b = b(q + 1) + 0$ e la P_{a+1} è vera. Se è $r < b - 1$ otteniamo $a + 1 = bq + r + 1$ con $0 < r + 1 < b$ e la P_{a+1} è vera.

Dimostriamo ora che comunque presi $a, b \in \mathbb{Z}$, $b \neq 0$, esistono $q, r \in \mathbb{Z}$ tali che $a = bq + r$ con $0 \leq r < |b|$. Il teorema è pertanto dimostrato quando è $a \geq 0$ e $b > 0$ e quando è $a = 0$ e $b < 0$ (basta prendere $q = r = 0$). Proviamo ora il teorema negli altri casi.

1) Sia $a < 0,\ b > 0$.

   Esistono $q,\ r \in \mathbb{N}$ tali che $-a = qb + r$ con $0 \leq r < b$. Se è $r = 0$ si ha $a = (-q)b + 0$ ed il risultato è provato. Se è $r > 0$ si ha $a = (-q - 1)b + (b - r)$ con $0 < b - r < b$ ed il risultato è provato.

2) Sia $a < 0,\ b < 0$.

   Si ha $-a = q(-b) + r$ con $q,\ r \in \mathbb{N}$ e $0 \leq r < |b|$. Se è $r = 0$ si ha $a = qb + 0$ ed il risultato è provato. Se è $r > 0$ si ha $a = (q+1)b - b - r = (q+1)b + |b| - r$ ed essendo $0 < |b| - r < |b|$ il risultato è provato.

3) Sia $a > 0,\ b < 0$.

   Si ha $a = q(-b) + r$ con $q,\ r \in \mathbb{N}$ e $0 \leq r < |b|$ e quindi $a = (-q)b + r$ ed il risultato è provato.

Dimostriamo infine l'unicità di q ed r. Supponiamo esistano anche q' ed r' interi tali che $a = q'b + r'$ con $0 \leq r' < |b|$ e con $r' \geq r$ (analogamente se fosse $r' \leq r$). Si ottiene $(q - q')b = r' - r$ con $0 \leq r' - r < |b|$ da cui segue $q = q'$ ed $r = r'$. ■

MCD di due interi

Definizione B.1.2 *Dati $a, b \in \mathbb{Z}$ non entrambi nulli, un intero $d \in \mathbb{Z}$ si dice* ***massimo comune divisore*** *di a e b se:*

1. *$d \mid a$ e $d \mid b$*
   (d è divisore sia di a che di b, cioè d è un divisore "comune" di a e b),

2. *se $d' \mid a$ e $d' \mid b$ allora $d' \mid d$*
   (ossia se d' è divisore comune di a e b, allora è un divisore di d).

Si osservi che se d è massimo comune divisore di a e b anche $-d$ lo è. In pratica in $\mathbb{Z}$ il massimo comune divisore è definito a meno del segno, e quindi, per convenzione, in $\mathbb{Z}$ si sceglie sempre come massimo comune divisore di due interi a, b non entrambi nulli quello positivo, e lo si indica con $\text{MCD}(a, b)$. Di conseguenza, praticamente, in $\mathbb{Z}$ il $\text{MCD}(a, b)$ è davvero il massimo (nel senso dell'ordinamento canonico di $\mathbb{Z}$) dei divisori comuni di a, b.

Teorema B.1.3 (Identità di Bézout) *Dati comunque $a, b \in \mathbb{Z}$ non entrambi nulli, esiste il loro massimo comune divisore $d = \text{MCD}(a, b)$. Inoltre si possono trovare $s, t \in \mathbb{Z}$ tali che $d = sa + tb$.*

Dimostrazione. Sia $T = \{xa + yb \mid x, y \in \mathbb{Z}, xa + yb > 0\} \subseteq \mathbb{N}$. Tale T è sicuramente non vuoto perché a e b non sono entrambi nulli e quindi, se ad esempio $a \neq 0$, sarà certamente $a > 0$ oppure $-a > 0$ e quindi a oppure $-a$ sono in T. In T esisterà pertanto un minimo: sia esso $d = x_0 a + y_0 b$. Proviamo che d è il massimo comune divisore di a e b. È ovvio che se $h \mid a$, ed $h \mid b$,

allora $h \mid d$. Proviamo che $d \mid a$ e $d \mid b$. Per il teorema precedente, possiamo scrivere $a = dq + r$, con $0 \leq r < d$. Si ha $0 \leq r = a - dq = a - (x_0 a + y_0 b)q = (1 - x_0)a + (-y_0 q)b \leq d$; per l'ipotesi di minimalità fatta su d deve essere $r = 0$ e quindi $d \mid a$. Analogamente si prova che $d \mid b$. Rimangono così dimostratate sia l'esistenza del $\text{MCD}(a, b)$ sia la scrittura nella forma $d = sa + tb$. ■

Corollario B.1.4 (Algoritmo euclideo) *Siano dati $a, b \in \mathbb{Z}, a \geq b > 0$. Operiamo le seguenti divisioni:*

$$\begin{array}{lcllll}
a & = & bq_1 & + & r_1 & 0 < r_1 < b \\
b & = & r_1 q_2 & + & r_2 & 0 < r_2 < r_1 \\
r_1 & = & r_2 q_3 & + & r_3 & 0 < r_3 < r_2 \\
\ldots & & \ldots & & & \\
r_{n-3} & = & r_{n-2} q_{n-1} & + & r_{n-1} & 0 < r_{n-1} < r_{n-2} \\
r_{n-2} & = & r_{n-1} q_n & + & r_n & 0 < r_n \quad < r_{n-1} \\
r_{n-1} & = & r_n \quad q_{n+1} & + & 0 &
\end{array}$$

Allora $MCD(a, b) = r_n$ (ultimo resto non nullo).

Il procedimento deve certamente avere termine (in meno di b passi) perché $b > r_1 > r_2 > \ldots$ è una successione strettamente decrescente di interi positivi. Ora, dall'ultima divisione si ha che $r_n \mid r_{n-1}$ per cui $\text{MCD}(r_n, r_{n-1}) = r_n$. Andando dal basso verso l'alto, si ha $r_n \mid r_{n-2}$, inoltre $c \mid r_n, c \mid r_{n-1}$ se e solo se $c \mid r_{n-1}, c \mid r_{n-2}$. Quindi $\text{MCD}(r_{n-1}, r_{n-2}) = \text{MCD}(r_n, r_{n-1}) = r_n$. Proseguendo verso l'alto si ha $r_n = \text{MCD}(a, b)$.

B.2 Strutture algebriche: definizioni

Già nei primi anni di scuola si percepisce che le operazioni sono un potente strumento della matematica. È imparando a "fare di conto" ossia è usando le operazioni che si riescono a risolvere i problemi dai più semplici ai più complessi, e ciò vale qualunque sia l'insieme numerico in cui si lavora. Le operazioni sono tanto importanti che in ambito scolastico per giustificare la necessità di estendere un insieme numerico, fra le motivazioni di base figura l'esigenza di rendere eseguibili operazioni talvolta impossibili nell'ambito dei numeri già noti.

In matematica, definire un'***operazione*** *(binaria) in un insieme non vuoto A* significa dare *una legge che ad ogni coppia ordinata di elementi di A associ uno ed un solo elemento di A.*

Si osservi che la definizione prescinde dalla natura degli elementi di A che pertanto vengono considerati *simboli* suscettibili di assumere i più svariati significati concreti e prescinde anche dal significato concreto della operazione; inoltre la definizione evidenzia che nello stesso insieme si possono definire più operazioni.

Perché è così importante prescindere dalla natura degli elementi dell'insieme e dal significato concreto dell'operazione?

Per rispondere consideriamo l'insieme $\mathbb{Z}$ dei numeri interi e in esso l'usuale operazione "+" di addizione. Consideriamo ora le rotazioni di un quadrato, intorno al suo centro, di ampiezza $90°, 180°, 270°, 360°$ (in senso orario) e indichiamo queste, rispettivamente, con $\alpha, \beta, \gamma, \iota$. Nell'insieme $T = \{\alpha, \beta, \gamma, \iota\}$ definiamo l'operazione "$\otimes$" ponendo $x \otimes y = z$ se z è la rotazione che si ottiene eseguendo successivamente le due rotazioni x e y. Così, ad esempio, $\alpha \otimes \alpha = \beta$ perché ruotando il quadrato di 90° e poi ancora di 90° si ottiene una rotazione di 180°. È immediato verificare che le operazioni "+" e "$\otimes$" considerate rispettivamente in $\mathbb{Z}$ e T verificano le seguenti proprietà:

$(\mathbb{Z}, +)$	$(T, \otimes)$
1. $a + (b + c) = (a + b) + c$ per ogni $a, b, c \in \mathbb{Z}$	1. $a \otimes (b \otimes c) = (a \otimes b) \otimes c$ per ogni $a, b, c \in T$
2. $a + 0 = 0 + a = a$ per ogni $a \in \mathbb{Z}$	2. $a \otimes \iota = \iota \otimes a = a$ per ogni $a \in T$
3. per ogni $a \in \mathbb{Z}$ esiste $-a \in \mathbb{Z}$ tale che $a + (-a) = (-a) + a = 0$	3. per ogni $a \in T$ esiste $-a \in T$ tale che $a \otimes (-a) = (-a) \otimes a = \iota$

Gli esempi considerati mostrano che:

1. lo studio di $(\mathbb{Z}, +)$ presenta notevoli analogie con lo studio di $(T, \otimes)$;
2. se si ha l'esigenza di operare in un ambiente in cui è sufficiente che vi sia una operazione con le proprietà 1., 2., 3., allora è del tutto ininfluente considerare $(\mathbb{Z}, +)$ o $(T, \otimes)$.

Si può anche affermare che, a prescindere dalla loro natura, tra gli elementi di un insieme esistono delle connessioni definite a partire solo da proprietà formali.

Nella matematica moderna, *considerare un insieme unitamente ad una o più operazioni in esso definite*, significa considerare una **struttura algebrica**. Lo studio delle strutture algebriche formali è ciò che differenzia l'algebra

"elementare" studiata alle scuole superiori dall'algebra "astratta" studiata all'università. Tenendo presente gli esempi precedentemente riportati, si può dire che la prima *studia separatamente* le proprietà della addizione in $\mathbb{Z}$ e le proprietà delle rotazioni di un quadrato; l'algebra astratta studia *un'unica struttura algebrica* di cui $(\mathbb{Z}, +)$ e $(T, \otimes)$ sono esempi particolari. Nel caso di questi due esempi, la struttura algebrica è quella di *gruppo*.

Definizione B.2.1 *Si definisce* ***gruppo*** *la struttura algebrica* $(G, \circ)$ *costituita da un insieme non vuoto* G *in cui è definita una operazione "*$\circ$*" tale che siano soddisfatti i seguenti assiomi:*

1. $a \circ (b \circ c) = (a \circ b) \circ c$ *per ogni* $a, b, c \in G$ *(associatività);*
2. *in* G *esiste ed è unico l'elemento* u *tale che* $a \circ u = u \circ a = a$ *per ogni* $a \in G$ *(elemento neutro);*
3. *per ogni* $a \in G$*, in* G *esiste ed è unico l'elemento* $\bar{a}$ *tale che* $a \circ \bar{a} = \bar{a} \circ a = u$ *(elemento inverso).*

Se vale anche la proprietà : $a \circ b = b \circ a$ per ogni $a, b \in G$, allora il gruppo si dice **commutativo** (o **abeliano**).

La struttura algebrica di gruppo è parte fondamentale dell'algebra astratta, non solo per la rilevanza nella storia della matematica, ma per essere il fondamento delle altre strutture algebriche. Essa è stata uno strumento potente nelle ricerche sulla soluzione delle equazioni algebriche e più in generale nelle applicazioni della matematica.

È importante sottolineare che le strutture algebriche studiate e gli assiomi che le definiscono non nascono "a tavolino", ma sono considerate degne di studio quelle che raggruppano un vasto numero di casi particolari. Inoltre anche se nello stesso insieme si possono definire più operazioni, solo quelle "ricche" di proprietà permettono di "lavorare" in quell'insieme. Ecco perché, ad esempio, nell'insieme delle matrici numeriche si considera il prodotto *righe per colonne* e non si considera, in analogia a quanto si fa per la somma, il prodotto fra matrici dello stesso tipo andando a considerare il prodotto degli elementi che occupano lo stesso posto nelle due matrici da moltiplicare.

Fra le strutture algebriche definite a partire da un insieme e da due operazioni, fondamentale è quella di *campo*.

Definizione B.2.2 *Si definisce* ***campo*** *la struttura algebrica* $(K, \oplus, \circ)$ *costituita da un insieme non vuoto* K *e da due operazioni "*$\oplus$*" e "*$\circ$*" tali che siano soddisfatti i seguenti assiomi:*

1. $(K, \oplus)$ *è un gruppo commutativo;*

2. $(K^*, \circ)$ *è un gruppo commutativo (con* $K^* = K \setminus \{0\}$, 0 *elemento neutro di "*$\oplus$*");*

3. $a \circ (b \oplus c) = (a \circ b) \oplus (a \circ c)$ *per ogni* $a, b, c \in K$.

L'insieme $\mathbb{Q}$ dei numeri razionali, l'insieme $\mathbb{R}$ dei numeri reali, l'insieme $\mathbb{C}$ dei numeri complessi, rispetto alle ordinarie operazioni di addizione "$+$" e di moltiplicazione "$\cdot$", hanno la struttura algebrica di campo, mentre non ha la struttura algebrica di campo l'insieme $\mathbb{Z}$ dei numeri interi perché rispetto alla moltiplicazione non è un gruppo non essendo verificata la proprietà che ogni intero diverso da 0 ha l'inverso in $\mathbb{Z}$.

Anche quando non si considerano insiemi numerici, per semplicità di notazione, le operazioni di un campo vengono usualmente indicate con i simboli "$+$" e "$\cdot$" e denominate rispettivamente addizione e moltiplicazione. È bene però ricordare che sono simboli e denominazioni generali da non confondere con l'addizione e la moltiplicazione dell'aritmetica ordinaria. Sempre per semplicità di notazione, quando si considera l'operazione "$+$" l'elemento neutro si indica con 0, l'elemento inverso di a si indica con $(-a)$ ed è detto "opposto" di a. Quando si considera l'operazione "$\cdot$" per indicare $a \cdot b$ si scrive semplicemente ab, l'elemento neutro si indica con "1" e l'elemento inverso di a si indica con a^{-1}.

Esistono sia campi con un numero infinito di elementi come ad esempio $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, sia campi con un numero finito di elementi come ad esempio $(\mathbb{Z}_p, +, \cdot)$, p primo, dove $\mathbb{Z}_p$ ha come elementi le p classi di equivalenza della relazione[1] di "congruenza modulo p" in $\mathbb{Z}$.

Il campo $\mathbb{Q}$ dei numeri razionali è il "più piccolo" campo con un numero non finito di elementi; ricordiamo che la sua cardinalità è $\aleph_0$ (si legge "alef zero"). Se ci limitiamo a considerare i suoi elementi, sappiamo che l'insieme $\mathbb{Q}$ dei numeri razionali è sottoinsieme dell'insieme $\mathbb{R}$ dei numeri reali: $\mathbb{Q} \subset \mathbb{R}$. Ma $\mathbb{Q}$ è **sottocampo** di $\mathbb{R}$ ossia le operazioni "$+$" e "$\cdot$" che determinano in $\mathbb{R}$ la struttura di campo sono le stesse che, considerate limitatamente agli elementi di $\mathbb{Q}$, determinano in $\mathbb{Q}$ la struttura di campo.

Definizione B.2.3 *Se* $H \subset K$*, si dice che* H *è una* ***sottostruttura*** *di* K *quando le operazioni che determinano la struttura algebrica di* K*, se considerate limitatamente agli elementi di* H*, determinano in* H *la stessa struttura algebrica di* K.

[1] Fissato $n \in \mathbb{N} \setminus \{0\}$, nell'insieme $\mathbb{Z}$ la relazione di congruenza modulo n è definita da "$a \equiv b \mod n$" se e solo se $a - b = nh$, $h \in \mathbb{Z}$.

Ad esempio

1. $(\mathbb{Z}, +)$ è sottogruppo di $(\mathbb{Q}, +)$.
2. $(\mathbb{Q}^*, \cdot)$ è sottogruppo di $(\mathbb{R}^*, \cdot)$.
3. Il campo $(\mathbb{Q}, +, \cdot)$ dei numeri razionali è sottocampo del campo $(\mathbb{C}, +, \cdot)$ dei numeri complessi ed è sottocampo di ogni campo numerico contenuto in $\mathbb{C}$.
4. Il campo $(\mathbb{R}, +, \cdot)$ è sottocampo di $(\mathbb{C}, +, \cdot)$.

Poiché in seguito verrà utilizzata, ricordiamo una proprietà utile a dimostrare che H è sottocampo di K. Non occorre dimostrare tutte le proprietà che definiscono la struttura di campo, vale infatti la proprietà seguente:

Sia $K(+, \cdot)$ un campo e sia $H \subset K, H \neq \emptyset$. $H(+, \cdot)$ è un sottocampo di K se e solo se risulta

- $x - y \in H$ *per ogni* $x, y \in H$.
- $xy^{-1} \in H$ *per ogni* $x, y \in H, y \neq 0$.

Una struttura su cui poggia, in particolare, tutta la geometria, è la struttura di *spazio vettoriale*. La definizione di spazio vettoriale si differenzia da quella delle altre strutture algebriche vere e proprie nel senso che coinvolge anche una operazione di "*prodotto scalare*" che non è interna all'insieme.

Definizione B.2.4 *Sia K un campo e V un insieme non vuoto. Si dice che V è uno* ***spazio vettoriale sul campo*** *K se in V è definita una operazione "+" tale che $(V, +)$ è un gruppo commutativo ed inoltre per ogni $\alpha \in K$, $v \in V$ è definito un elemento $\alpha v \in V$ in modo tale che per ogni $\alpha, \beta \in K; v, w \in V$ si abbia*

1. $\alpha(v + w) = \alpha v + \alpha w$
2. $(\alpha + \beta)v = \alpha v + \beta v$
3. $\alpha(\beta v) = (\alpha\beta)v$
4. $1v = v$, *con* 1 *elemento neutro di K rispetto la moltiplicazione*

Gli elementi di V sono usualmente denominati *vettori*.

Si faccia attenzione che nell'assioma 1. l'operazione "+" è quella di V, mentre nell'assioma 2. l'operazione di "+" del primo membro è quella di K e l'operazione di "+" al secondo membro è quella di V.

Esempio B.2.5 Sia V l'insieme delle n–ple $(a_1, a_2, \ldots, a_n)$ ad elementi in un campo $(K, +, \cdot)$. V è un gruppo commutativo rispetto all'operazione:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

Definiamo ora l'operazione "prodotto scalare" ponendo per ogni $\alpha \in K$:

$$\alpha(a_1, a_2, \ldots, a_n) = (\alpha a_1, \alpha a_2, \ldots, \alpha a_n)$$

È immediato verificare che rispetto a queste operazioni V è uno spazio vettoriale su K.

Definizione B.2.6 *Sia V uno spazio vettoriale su K e siano $v_1, v_2, \ldots, v_n$ elementi di V ($n \in \mathbb{N} \setminus \{0\}$)*

1. *Un elemento di V della forma $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$ con $\alpha_i \in K$, $i = 1, \ldots, n$, si chiama **combinazione lineare** su K dei vettori $v_1, v_2, \ldots, v_n$.*

2. *Si dice che $v_1, v_2, \ldots, v_n$ sono **linearmente dipendenti** su K se esistono $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ non tutti nulli tali che $\lambda_1 v_1 + \lambda_2 v_2 + \ldots + \lambda_n v_n = 0$. Se i vettori non sono linearmente dipendenti su K essi si dicono **linearmente indipendenti** su K.*

Definizione B.2.7 *Sia V uno spazio vettoriale su K. Un sottoinsieme B di V si chiama **base** di V se ogni vettore di V si può esprimere in uno ed un sol modo come combinazione lineare di un numero finito di elementi del sottoinsieme B. L'insieme B può avere un numero finito di elementi, ma può anche avere infiniti elementi.*

Si può dimostare che uno spazio vettoriale, non formato dal solo vettore nullo, è sempre dotato di una base (finita o infinita). Inoltre la cardinalità di due basi diverse è sempre la stessa. Questa importante proprietà permette di dare la seguente definizione.

Definizione B.2.8 *Sia B una base dello spazio vettoriale V. Si chiama **dimensione** di V la cardinalità dell'insieme B, e si indica con* $\dim(V)$.

Lo spazio vettoriale dell'Esempio B.2.5 è uno spazio vettoriale di dimensione finita n. Una sua base è l'insieme

$$B = \{(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0), (0, 0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 0, 1)\}$$

Il prossimo esempio mostra che esistono spazi vettoriali di dimensione infinita.

Esempio B.2.9 Sia $\mathbb{R}[x]$ l'insieme dei polinomi di grado qualunque a coefficienti reali. Tale insieme, con le consuete operazioni di addizione di polinomi e di moltiplicazione di un polinomio per un numero reale, è uno spazio vettoriale. Tale spazio non può essere dotato di una base formata da un numero finito di elementi. Infatti, dato un numero n di questi polinomi, qualsiasi combinazione lineare di essi è un polinomio di grado minore od uguale al grado massimo degli n polinomi. Tali polinomi non possono quindi generare tutto $\mathbb{R}[x]$. I polinomi $1, x, x^2, x^3, x^4, \ldots$ formano una base infinita di $\mathbb{R}$. ■

Nello studio delle strutture algebriche è fondamentale la nozione di *isomorfismo* fra strutture algebriche dello stesso tipo. Prima di dare la definizione, introduciamo questa nozione attraverso la considerazione di semplici esempi da cui si può già intuire che due strutture algebriche sono isomorfe se, con una espressione grossolana, una non è altro che la copia dell'altra e quindi in questo senso "uguali".

Iniziamo prendendo in esame la struttura di gruppo. Consideriamo il gruppo $(T, \otimes)$ delle rotazioni di un quadrato in se stesso, già illustrato precedentemente, ricordiamo che $T = \{\alpha, \beta, \gamma, \iota\}$ con $\alpha, \beta, \gamma, \iota$ rotazioni rispettivamente di $90°, 180°, 270°, 360°$.

Consideriamo ora il gruppo $(H, \cdot)$ i cui elementi sono le radici di $x^4 - 1 = 0$ e l'operazione è l'ordinaria moltiplicazione di $\mathbb{R}$; $H = \{1, -1, i, -i\}$ dove $i = \sqrt{-1}$.

Indichiamo con $f : T \to H$ la corrispondenza che agisce in questo modo: $f(\alpha) = i, f(\beta) = -1, f(\gamma) = -i, f(\iota) = 1$.

La f è banalmente una corrispondenza biunivoca (corrispondenza uno a uno) ma è anche verificato che $f(x \otimes y) = f(x) \cdot f(y)$ qualunque siano $x, y \in T$. Ad esempio $f(\alpha \otimes \beta) = f(\gamma) = -i$, d'altra parte $f(\alpha)f(\beta) = i \cdot (-1) = -i$ e dunque $f(\alpha \otimes \beta) = f(\alpha) \cdot f(\beta)$.

L'esistenza di questa corrispondenza f ci assicura che $(T, \otimes)$ e $(H, \cdot)$ sono due gruppi "identici", differiscono solo per la denominazione degli elementi.

Definizione B.2.10 *Due gruppi $(G, \circ)$ e $(G', \bullet)$ sono **isomorfi** se fra gli elementi di G e gli elementi di G' esiste una corrispondenza biunivoca f tale che per ogni $g_1, g_2 \in G$ si abbia: $f(g_1 \circ g_2) = f(g_1) \bullet f(g_2)$*

Definizione B.2.11 *Due campi $(K, +, \cdot)$ e $(H, +, \cdot)$ sono **isomorfi** se fra gli elementi di K e gli elementi di H esiste una corrispondenza biunivoca f tale che si abbia*

1. $f(x + y) = f(x) + f(y)$ *per ogni* $x, y \in K$
2. $f(x \cdot y) = f(x)f(y)$ *per ogni* $x, y \in K^* = K \setminus \{0\}$

Esempio B.2.12

1. Sia $(\mathbb{R}^*, \cdot)$ il gruppo dei numeri reali positivi rispetto alla usuale moltiplicazione. Sia $(L, +)$ il gruppo i cui elementi sono i logaritmi naturali dei reali positivi e l'operazione di "+" è l'ordinaria addizione fra logaritmi ($\log x + \log y = \log xy$). I due gruppi $(\mathbb{R}^*, \cdot)$ e $(L, +)$ sono isomorfi perché la corrispondenza $f : \mathbb{R}^* \to L$ definita da $f(x) = \log x$ è un isomorfismo essendo biunivoca e tale che $f(xy) = f(x) + f(y)$ per ogni $x, y \in \mathbb{R}^*$.

2. Sia $(\mathbb{C}, +, \cdot)$ il campo dei numeri complessi e sia $(\mathbb{R}^2, +, \cdot)$ il campo i cui elementi sono le coppie di numeri reali e le operazioni sono le usuali operazioni di "+" e "$\cdot$" definite da :

$$(a, b) + (c, d) = (a + c, b + d)$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

   Indichiamo con $f : \mathbb{C} \to \mathbb{R}^2$ la corrispondenza definita da $f(a + ib) = (a, b)$. Questa corrispondenza è banalmente biunivoca ed è tale che

   1. $f(x + y) = f(x) + f(y)$ per ogni $x, y \in \mathbb{C}$
   2. $f(xy) = f(x)f(y)$ per ogni $x, y \in \mathbb{C}^*$

   L'esistenza di questa corrispondenza f ci assicura che i due campi sono isomorfi ossia considerare il campo $(\mathbb{C}, +, \cdot)$ oppure considerare il campo $(\mathbb{R}^2, +, \cdot)$ è la "stessa cosa". ■

In analogia a quanto definito per i gruppi ed i campi, qualunque sia il tipo di struttura algebrica considerata, un isomorfismo fra due di esse è una corrispondenza biunivoca che *conserva le operazioni* e che, pertanto, ci permette di dire che le due strutture sono "uguali" anche se rappresentate con simboli e operazioni diverse. La nozione di strutture algebriche isomorfe, ossia di strutture uguali in senso astratto, è importante anche perché la dimostrazione di un teorema è talvolta facilitata se si passa da una struttura ad una sua struttura isomorfa.

Automorfismi del campo $\mathbb{C}$ dei complessi

Si parla di automorfismo quando si considera un isomorfismo di una struttura algebrica in se stessa. Parliamo dunque degli isomorfismi del campo $\mathbb{C}$ dei numeri complessi in se stesso. Sia $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}, i^2 = -1\}$, quando si parla degli automorfismi di $\mathbb{C}$, di norma, si indicano sempre solo due automorfismi:

1. **Automorfismo identità** che ad ogni elemento associa se stesso:
   $\varphi_1 \ : \ a + ib \to a + ib$

2. **Automorfismo coniugio** che ad un elemento associa il suo coniugato:
   $\varphi_2 \ : \ a + ib \to a - ib$

Si faccia attenzione che però questi due automorfismi non sono i soli automorfismi di $\mathbb{C} = \mathbb{R}(i)$, infatti il gruppo di tutti gli automorfismi di $\mathbb{C}$ è infinito, più precisamente ha cardinalità $2^{|\mathbb{R}|}$ (Gabelli, 2008, p. 225). Gli automorfismi φ_1 e φ_2 sono **i soli automorfismi** di $\mathbb{C}$ che hanno la proprietà di fissare i numeri reali, ossia per ogni $r \in \mathbb{R}$, si ha $\varphi_1(r) = \varphi_2(r) = r$.

Questi due automorfismi sono particolarmente importanti perché ricordiamo che la svolta che ha permesso di risolvere completamente il problema di determinare quali sono le equazioni algebriche risolubili per radicali, è proprio l'aver considerato gli automorfismi che fissano gli elementi del campo dei coefficienti dell'equazione.

B.3 Estensione di un campo

In questa sezione riportiamo alcune nozioni relative ai campi che non solo sono utili per la comprensione di varie parti di questo volume, ma sono basilari per il prossimo paragrafo dedicato alla costruzione di un numero reale con riga e compasso. L'esposizione è arricchita con applicazioni ai campi numerici mediante esempi e osservazioni di tipo anche didattico. Per uno studio più approfondito e completo sull'estensione di un campo, si rinvia a Dikranjan e Lucido (2007).

Dato un qualunque campo $K(+, \cdot)$:

- comunque presi $a, b \in K$, si ha $ab = 0$ se e solo se $a = 0$ oppure $b = 0$; segue immediatamente dagli assiomi che definiscono il campo;

- se $n \in \mathbb{N}^*$ e $a \in K$, con la scrittura "$n \cdot a$" si intende la somma di n addendi uguali ad a, ossia

$$n \cdot a = na = \underbrace{a + a + \cdots + a}_{n \text{ addendi}}$$

  Si faccia attenzione che il simbolo "$\cdot$" di $n \cdot a$ non è da confondere con l'operazione "$\cdot$" del campo $K(+, \cdot)$.

Teorema B.3.1 *Sia $K(+,\cdot)$ un campo in cui esiste un elemento $a \in K^*$ tale che $ta = 0$, $t \in \mathbb{N}^*$. Indicato con n il più piccolo intero positivo per cui $na = 0$, risulta $nb = 0$ per ogni $b \in K^*$.*

DIMOSTRAZIONE. Sia $a \in K^*$ tale che $na = 0$, con n minimo intero positivo per cui ciò accade. Qualunque sia $b \in K^*$, da $na = 0$ segue $(na)b = 0$ e quindi

$$(\underbrace{a + a + \cdots + a}_{n \text{ addendi}})b = \underbrace{ab + ab + \cdots + ab}_{n \text{ addendi}} = a(\underbrace{b + b + \cdots + b}_{n \text{ addendi}}) = a(nb) = 0$$

da cui $nb = 0$. Se esistesse anche $m < n, m \in \mathbb{N}^*$, tale che $mb = 0$ seguirebbe (procedendo come sopra) $ma = 0$ contro l'ipotesi di minimalità fatta su n. ■

Il teorema precedente permette di dare la seguente definizione:

Definizione B.3.2 *Si dice che un campo K ha* ***caratteristica*** *0 se $na \neq 0$ per ogni $n \in \mathbb{N}^*$ e ogni $a \in K^*$. Si dice che K ha* ***caratteristica*** *$n > 0$ se n è il più piccolo intero positivo per cui $na = 0$ per ogni $a \in K^*$.*

Teorema B.3.3 *La caratteristica di un campo K è zero oppure è un numero primo.*

DIMOSTRAZIONE. Sia K un campo di caratteristica $n \neq 0$. Se n non è primo, sia $n = r \cdot s,\ 1 < r, s < n$. Considerato $a \in K^*$, da $na = 0$ si avrebbe $(rs)a = 0,\ r(sa) = 0$. Se $sa = 0$ si ha un assurdo perché $s < n$; se $sa \neq 0$ si ha un assurdo perché $r < n$. Rimane così provato che deve essere n numero primo. ■

Osservazione B.3.4 Se un campo è finito allora la sua caratteristica è certamente un numero finito $p \neq 0$, ma non vale il viceversa, ossia non è vero che se un campo ha caratteristica finita esso abbia un numero finito di elementi. Ad esempio il campo delle funzioni razionali a coefficienti in $\mathbb{Z}_p$ è infinito ma ha caratteristica finita p. Se un campo ha caratteristica 0 allora il campo ha certamente un numero infinito di elementi.

Osservazione B.3.5 Tutti i campi numerici hanno caratteristica 0. Hanno dunque caratteristica 0 il campo $\mathbb{C}$ dei numeri complessi, il campo $\mathbb{R}$ dei numeri reali e tutti i sottocampi di $\mathbb{R}$. In particolare ha caratteristica 0 *il campo $\mathbb{Q}$ dei numeri razionali* che, come si verifica facilmente, *è contenuto, a meno di isomorfismi, in un qualunque campo di caratteristica* 0.

Nello studio di una teoria matematica è importante determinare quale è l'ambiente minimo in cui essa ha senso e trova giustificazione. Se, ad esempio, consideriamo la teoria delle equazioni algebriche,[2] il teorema fondamentale dell'algebra ci assicura che nel campo dei numeri complessi esistono tutte le soluzioni di una qualunque equazione algebrica, ma rimane il problema di determinare quale è il più piccolo campo in cui una determinata equazione ammette tutte le soluzioni. Se ad esempio consideriamo l'equazione $x^2 + 7 = 0$, nel campo $\mathbb{Q}$ dei numeri razionali essa non ha nessuna soluzione, ma nel campo $\mathbb{R}$ dei numeri reali troviamo entrambe le sue soluzioni : $\sqrt{7}$ e $-\sqrt{7}$. Il campo $\mathbb{R}$ non è però il più piccolo campo contenente $\sqrt{7}$ e $-\sqrt{7}$. Infatti se consideriamo l'insieme $\mathbb{Q}(\sqrt{7}) = \{a + b\sqrt{7} \mid a, b \in \mathbb{Q}\}$ e in esso consideriamo le operazioni "+" e "$\cdot$" così definite:

$$(a + b\sqrt{7}) + (c + d\sqrt{7}) = (a + c) + (b + d)\sqrt{7}$$

$$(a + b\sqrt{7}) \cdot (c + d\sqrt{7}) = (ac + 7bd) + (ad + bc)\sqrt{7}$$

è facile verificare che $(\mathbb{Q}(\sqrt{7}), +, \cdot)$ è un campo, e poiché $\sqrt{7}$ e $-\sqrt{7}$ sono elementi del campo, significa che l'equazione $x^2 + 7 = 0$ ammette in $\mathbb{Q}(\sqrt{7})$ tutte le soluzioni, anzi $\mathbb{Q}(\sqrt{7})$ è il più piccolo campo contenente $\sqrt{7}$ e $-\sqrt{7}$.

Tenendo presente gli esempi di sottocampi già incontrati, appare naturale la seguente definizione

Definizione B.3.6 Si chiama ***estensione*** *(o* ***ampliamento****)* di un campo $(K, +, \cdot)$ un qualunque campo $(L, +, \cdot)$ che contenga K come sottocampo.

Abbiamo già ricordato che $\mathbb{Q}$ è il "più piccolo" campo con un numero infinito di elementi, ora possiamo precisare che ogni campo di caratteristica zero è estensione del campo dei razionali (ossia "contiene" il campo dei razionali). In particolare, $\mathbb{Q}$ è sottocampo di tutti i sottocampi del campo $\mathbb{R}$ dei numeri reali perché questi sono tutti campi di caratteristica 0.

Ogni campo L, rispetto alle sue due operazioni, si può pensare come spazio vettoriale sopra un suo qualunque sottocampo K e come tale L avrà una sua dimensione.

Definizione B.3.7 *Sia K un campo e sia L una sua estensione. Si definisce* ***grado di*** *L su K, e si indica con $[L : K]$, la dimensione di L come spazio vettoriale su K.*

[2] Con *equazione algebrica* si intende una equazione a coefficienti razionali; si può anche dire a coefficienti interi perché, per esempio, $\frac{1}{3}x^2 + \frac{1}{5}x - 1 = 0$ si può scrivere come $5x^2 + 3x - 15 = 0$.

Ovviamente si ha $[L : K] = 1$ se e solo se $L = K$.

Esempio B.3.8 Il campo $\mathbb{C}$ dei numeri complessi ha grado 2 rispetto al campo $\mathbb{R}$ dei numeri reali: $[\mathbb{C} : \mathbb{R}] = 2$; una base è $\{1, i\}$.

Esempio B.3.9 Il campo $\mathbb{R}$ dei numeri reali ha grado infinito rispetto al campo $\mathbb{Q}$ dei numeri razionali: $[\mathbb{R} : \mathbb{Q}] = \infty$. Infatti, se esistesse una base finita di $\mathbb{R}$ su $\mathbb{Q}$, esisterebbe un numero finito n di numeri reali tali che ogni numero reale sarebbe combinazione lineare di questi n numeri reali a coefficienti razionali; siccome queste combinazioni lineari sono un insieme numerabile (Fiori e Invernizzi, 2009), si ha un assurdo.

Definizione B.3.10 *Una estensione L del campo K si dice* ***estensione algebrica*** *se il grado $[L : K]$ è finito, si dice* ***estensione trascendente*** *se il grado $[L : K]$ è infinito.*

Quando L ha dimensione finita su K, si dice anche che L è una **estensione finita di** K e si ha il seguente importante teorema.

Teorema B.3.11 *Se L è una estensione finita di K e M è una estensione finita di L allora M è una estensione finita di K e risulta*

$$[M : K] = [M : L] \cdot [L : K]$$

Dimostrazione. Sia $[M : L] = m, [L : K] = n$ e siano $X = \{x_1, x_2, \ldots, x_m\}$ una base di M su L e $Y = \{y_1, y_2, \ldots, y_n\}$ una base di L su K. Dimostreremo che l'insieme degli elementi ottenuti moltiplicando fra loro gli elementi di X con quelli di Y, risulta essere una base di M su K.

(a) *Gli elementi $x_i y_j$ sono generatori di M.* Infatti sia v un qualunque elemento di M. Allora v è combinazione lineare degli elementi di X a coefficienti in L:

$$v = l_1 x_1 + l_2 x_2 + \ldots + l_m x_m = \sum_{i=1}^{m} l_i x_i, \quad l_i \in L.$$

D'altra parte, essendo Y una base di L su K, ogni l_i si scrive come combinazione lineare degli elementi di Y a coefficienti in K. Risulta pertanto

$$v = \sum_{i=1}^{m} \Big(\sum_{j=1}^{n} a_{ij} y_j \Big) x_i = \sum_{i,j} a_{ij} y_j x_i \ , \quad a_{ij} \in K$$

(b) *Gli $x_i y_i$ sono linearmente indipendenti su K.* Infatti se

$$\sum_{i,j} a_{ij}(y_j x_i) = 0, \quad a_{ij} \in K$$

allora si ha

$$0 = \sum_{i=1}^{m} \Big(\underbrace{\sum_{j=1}^{n} a_{ij} y_j}_{\in L} \Big) x_i$$

da cui, per la indipendenza degli x_i su L,

$$\sum_{j=1}^{n} a_{ij} y_j = 0.$$

Poiché gli y_j sono indipendenti su K, segue che $a_{ij} = 0$ per ogni i, j. ■

Osservazione B.3.12 Il teorema assicura che non vi può essere nessun campo contenuto in $\mathbb{C}$ e contenente $\mathbb{R}$. Se infatti fosse $\mathbb{C} \supset \mathbb{H} \supset \mathbb{R}$, poiché $[\mathbb{C} : \mathbb{R}] = 2$ dovrebbe essere o $[\mathbb{C} : \mathbb{H}] = 1$ oppure $[\mathbb{H} : \mathbb{R}] = 1$ e dunque o $\mathbb{C} = \mathbb{H}$ oppure $\mathbb{H} = \mathbb{R}$.

Osservazione B.3.13 Considerato $\mathbb{R}$ sappiamo che le coppie di numeri reali formano un campo: $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Ma formano un campo anche le quaterne di numeri reali, è il campo dei quaternioni $Q_u = \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}$. Poiché $Q_u \supset \mathbb{C} \supset \mathbb{R}$ e $[\mathbb{C} : \mathbb{R}] = 2$, $[Q_u : \mathbb{R}] = 4$, il teorema assicura che fra $\mathbb{C}$ e Q_u non può esserci nessun campo e pertanto, per esempio, le terne di numeri reali non costituiscono un campo a differenza delle coppie e delle quaterne. Le terne di numeri reali costituiscono però uno spazio vettoriale.

B.3.1 Estensione semplice

Dato un campo K e un suo ampliamento L, è importante vedere come si possono costruire degli ampliamenti intermedi tra K ed L.

Il caso più semplice consiste nell'*aggiungere* a K un solo elemento α di L. Ossia considerare il più piccolo sottocampo di L che contenga sia K che α. In questo caso si parla di **estensione semplice** di K e viene indicata con $K(\alpha)$. Vediamo che forma hanno gli elementi di questa estensione.

Teorema B.3.14 *Sia L una estensione di K e sia $\alpha \in L$. Allora*

$$K(\alpha) = \left\{ \frac{a_0 + a_1\alpha + \ldots + a_n\alpha^n}{b_0 + b_1\alpha + \ldots + b_m\alpha^m} \mid a_i, b_i \in K; n, m \in \mathbb{N}; \sum_{k=0}^{m} b_k \alpha^k \neq 0 \right\}$$

DIMOSTRAZIONE. Consideriamo l'insieme

$$A = \left\{ \frac{a_0 + a_1\alpha + \ldots + a_n\alpha^n}{b_0 + b_1\alpha + \ldots + b_m\alpha^m} \mid a_i, b_i \in K; n, m \in N; \sum_{k=0}^{m} b_k\alpha^k \neq 0 \right\}$$

È immediato verificare che A è un campo che contiene K ed α e pertanto $K(\alpha) \subseteq A$. D'altra parte un qualunque campo contenente K ed α contiene anche gli elementi del tipo $\dfrac{a_0 + a_1\alpha + \ldots + a_n\alpha^n}{b_0 + b_1\alpha + \ldots + b_m\alpha^m}$ e pertanto $A \subseteq K(\alpha)$. Si conclude $K(\alpha) = A$. ■

Esempio B.3.15 Sia $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt{2}$. Risulta

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a_0 + a_1\sqrt{2} + \ldots + a_n(\sqrt{2})^n}{b_0 + b_1\sqrt{2} + \ldots + b_m(\sqrt{2})^m} \mid a_i, b_i \in \mathbb{Q}; n, m \in \mathbb{N}; \sum_{k=0}^{m} b_k(\sqrt{2})^k \neq 0 \right\}.$$

Ma $(\sqrt{2})^2 = 2$, allora le espressioni degli elementi di $\mathbb{Q}(\sqrt{2})$ si riducono e si ottiene

$$\mathbb{Q}(\sqrt{2}) = \left\{ \frac{a_0 + a_1\sqrt{2}}{b_0 + b_1\sqrt{2}} \mid a_i, b_i \in \mathbb{Q}; b_0 + b_1(\sqrt{2}) \neq 0 \right\}.$$

Ma poiché $\dfrac{1}{b_0 + b_1\sqrt{2}} = \dfrac{b_0 - b_1\sqrt{2}}{b_0^2 - 2b_1^2} = \dfrac{b_0}{b_0^2 - 2b_1^2} - (\dfrac{b_1}{b_0^2 - 2b_1^2})\sqrt{2}$

con $\dfrac{b_0}{b_0^2 - 2b_1^2}, \dfrac{b_1}{b_0^2 - 2b_1^2} \in \mathbb{Q}$, l'espressione degli elementi di $\mathbb{Q}\sqrt{2}$ si semplifica ulteriormente e si possono scrivere tutti nella forma $q_0 + q_1\sqrt{2}$ con $q_0, q_1 \in \mathbb{Q}$. In definitiva si ha

$$\mathbb{Q}\sqrt{2} = \left\{ a_0 + a_1\sqrt{2} \,|\, a_i \in \mathbb{Q} \right\}$$

Esempio B.3.16 Sia $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \pi$. Risulta

$$\mathbb{Q}(\pi) = \left\{ \frac{a_0 + a_1\pi + \ldots + a_n\pi^n}{b_0 + b_1\pi + \ldots + b_m\pi^m} \mid a_i, b_i \in \mathbb{Q}; n, m \in \mathbb{N}; \sum_{k=0}^{m} b_k\pi^k \neq 0 \right\}$$

A differenza dell'esempio precedente, non si può "razionalizzare" e pertanto le espressioni degli elementi di $\mathbb{Q}(\pi)$ non si possono semplificare.

Le estensioni semplici dei due esempi precedenti mostrano comportamenti diversi. Nell'Esempio B.3.15 le espressioni degli elementi possono essere semplificate mentre nell'Esempio B.3.16 questo non è possibile. Il motivo della diversità di comportamento è dovuto alla *diversa natura* dell'elemento α che si sta "aggiungendo".

Indichiamo con $K[x]$ l'insieme dei polinomi in x a coefficienti in K: $f(x) \in K[x]$ se $f(x) = a_0 + a_1x + \ldots + a_nx^n$ con $a_i \in K, i = 0, \ldots, n$.

Definizione B.3.17 *Sia $K \subset L$ una estensione di campi. Un elemento $\alpha \in L$ si dice **algebrico su** K se esiste un polinomio $f(x) \in K[x], f(x) \neq 0$, tale che $f(\alpha) = 0$. In caso contrario si dice che α è **trascendente su** K.*

Esempio B.3.18

1. $\sqrt{2}$ è algebrico su $\mathbb{Q}$ perché è radice del polinomio $x^2 - 2 \in \mathbb{Q}[x]$.

2. e è trascendente rispetto a $\mathbb{Q}$ (Teorema di Hermite).

3. π è trascendente rispetto a $\mathbb{Q}$ (Teorema di Lindemann).

4. π è algebrico su $\mathbb{R}$ perché è radice del polinomio $x - \pi \in \mathbb{R}[x]$.

In matematica, quando si parla di **numeri algebrici** e **numeri trascendenti** si intendono gli elementi di $\mathbb{C}$ che sono **algebrici o trascendenti su** $\mathbb{Q}$.

Sappiamo che tutti i numeri reali, eccettuata una quantità numerabile di essi (gli algebrici), sono trascendenti (Fiori e Invernizzi, 2009, p. 133). Malgrado ciò, come si è visto nei Capitoli 3 e 4, è da un lato relativamente abbastanza semplice produrre esempi *espliciti* di numeri trascendenti, ad esempio i numeri di Liouville, ma può rivelarsi piuttosto difficile dimostrare che un numero reale α assegnato a priori, come e o π, è trascendente (se lo è davvero).

Nel caso generale siamo però talvolta aiutati dal fatto che, considerata un'estensione semplice $K(\alpha)$, l'essere $[K(\alpha) : K]$ finito o infinito caratterizza l'essere α algebrico o trascendente su K. Infatti, come verrà mostrato nel Teorema B.3.23, si ha che:

1. *α è algebrico su K se e solo se $K(\alpha)$ è un'estensione finita.*

2. *Le estensioni $K(\alpha)$ con α trascendente su K sono estensioni infinite (tutte isomorfe tra loro).*

Per la 2., se $K(\alpha)$ è un'estensione trascendente, si può riguardare l'elemento α come una indeterminata x; in questo caso $K(\alpha)$ si "identifica" con le funzioni razionali nella indeterminata x:

$$K(x) = \left\{ \frac{a_0 + a_1 x + \ldots + a_n x^n}{b_0 + b_1 x + \ldots + b_m x^m} \mid a_i, b_i \in K; n, m \in \mathbb{N}; \sum_{k=0}^{m} b_k x^k \neq 0 \right\}$$

B.3.2 Estensioni algebriche

Sia $K \subset L$, $\alpha \in L$, α algebrico rispetto a K. Fra i polinomi di $K[x]$ che ammettono α come radice particolare importanza hanno i polinomi di grado minimo e fra questi quello in cui il coefficiente del termine di grado massimo (altrimenti detto *coefficiente direttore*) è 1; esso è detto **polinomio minimo di** α.

Definizione B.3.19 *Se $\alpha \in L$ è algebrico rispetto a K, si dice **grado** di α il grado del suo polinomio minimo.*

Esempio B.3.20

- i è algebrico di grado 2 su $\mathbb{Q}$; il suo polinomio minimo è $x^2 + 1 \in \mathbb{Q}[x]$.
- $\sqrt{2}$ è algebrico di grado 2 su $\mathbb{Q}$; il suo polinomio minimo è $x^2 - 2 \in \mathbb{Q}[x]$.
- $\sqrt[3]{2}$ è algebrico di grado 3 su $\mathbb{Q}$; il suo polinomio minimo è $x^3 - 2 \in \mathbb{Q}[x]$.

Definizione B.3.21 *Un numero reale α irrazionale e algebrico su $\mathbb{Q}$ di grado 2, è detto **irrazionale quadratico**.*

Come dimostrato nel Teorema 2.7.1, lo sviluppo in frazione continua di un numero reale α è definitivamente periodico se e solo se α è algebrico su $\mathbb{Q}$ di grado 2.

Definizione B.3.22 Sia $K \subset L$ un'estensione di campi. L'estensione è detta ***estensione algebrica*** se ogni elemento di L è algebrico su K.

Il prossimo Teorema B.3.23 assicura che le Definizioni B.3.10 e B.3.22 di estensione algebrica sono equivalenti.

Come già anticipato con gli Esempi B.3.15 e B.3.16, la diversa natura dell'elemento α si riflette sulla struttura dell'estensione semplice $K(\alpha)$ di un campo K.

Il seguente teorema chiarisce completamente la questione e mostra il legame fra estensioni algebriche ed estensioni finite.

Teorema B.3.23 *Sia $K \subset L$ una estensione di campi. Si ha*

1. *Se $\alpha \in L$ è algebrico di grado finito n su K allora*

$$K(\alpha) = \left\{ a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in K \right\}$$

2. *Se L è estensione finita allora L è estensione algebrica.*

3. *$\alpha \in L$ è algebrico di grado n rispetto K se e solo se $[K(\alpha) : K] = n$.*

DIMOSTRAZIONE. 1. Sia $p(x) = h_0 + h_1x + \ldots + h_{n-1}x^{n-1} + x^n$ il polinomio minimo di α, $p(\alpha) = 0$. Indichiamo con $\overline{K}(\alpha)$ l'insieme $\overline{K}(\alpha) = \{a_0 + a_1\alpha + \ldots, a_{n-1}\alpha^{n-1} \mid a_i \in K\}$ e dimostriamo che $\overline{K}(\alpha)$ è il più piccolo sottocampo di L contenente K ed α, ossia è l'estensione semplice di K tramite α. Per dimostrare che $\overline{K}(\alpha)$ è un campo occorre provare che

(i) $a - b \in \overline{K}(\alpha)$ per ogni $a, b \in \overline{K}(\alpha)$.

(ii) $ab^{-1} \in \overline{K}(\alpha)$ per ogni $a, b \in \overline{K}(\alpha), b \neq 0$.

La (i) segue immediatamente dalla definizione di $\overline{K}(\alpha)$.
Per provare la (ii) proviamo anzitutto che per ogni $b \in \overline{K}(\alpha), b \neq 0$, esiste $b^{-1} \in \overline{K}(\alpha)$. Sia $b = b_0 + b_1\alpha + \ldots, b_{n-1}\alpha^{n-1}$, allora il polinomio $h(x) = b_0 + b_1x + \ldots, b_{n-1}x^{n-1} \in K[x]$ è tale che $h(\alpha) = b \neq 0$ e quindi, poiché il $\text{MCD}(h(x), p(x))$ è un divisore del polinomio minimo $p(x)$, deve essere necessariamente $\text{MCD}(h(x), p(x)) = 1$ oppure $\text{MCD}(h(x), p(x)) = p(x)$. Se fosse $\text{MCD}(h(x), p(x)) = p(x)$ si avrebbe che $p(x)$ divide $h(x)$ e quindi $h(\alpha) = 0$ e ciò è assurdo perché $h(\alpha) = b \neq 0$. Deve dunque essere $\text{MCD}(h(x), p(x)) = 1$; allora esistono $\lambda(x), \mu(x) \in K[x]$ tali che $\lambda(x)p(x) + \mu(x)h(x) = 1$. Posto $\mu(x) = p(x)q(x) + r(x)$ si ottiene $\lambda(x)p(x) + p(x)q(x)h(x) + r(x)h(x) = 1$ da cui $\lambda(\alpha)p(\alpha) + p(\alpha)q(\alpha)h(\alpha) + r(\alpha)h(\alpha) = 1$ e quindi (ricordando che $p(\alpha) = 0$), si ha $r(\alpha)h(\alpha) = 1$. Poiché $h(\alpha) = b$, da $1, b \in \overline{K}(\alpha)$ segue $r(\alpha) \in \overline{K}(\alpha)$ e $r(\alpha) \cdot b = 1$ assicura che in $\overline{K}(\alpha)$ esiste l'inverso dell'elemento b, ossia $r(\alpha) = b^{-1} \in \overline{K}(\alpha)$.
Per dimostrare che $ab^{-1} \in \overline{K}(\alpha)$ per ogni $a, b \in \overline{K}(\alpha)$, basta ora dimostrare che il prodotto di due elementi di $\overline{K}(\alpha)$ è ancora un elemento di $\overline{K}(\alpha)$, ma questo segue immediatamente dal fatto che poiché $p(\alpha) = 0$ si ha $\alpha^n = -h_0 - h_1\alpha - \ldots - h_{n-1}\alpha^{n-1}$. Rimane così provato che $\overline{K}(\alpha)$ è un campo.
Infine, per come definito $\overline{K}(\alpha)$, si ha $K \subseteq \overline{K}(\alpha)$ e $\alpha \in \overline{K}(\alpha)$. Inoltre ogni campo che contenga sia K sia α deve contenere gli elementi del tipo α^t e dunque anche gli elementi del tipo $h_0 + h_1\alpha + \ldots + h_{n-1}\alpha^{n-1}$, si può pertanto

affermare che $\overline{K}(\alpha)$ è il più piccolo campo che contiene sia K sia α e dunque risulta $\overline{K}(\alpha) = K(\alpha)$.

2. Sia $[L : K] = n$, L è spazio vettoriale su K di dimensione n e quindi $(n+1)$ vettori di L sono linearmente dipendenti rispetto K. Sia $v \in L; v^0, v^1, \ldots, v^n \in L$ e perciò esistono $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$ tali che $\lambda_0 v^0 + \lambda_1 v^1 + \ldots, \lambda_n v^n = 0$. Allora in $K[x]$ esiste il polinomio $g(x) = \lambda_0 x^0 + \lambda_1 x^1 + \ldots, \lambda_n x^n \in K[x]$ che ammette v come radice e pertanto v è algebrico rispetto K.

3. Sia $\alpha \in L$ algebrico di grado n rispetto K. Per (1) si ha $K(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in K\}$. Gli elementi di $K(\alpha)$ sono combinazioni lineari di $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ a coefficienti in K. Ma $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ sono una base di $K(\alpha)$ perché sono linearmente indipendenti, infatti se per $\lambda_i \in K, i = 0, 1, \ldots, n-1$, si ha $\lambda_0 + \lambda_1\alpha^1 + \ldots + \lambda_{n-1}\alpha^{n-1} = 0$, il polinomio $g(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_{n-1}x^{n-1} \in K[x]$ ammette α come radice e poiché α è algebrico di grado n non esistono polinomi con grado minore di n che ammettono α come radice e dunque $g(x) = 0$ da cui $\lambda_0 = \lambda_1 = \ldots = \lambda_{n-1} = 0$. Rimane così provato che $[K(\alpha) : K] = n$.
Viceversa, sia $[K(\alpha) : K] = n$; proviamo che ogni elemento $\alpha \in K(\alpha)$ è algebrico di grado n rispetto K. Consideriamo gli $(n+1)$ elementi $\alpha^0, \alpha^1, \ldots, \alpha^n \in K(\alpha)$; poiché $K(\alpha)$ ha dimensione n su K, essi sono linearmente dipendenti e perciò esistono $\lambda_0, \lambda_1, \ldots, \lambda_n \in K$ non tutti nulli tali che $\lambda_0\alpha^0 + \lambda_1\alpha^1 + \ldots + \lambda_n\alpha^n = 0$. Allora il polinomio $g(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n \in K[x]$ è diverso da zero perché i suoi coefficienti non sono tutti nulli ed è tale che $g(\alpha) = 0$ e pertanto α è algebrico rispetto K. ■

Esempio B.3.24 $\mathbb{Q}(\sqrt[3]{2}) = \left\{a_0 + a_1(\sqrt[3]{2}) + a_2(\sqrt[3]{2})^2 \mid a_i \in \mathbb{Q}\right\}$ perché $\sqrt[3]{2}$ è algebrico di grado 3 su $\mathbb{Q}$ essendo $x^3 - 2$ il polinomio minimo di cui è radice.

Esempio B.3.25 $\mathbb{R}$ è estensione trascendente di $\mathbb{Q}$, poiché $[\mathbb{R} : \mathbb{Q}] = \infty$ (Esempio B.3.9).

Osservazione B.3.26 Nel caso α sia algebrico su K, il Teorema B.3.23 ci assicura che la scrittura degli elementi del più piccolo campo che contiene K e α si semplifica in

$$K(\alpha) = \left\{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in K\right\}.$$

È questo il motivo per cui quando alle scuole secondarie si studiano i radicali, di norma viene richiesta la razionalizzazione dei risultati. Solo razionalizzando appare chiaro che l'ambiente in cui si sta "lavorando" è del tipo polinomi interi

e non fratti. Per esempio assicura che $\frac{1}{1+\sqrt{2}} \in \mathbb{Q}(\sqrt{2}) = \left\{a_0 + a_1\sqrt{2} \mid a_i \in \mathbb{Q}\right\}$ perché $\frac{1}{1+\sqrt{2}} = \frac{1}{3} - \frac{1}{3}\sqrt{2}$ e quindi $\frac{1}{1+\sqrt{2}}$ è elemento di un campo numerico più piccolo di $\mathbb{R}$. Se l'intento è quello di lavorare in $\mathbb{R}$ e non nel più piccolo campo possibile, l'esercizio è già finito quando si arriva a $\frac{1}{1+\sqrt{2}}$ e non ha significato razionalizzare perché $\frac{1}{1+\sqrt{2}}$ e $(\frac{1}{3} - \frac{1}{3}\sqrt{2})$ hanno lo stesso valore.

Teorema B.3.27 *Sia L una estensione di K. Gli elementi di L algebrici su K formano un sottocampo di L.*

DIMOSTRAZIONE. Basta provare che se a, b sono algebrici su K, lo sono anche gli elementi $a - b, ab^{-1}$. Sia a di grado n e b di grado m. Allora $[K(a) : K] = n$; consideriamo $K(a,b) = (K(a))(b)$. Essendo b di grado m su K, esso sarà algebrico di grado $\leq m$ su $K(a)$. Ne segue $[K(a,b) : K] = [K(a,b) : K(a)] \cdot [K(a) : K] \leq mn$. Ora gli elementi $a - b$ e ab^{-1} appartengono al campo $K(a,b)$ e pertanto $K(a-b) \subseteq K(a,b), K(ab^{-1}) \subseteq K(a,b)$ con $K(a,b)$ estensione finita di K. Per la 3. del Teorema B.3.23 gli elementi $a - b$ e ab^{-1} sono dunque algebrici su K. ■

Osservazione B.3.28 Il campo A di tutti i numeri algebrici su $\mathbb{Q}$ è chiaramente un'estensione di $\mathbb{Q}$ in cui ogni elemento $a \in A$ è algebrico e quindi $[\mathbb{Q}(a) : \mathbb{Q}]$ ha grado finito, ma $[A : \mathbb{Q}]$ ha grado infinito. Infatti supponiamo per assurdo che sia $[A : \mathbb{Q}] = n \in \mathbb{N}^*$. Consideriamo l'elemento $z = \sqrt[n+1]{2}$, esso è radice del polinomio $x^{n+1} - 2$ irriducibile su $\mathbb{Q}$ e quindi è il polinomio minimo di z. Risulta allora $[\mathbb{Q}(z) : \mathbb{Q}] = n + 1 > [A : \mathbb{Q}] = n$ e ciò è assurdo perchè abbiamo supposto $z \in A$.

Dopo avere completamente caratterizzato le estensioni algebriche semplici, ci chiediamo come costruire l'estensione di un campo K tramite un numero finito di elementi $\alpha_1, \alpha_2, \ldots, \alpha_n$ algebrici su K e calcolare il grado di questa estensione su K. La risposta è molto semplice: per trovare il più piccolo campo che contenga K e gli elementi $\alpha_1, \alpha_2, \ldots, \alpha_n$ basta procedere per estensioni successive. Prima si costruisce $K(\alpha_1)$ poi a questa estensione si aggiunge l'elemento α_2 ottenendo così l'estensione $K(\alpha_1, \alpha_2)$ e così via fino ad ottenere l'estensione $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Ma se K è un campo di caratteristica zero allora tutte le estensioni finite di K si possono ottenere come estensioni semplici.[3] Vale infatti il seguente teorema noto come **Teorema dell'elemento primitivo**.[4]

[3] Ricordiamo che i campi numerici sono tutti di caratteristica zero.

[4] Il teorema dell'elemento primitivo vale anche per i campi finiti se si richiede l'ulteriore ipotesi che $\alpha_1, \alpha_2, \ldots, \alpha_h$ siano separabili.

Teorema B.3.29 *Sia K un campo di caratteristica zero e sia $K(\alpha_1, \alpha_2, \ldots, \alpha_h)$ una estensione di K con $\alpha_1, \alpha_2, \ldots, \alpha_h$ algebrici su K. Allora esiste un elemento $\gamma \in K(\alpha_1, \alpha_2, \ldots, \alpha_h)$ tale che $K(\alpha_1, \alpha_2, \ldots, \alpha_h) = K(\gamma)$.*

DIMOSTRAZIONE. Procediamo per induzione su h. Proviamo il teorema per $h = 2$. Siano $f(x), g(x) \in K[x]$ i polinomi minimi (irriducibili) di α_1 e α_2 rispettivamente. Indicata con L un'estensione di K in cui entrambi i polinomi ammettono tutte le radici, siano

$$\alpha_1 = \alpha_{1,1}, \alpha_{1,2}, \ldots, \alpha_{1,n}, \qquad \alpha_2 = \alpha_{2,1}, \alpha_{2,2}, \ldots, \alpha_{2,m}$$

le radici in L di $f(x)$ e $g(x)$ rispettivamente. Poiché il campo è di caratteristica zero e i polinomi sono irriducibili, per noti risultati algebrici elementari tutte le radici sono distinte, ossia tutti gli $\alpha_{1,i}$ sono distinti così come sono tutti distinti fra di loro gli $\alpha_{2,j}$ (Gabelli, 2008, p. 57, Proposizione 2.4.3; Birkhoff e Mac Lane, 1965, p. 403, Corollary 2). Per ogni $i = 1, 2, \ldots, n$ e ogni $j = 2, \ldots, m$ l'equazione nell'incognita λ

$$\alpha_{1,i} + \lambda\alpha_{2,j} = \alpha_1 + \lambda\alpha_2$$

ammette una ed una sola soluzione in L data da

$$\lambda = \frac{\alpha_{1,i} - \alpha_1}{\alpha_2 - \alpha_{2,j}}.$$

Poiché ha caratteristica zero, K ha infiniti elementi, siamo pertanto certi di poter scegliere un elemento $\gamma \in K$ che non soddisfi nessuna delle $n(m-1)$ equazioni precedenti. Sia $\alpha = \alpha_1 + \gamma\alpha_2$, proviamo che

$$K(\alpha_1, \alpha_2) = K(\alpha).$$

Per come è stato definito, è ovvio che $\alpha \in K(\alpha_1, \alpha_2)$ e pertanto $K(\alpha) \subseteq K(\alpha_1, \alpha_2)$. Proviamo ora che $K(\alpha_1, \alpha_2) \subseteq K(\alpha)$, per fare questo basta provare che $\alpha_2 \in K(\alpha)$. Da $f(\alpha_1) = 0$ segue $f(\alpha - \gamma\alpha_2) = 0$ ossia α_2 è radice del polinomio

$$p(x) = f(\alpha - \gamma x) \in K(\alpha)[x].$$

L'elemento α_2 è radice sia di $g(x)$ sia di $p(x)$ e quindi, in una opportuna estensione di $K(\alpha)$, $x - \alpha_2$ è un fattore sia di $g(x)$ sia di $p(x)$ ossia $x - \alpha_2$ è un divisore del $\text{MCD}(g(x), p(x))$. Anzi è il loro massimo comune divisore perché $g(x)$ e $p(x)$ oltre ad α_2 non hanno altre radici in comune, infatti se $\alpha_{2,j}$ fosse radice di $p(x)$ si avrebbe $\alpha - \gamma\alpha_{2,j} = \alpha_{1,i}$ ossia $\alpha = \alpha_{1,i} + \gamma\alpha_{2,}$ e poiché

$\alpha = \alpha_1 + \gamma\alpha_2$, si ottiene $\alpha_1 + \gamma\alpha_2 = \alpha_{1,i} + \gamma\alpha_{2,j}$ e quindi γ sarebbe soluzione di una delle equazioni

$$\alpha_{1,i} + \lambda\alpha_{2,j} = \alpha_1 + \lambda\alpha_2$$

contro l'ipotesi. Il massimo comune divisore di $g(x)$ e $p(x)$ non può nemmeno essere $(x - \alpha_2)^t$ con $t > 1$ perché $g(x)$ ha tutte radici semplici (ossia diverse). Rimane dunque provato che $x - \alpha_2 = \text{MCD}(g(x), p(x))$. Poiché $g(x)$, $p(x)x) \in K(\alpha)[x]$, anche $x - \alpha_2 \in K(\alpha)[x]$ e quindi $\alpha_2 \in K(\alpha)$ e da $\alpha = \alpha_1 + \gamma\alpha_2$ segue $\alpha_1 \in K(\alpha)$. Resta così provato che $K(\alpha_1, \alpha_2) \subseteq K(\alpha)$ e pertanto si conclude $K(\alpha_1, \alpha_2) = K(\alpha)$.

Per induzione, se $K(\alpha_1, \ldots, \alpha_{h-1})$ è un'estensione semplice, tale è anche $K(\alpha_1, \ldots, \alpha_h)$. Infatti poiché, per ipotesi di induzione, $K(\alpha_1, \ldots, \alpha_{h-1})$ è un'estensione semplice, esiste $w \in K(\alpha_1, \ldots, \alpha_{h-1})$ tale che $K(\alpha_1, \ldots, \alpha_{h-1}) = K(w)$ e poiché il polinomio minimo irriducibile di α_h ha tutte radici distinte, per quanto dimostrato sopra esiste α tale che $K(\alpha_1, \ldots, \alpha_h) = K(w, \alpha_h) = K(\alpha)$. ■

Corollario B.3.30 *Ogni estensione finita di un campo a caratteristica zero è una estensione semplice.*

Esempio B.3.31 Supponiamo di voler costruire l'estensione di $\mathbb{Q}$ tramite i numeri algebrici $\sqrt{2}$ e $\sqrt{3}$. Dapprima estendiamo $\mathbb{Q}$ tramite $\sqrt{2}$ ottenendo il campo

$$\mathbb{Q}(\sqrt{2}) = \left\{ a_0 + a_1\sqrt{2} \mid a_i \in \mathbb{Q} \right\}$$

e risulta $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ perché $\sqrt{2}$ è algebrico di grado 2 rispetto a $\mathbb{Q}$ essendo $x^2 - 2 \in \mathbb{Q}[x]$ il polinomio minimo irriducibile di cui è radice. Ora estendiamo $\mathbb{Q}(\sqrt{2})$ con l'elemento $\sqrt{3}$. Il polinomio $x^2 - 3$ è irriducibile non solo su $\mathbb{Q}$ ma anche su $\mathbb{Q}(\sqrt{2})$ e quindi l'estensione $(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ha grado 2 su $\mathbb{Q}(\sqrt{2})$ e risulta

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{ \alpha + \beta\sqrt{3} \mid \alpha, \beta \in \mathbb{Q}(\sqrt{2}) \right\} = \left\{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \right\}.$$

L'estensione $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ ha grado 4 su $\mathbb{Q}$ perché

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

D'altra parte, poiché $\sqrt{2}$ e $\sqrt{3}$ sono algebrici, per il teorema dell'elemento primitivo deve esistere un elemento γ tale che $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\gamma)$. È immediato verificare che questo elemento è $\sqrt{2} + \sqrt{3}$ che effettivamente è di grado 4 rispetto a $\mathbb{Q}$ perché radice del polinomio $x^4 - 10x^2 + 1$ irriducibile in $\mathbb{Q}[x]$.

B.3.3 Il caso dell'estensione quadratica

Nella determinazione delle equazioni algebriche risolubili per radicali e nelle costruzioni con riga e compasso, giocano un ruolo particolarmente importante le estensioni quadratiche. Si dice che il campo L è un'estensione quadratica del campo K se $[L : K] = 2$. In questo caso, per ogni $\alpha \in L - K$, risulta $[K(\alpha) : K] = 2$ e dunque $L = K(\alpha)$. Inoltre α è radice di un polinomio irriducibile $x^2 + bx + c$ a coefficienti in K e una base di L su K è $\{1, \alpha\}$.

Sia ora K un campo[5] di caratteristica diversa da 2 e sia $K(\alpha)$ un ampliamento quadratico con $\alpha^2 + b\alpha + c = 0,\ b, c \in K$. Posto $\Delta = b^2 - 4c$, si ha $\Delta \in K$ e

$$\alpha^2 + b\alpha = -c$$

$$b^2 + 4\alpha^2 + 4b\alpha = b^2 - 4c$$

$$(2\alpha + b)^2 = \Delta$$

Quindi in $K(\alpha)$ esiste un elemento γ tale che $\gamma^2 = \Delta \in K$, è l'elemento $\gamma = \pm(2\alpha + b)$. Inoltre risulta $\alpha = \frac{1}{2}(\gamma - b)$. In analogia con le notazioni usate nei campi numerici, possiamo porre $\gamma = \pm\sqrt{\Delta}$ e ritrovare in questo modo le usuali formule risolutive delle equazioni di secondo grado

$$\alpha = \frac{-b \pm \sqrt{\Delta}}{2}.$$

Poiché $\alpha \in K(\gamma)$, allora $\gamma \notin K$ e $K(\alpha) = K(\gamma)$. Viceversa, se $\gamma \notin K$ e $\gamma^2 = c \in K$, allora il polinomio $x^2 - c$ è irriducibile su K e $K(\gamma)$ è una estensione quadratica di K.

Possiamo dunque concludere che *tutte e sole le estensioni quadratiche di un campo K di caratteristica diversa da 2 sono quelle del tipo $K(\gamma)$, con $\gamma \notin K$ e $\gamma^2 \in K$.*

B.3.4 Campo di riducibilità completa di un polinomio

Definizione B.3.32 Sia K un campo e $f(x)$ un polinomio di grado n a coefficienti in K. Un'estensione L di K si dice ***campo di riducibilità completa*** *o* ***campo di spezzamento*** di $f(x)$ se esistono $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ e $a \in K$ tali che*:*

1. $f(x) = a(x - \alpha_1) \ldots (x - \alpha_n)$
2. $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$

[5] Un campo H ha caratteristica 2 se $a + a = 0$ per ogni $a \in H$.

La 1. dice che in L ci sono tutte le radici di $f(x)$ perché $f(x)$ si "spezza" nel prodotto di fattori lineari. La 2. dice che L è la più piccola estensione di K che contiene tutte le radici di $f(x)$.

Esempio B.3.33 Riprendendo esempi già incontrati, ora possiamo dire che

- $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ è il campo di spezzamento di $x^2-2 \in \mathbb{Q}[x]$.
- $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\right\}$ è il campo di spezzamento di $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$.
- $\mathbb{C} = \{a+ib \mid a, b \in \mathbb{R}\}$ è il campo di spezzamento del polinomio $x^2+1 \in \mathbb{Q}[x]$.

Esempio B.3.34 Consideriamo il polinomio $f(x) = x^2 + 1$.

- Se lo si pensa come polinomio a coefficienti in $\mathbb{Q}$, il suo campo di spezzamento è $\mathbb{Q}(i)$.
- Se lo si pensa come polinomio a coefficienti in $\mathbb{R}$, il suo campo di spezzamento è $\mathbb{R}(i) = \mathbb{C}$.

Come esplicitato in quest'ultimo esempio, nella determinazione di un campo di spezzamento è essenziale *specificare il campo in cui si sta considerando il polinomio.* Inoltre, se del polinomio $f(x)$ si conoscono le radici, per determinare un campo di spezzamento di $f(x)$ basta ampliare il campo K con le radici del polinomio $f(x)$.

Ma si può trovare il campo di spezzamento di un polinomio $f(x) \in K[x]$ anche quando *non si conoscono esplicitamente le radici* del polinomio.

Infatti, qualunque sia il polinomio $f(x) \in K[x]$, K campo, si riesce a costruire un campo che contiene **una** radice di $f(x)$. Dopo questo primo passo, con un procedimento induttivo si dimostra che esiste un campo che contiene **tutte** le radici di $f(x)$.

Teorema B.3.35 *Sia K un campo e sia $f(x)$ un polinomio di grado n su K. Esiste il campo L di spezzamento di $f(x)$ su K ed è unico a meno di isomorfismi.*

Di questo teorema non riportiamo la dimostrazione perché coinvolge anche altre nozioni di algebra non riportate in questo compendio: si rinvia ad un

qualunque testo di algebra, ad esempio Dikranjan e Lucido (2007, pp. 294–295). L'esistenza del campo di spezzamento di un polinomio è fondamentale per lo studio delle equazioni algebriche.

Ad esempio permette di stabilire importanti relazioni fra i coefficienti di un polinomio e le sue radici.

Osservazione B.3.36 (Formule di Viète) Sia K un campo e sia $f(x) \in K[x], f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$. Se L è il campo di spezzamento di $f(x)$, siano $v_1, v_2, \ldots, v_n \in L$ le radici (non necessariamente distinte) di $f(x)$. In $L[x]$ si ha $f(x) = (x - v_1)(x - v_2) \cdot \ldots \cdot (x - v_n)$, dopo aver eseguito i calcoli al secondo membro, confrontando i coefficienti del polinomio $f(x)$ con quelli del polinomio $(x - v_1)(x - v_2) \cdot \ldots \cdot (x - v_n)$ si ottengono i coefficienti $a_1, a_2, \ldots, a_n$ in funzione delle radici $v_1, v_2, \ldots, v_n$ (funzioni simmetriche):

$$a_1 = -\sum_1^n v_i, \qquad a_2 = \sum_{1 \le i < j \le n} v_i v_j, \qquad a_3 = -\sum_{1 \le i < j < k \le n} v_i v_j v_k,$$

$$\ldots, \quad a_{n-1} = (-1)^{n-1}(v_1 v_2 \ldots v_{n-1} + v_1 v_2 \ldots v_{n-2} v_n + \ldots + v_2 v_3 \ldots v_n),$$

$$a_n = (-1)^n v_1 v_2 \ldots v_n.$$

Esempio B.3.37

- Se $f(x) = x^2 + a_1x + a_2$, indicate con v_1 e v_2 le radici del polinomio, si ha
$$a_1 = -(v_1 + v_2), \qquad a_2 = v_1 v_2$$

- Se $f(x) = x^3 + a_1x^2 + a_2x + a_3$, indicate con v_1, v_2, v_3 le radici del polinomio, si ha
$$a_1 = -(v_1 + v_2 + v_3), \quad a_2 = v_1v_2 + v_1v_3 + v_2v_3, \quad a_3 = -v_1v_2v_3$$

- Se $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$, indicate con v_1, v_2, v_3, v_4 le radici del polinomio, si ha
$$a_1 = -(v_1 + v_2 + v_3 + v_4), \quad a_2 = v_1v_2 + v_1v_3 + v_1v_4 + v_2v_3 + v_2v_4 + v_3v_4,$$
$$a_3 = -(v_1v_2v_3 + v_1v_2v_4 + v_1v_3v_4 + v_2v_3v_4), \quad a_4 = v_1v_2v_3v_4$$

B.3.5 Campo di spezzamento del polinomio $x^n - 1 \in \mathbb{Q}[x]$

Il grado del campo di spezzamento di questo polinomio determina se il poligono regolare di n lati è, oppure no, costruibile "con riga e compasso" (preciseremo in seguito il senso di questa terminologia). Nel campo dei numeri complessi, il polinomio $x^n - 1$ ha n radici distinte (dette radici n-esime dell'unità) e si esprimono nella forma[6]

$$\xi_{n,k} = \cos\frac{2k\pi}{n} + i\ \sin\frac{2k\pi}{n},\ k = 0, 1, \ldots, n-1$$

Queste n radici hanno la proprietà che si ottengono tutte come potenze della radice

$$\xi_n = \xi_{n,1} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

detta *radice primitiva*.[7] Di radici le cui potenze danno tutte le radici di $x^n - 1$ (radici primitive) non c'è solo ξ_n ma anche, ovviamente, quelle del tipo ξ_n^r con r primo con n ossia $\text{MCD}(r, n) = 1$. Perciò di radici primitive ce ne sono tante quanti sono gli interi positivi primi con n, ossia sono $\varphi(n)$ (funzione di Eulero).[8] Indicate con $\xi = \xi_1, \xi_2, \ldots, \xi_{\varphi(n)}$ le radici primitive di $x^n - 1$, il polinomio

$$\phi_n = (x - \xi_1)(x - \xi_2)\ldots(x - \xi_{\varphi(n)})$$

è ovviamente monico e di grado $\varphi(n)$. Si dimostra che $\phi_n \in \mathbb{Q}[x]$ ed è irriducibile in $\mathbb{Q}[x]$ (Dikranjan e Lucido, 2007, p. 302) quindi ϕ_n è il polinomio minimo di ξ su $\mathbb{Q}$ e pertanto il campo di spezzamento del polinomio $x^n - 1 \in \mathbb{Q}[x]$ è $\mathbb{Q}(\xi)$ con $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(n)$.

Esempio B.3.38

[6] Un numero complesso z può essere rappresentato in forma algebrica con una coppia (a, b) di numeri reali oppure in forma trigonometrica (o polare) con una coppia formata da un numero reale (modulo) e da un angolo (argomento): $z = a + ib = \rho(\cos\vartheta + i\sin\vartheta)$. Il legame fra le due forme è espresso da

$$\rho = \sqrt{a^2 + b^2},\quad \cos\vartheta = \frac{a}{\sqrt{a^2 + b^2}},\quad \sin\vartheta = \frac{b}{\sqrt{a^2 + b^2}}$$

[7] Questa terminologia è attribuita a Gauss; lo stesso aggettivo viene utilizzato, con significato esteso, nel Teorema dell'elemento primitivo.

[8] Si chiama **funzione di Eulero** la funzione $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ definita da $\varphi(1) = 1$ e, per ogni $n > 1$, $\varphi(n)$ il numero dei numeri naturali k coprimi con n (ossia $\text{MCD}(n, k) = 1$) e tali che $1 \leq k < n$.

1. $x^3 - 1 = 0$ ha come radici

$$\xi = \cos\frac{2\pi}{3} + i\ \sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$
$$\xi^2 = \cos\frac{4\pi}{3} + i\ \sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$
$$\xi^3 = \cos 2\pi + i\ \sin 2\pi = 1$$

di cui ξ e ξ^2 sono radici primitive. Si ha $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(3) = 2$ e $\mathbb{Q}(\xi)$ è campo di spezzamento del polinomio $x^3 - 1 \in \mathbb{Q}[x]$. D'altra parte $x^3 - 1 = (x-1)(x^2 + x + 1)$ con $x^2 + x + 1$ irriducibile in $\mathbb{Q}[x]$, di grado 2, ed avente come radici ξ e ξ^2.

2. $x^4 - 1 = 0$ ha come radici

$$\xi = \cos\frac{\pi}{2} + i\ \sin\frac{\pi}{2} = i, \quad \xi^2 = i^2 = -1, \quad \xi^3 = i^3 = -i, \quad \xi^4 = i^4 = 1$$

di cui ξ e ξ^3 sono radici primitive. Si ha $[\mathbb{Q}(\xi) : \mathbb{Q}] = \varphi(4) = 2$ e $\mathbb{Q}(\xi)$ è campo di spezzamento del polinomio $x^4 - 1 \in \mathbb{Q}[x]$. D'altra parte $x^4 - 1 = (x-1)(x+1)(x^2+1)$ con $x^2 + 1$ irriducibile in $\mathbb{Q}[x]$, di grado 2, ed avente come radici i e $-i$.

B.4 Caratterizzazione algebrica delle costruzioni con riga e compasso

La risolubilità di problemi geometrici con il solo utilizzo della riga e del compasso[9] è stata una questione centrale della matematica greca dell'antichità.[10] Solo dopo quasi 2000 anni da Euclide, lo sviluppo dell'algebra ha permesso,

[9] Riga non graduata e compasso che si richiude appena sollevato dal foglio ossia non permette il trasporto meccanico di lunghezze.

[10] La riga ed il compasso furono per molti secoli lo strumento analogico di calcolo per eccellenza. Alla riga ed al compasso vennero affidate le progettazioni sulle tavole da disegno della geometria dei bastioni difensivi angolati, che divennero necessari dopo l'evoluzione delle armi da fuoco pesanti che erano diventate in grado di abbattere le mura classiche lineari, del tipo di quelle del XIV secolo di Montagnana (Padova). La nuova architettura difensiva raggiunse la sua massima espressione nella fortificazione ad ennagono stellato di Palmanova (Udine), realizzata essenzialmente dal 1593 al 1599 da Giulio Savorgnan, generale della Serenissima. Il progetto originale di Palmanova del 1593 prevedeva una pianta decagonale, basata cioè su un poligono regolare, il decagono, costruibile con riga e compasso; ma successivamente il Senato decise per l'ennagono, riducendo così del 10% le spese della costruzione dei bastioni. Come vedremo, l'ennagono non è costruibile con riga e compasso, ma è costruibile con riga

grazie alla Teoria di Galois, di risolvere completamente il problema di quali siano le costruzioni possibili con il solo uso della riga e del compasso. Poiché queste questioni sono strettamente legate anche all'essere un numero reale algebrico o trascendente, ci è parso opportuno inserire un paragrafo dedicato a questo argomento. D'altra parte queste problematiche, anche se antiche e ora completamente risolte, continuano ad essere molto attuali non solo per la loro intrinseca bellezza ma perché si prestano molto bene all'uso del computer per applicazioni didattiche.

B.4.1 Punti costruibili

Nel piano reale $\mathbb{R}\times\mathbb{R}$, i punti costruibili con riga e compasso (o con costruzioni euclidee) sono definiti con un procedimento ricorsivo a partire da due punti fissati, O ed U, assunti come costruibili. Posto $S_0 = \{O, U\}$ si dice che un punto P del piano reale è un ***punto costruibile*** se esiste una successione finita di punti distinti $P_1, P_2, \ldots, P_n = P$ tali che per ogni $i = 1, \ldots, n$, il punto P_i sia ottenibile tramite le operazioni di

1. intersezione di due rette,

2. intersezione di una retta e di una circonferenza,

3. intersezione di due circonferenze,

dove rette e circonferenze sono quelle determinate da due punti dell'insieme $S_{i-1} = \{O, U, P_1, \ldots, P_{i-1}\}$.[11]

Nel seguito parleremo semplicemente di punti costruibili sottointendendo "con riga e compasso". Se P e Q sono due punti costruibili, si dice anche che sono costruibili il segmento $\overline{PQ}$, la retta PQ, la circonferenza C_{PQ} di centro P e raggio $\overline{PQ}$.

---

e compasso il numero $1/\sqrt{\frac{1}{4} + \left(\frac{2}{3} + \frac{1}{\sqrt{2}}\right)^2}$, che approssima il valore (esatto) $2\sin(\pi/9)$ del lato dell'ennagono regolare inscritto nel cerchio di raggio $r = 1$ con un errore in modulo minore di 0.000016. Non è casuale che agli stessi anni, e precisamente al 1594, risalga il giovanile *Trattato di fortificazione* di Galileo Galilei. Va tuttavia osservato che Galileo non segue strettamente le regole euclidee, anzi ne esce volutamente con la progettazione di nuovi tipi di compassi, come il suo noto *compasso geometrico e militare*, sull'uso del quale scrisse successivamente un apposito trattato tecnico.

[11] Se i punti sono P_r e P_s, con la riga e il compasso si può tracciare la retta P_rP_s, disegnare il segmento $\overline{P_rP_s}$, disegnare la circonferenza avente centro P e raggio uguale alla distanza dei punti P_r e P_s.

Esempio B.4.1 Come è ben noto, fra le principali costruzioni con riga e compasso ci sono quelle sottoelencate. Per la dimostrazione si rinvia a Gabelli (2008, pp. 348–351).

1. Il punto medio di un segmento.
2. Dati una retta r ed un suo punto P, la retta perpendicolare ad r e passante per P.
3. Dati una retta r ed un punto $P \notin r$, la retta parallela ad r e passante per P.
4. Il punto simmetrico a un dato punto P rispetto una data retta r.
5. La bisezione di un angolo.
6. La sezione aurea di un segmento.
7. Il quadrato di lato $\overline{PQ}$.

Esempio B.4.2 (Costruzione del riferimento cartesiano ortogonale) Dati due punti O e U del piano, con la seguente costruzione rimane determinato un riferimento cartesiano ortogonale di cui O ed U sono rispettivamente l'origine e il punto unitario dell'asse delle ascisse.

Definiamo la retta OU asse delle ascisse. Intersecando questa retta con la circonferenza di centro O e raggio $\overline{OU}$, rimane determinato il punto $P \neq U$ e O è il punto medio del segmento $\overline{PU}$. Si può allora costruire la retta perpendicolare alla retta delle ascisse e passante per O, questa la definiamo asse delle ordinate.

B.4.2 Caratterizzazione algebrica dei punti costruibili

Utilizzeremo i risultati algebrici della Sezione B.3 per dare una caratterizzazione algebrica dei punti costruibili con riga e compasso.

Definizione B.4.3 Un ***numero reale*** α si dice ***costruibile*** se con riga e compasso (e unità di misura fissata) si riesce a costruire un segmento di lunghezza $|\alpha|$.

Questa definizione permette di parlare in modo *equivalente di punti costruibili* e *di numeri reali costruibili*. Nel seguito supporremo che nel piano $\mathbb{R} \times \mathbb{R}$ sia definito un sistema di riferimento cartesiano ortogonale in cui l'origine O, il punto U e gli assi coordinati siano costruibili. L'Esempio B.4.2 assicura che ciò non è restrittivo. Inoltre dalle (2) e (3) dell'Esempio B.4.1, segue che

- $P(x,0)$ è costruibile se e solo se lo è il punto $Q(0,x)$.
- Un punto $P(x,y)$ è costruibile se e solo se lo sono i punti $P_x = (x,0)$ e $P_y = (y,0)$

Possiamo allora dire che **un punto P è costruibile se e solo se lo sono le sue coordinate** rispetto ad un fissato sistema di assi cartesiani.

Teorema B.4.4 *Sia $\mathcal{C}$ l'insieme delle coordinate di tutti i punti costruibili: $\mathcal{C} = \{x \in \mathbb{R} \mid P = (x,0)$ è costruibile $\}$. Si ha*

1. *$\mathcal{C}$ è un campo.*
2. *$\mathbb{Q} \subseteq \mathcal{C}$.*
3. *$\sqrt{x} \in \mathcal{C}$ per ogni $x \in \mathcal{C}, x \geq 0$.*

Dimostrazione. 1. Siano $x, y \in \mathcal{C}$, ossia $P = (x,0)$ e $Q = (y,0)$ sono punti costruibili. Per dimostrare che $\mathcal{C}$ è un campo, facciamo vedere che per ogni $x, y \in \mathcal{C}$ si ha $x - y \in \mathcal{C}$ e, se $y \neq 0$, $xy^{-1} \in \mathcal{C}$. Il punto $R = (-y, 0)$ è costruibile perché intersezione della retta delle ascisse con la circonferenza di centro O e raggio $\overline{OQ}$. Consideriamo ora il punto medio del segmento $\overline{PR}$ che sappiamo essere costruibile, sia $M = (\frac{x-y}{2}, 0)$; allora il punto $S = (x - y, 0)$ è costruibile perché è intersezione della retta delle ascisse con la circonferenza di centro M e raggio $\overline{MO}$. Rimane dunque provato che per ogni $x, y \in \mathcal{C}$ si ha $x - y \in \mathcal{C}$. Poiché, come visto, se $x \in \mathcal{C}$ allora anche $-x \in \mathcal{C}$, senza ledere in generalità, consideriamo $x, y \in \mathcal{C}$ con x, y positivi non nulli, dimostriamo che $xy^{-1} \in \mathcal{C}$. Siano $P = (x,0), Q = (y,0), V = (0,1)$, costruiamo la retta passante per P e parallela alla retta QV. L'intersezione di questa retta con l'asse delle ordinate sia $Z = (0,z)$. I triangoli di vertici VOQ e ZOP sono simili e pertanto $z = xy^{-1} \in \mathcal{C}$.

2. Poiché $1 \in \mathcal{C}$ e $\mathcal{C}$ sottocampo di $\mathbb{R}$ (e quindi di caratteristica 0), si ha $\mathbb{Q} \subseteq \mathcal{C}$.

3. Sia $x \in \mathcal{C}, x > 0$, ossia $P = (x,0)$ è costruibile. Poiché $-1 \in \mathcal{C}$, si può costruire il punto medio N del segmento $\overline{AP}$ con $A = (-1,0)$. Sia $T = (0,t)$ il punto intersezione del semiasse positivo delle ordinate con la circonferenza di centro N e raggio $\overline{NP}$. Il triangolo ATP è rettangolo in T, il segmento $\overline{TO}$ è l'altezza relativa all'ipotenusa $\overline{AP}$ e quindi, per il secondo teorema di Euclide, il segmento $\overline{OT}$ è medio proporzionale tra $\overline{AO}$ e $\overline{OP}$ e pertanto $t^2 = x$. Essendo T costruibile si conclude $t = \sqrt{x} \in \mathcal{C}$. ■

Sia F un sottocampo di $\mathbb{R}$. Se $\mathcal{P}$ è l'insieme dei punti del piano $F \times F$, i punti del piano reale che si possono ottenere con costruzioni euclidee a partire da $\mathcal{P}$, sono quelli ottenibili tramite:

1. intersezione di due rette di F,
2. intersezione di una retta e di una circonferenza di F,
3. intersezione di due circonferenze di F.

Nel caso 1. non si ottengono nuovi punti perché si tratta di risolvere un sistema lineare a coefficienti in F e quindi la soluzione è ancora un elemento di F. Nei casi 2. e 3. si tratta di risolvere un'equazione di secondo grado e perciò la soluzione è un elemento di F oppure un elemento di una estensione quadratica di F, $F(\sqrt{a}), a \in F$. I soli punti del piano reale che si possono costruire a partire da F sono quindi punti le cui coordinate appartengono a campi della forma $F(\alpha)$, con $\alpha \in \mathbb{R}, \alpha^2 \in F$. D'altra parte, ogni punto avente coordinate in una estensione $F(\beta), \beta \in \mathbb{R}, \beta^2 \in F$ è effettivamente costruibile perché, come dimostrato nel Teorema B.4.4, la radice quadrata di un numero costruibile è costruibile.

Formalizziamo tutto ciò in termini di ampliamenti di campo.

Teorema B.4.5 *Sia F un sottocampo di $\mathcal{C}$, K un campo tale che $F \subseteq K \subseteq \mathbb{R}$. Se $[K : F] \leq 2$ allora $K \subseteq \mathcal{C}$.*

Dimostrazione. Se $[K : F] = 1$ allora $K = F \subseteq \mathcal{C}$. Se $[K : F] = 2$ risulta $K = F(\alpha)$ con $\alpha^2 \in F$. Essendo K un sottocampo di $\mathbb{R}$ e $\alpha^2 > 0$, si ha $\alpha \in \mathcal{C}$ per la (3) del Teorema B.4.4. ■

Teorema B.4.6 *Il punto $P = (x, y)$ è costruibile se e soltanto se esiste una catena finita di campi numerici reali*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$$

tali che $x, y \in K$ e $[K_i : K_{i-1}] \leq 2 \quad$ per $\quad i = 1, 2, \ldots, n$.

Dimostrazione. Sia P un punto costruibile. Allora esiste una successione finita di punti $P_1, P_2, \ldots, P_n = P$ tali che, per ogni $i = 1, 2, \ldots, n$, P_i è ottenibile come intersezione di due rette, oppure di due circonferenze, oppure di una retta e una circonferenza definite da due punti dell'insieme $S_{i-1} = \{O, U, P_1, \ldots, P_{i-1}\}$. Se $P_i = (x_i, y_i)$, poniamo $K_0 = \mathbb{Q}$ e $K_i = K_{i-1}(x_i, y_i)$, per $i = 1, 2, \ldots, n$. Le equazioni di rette e circonferenze definite da due punti di S_{i-1} hanno i coefficienti che appartengono a K_{i-1}; inoltre, se P_i è intersezione di due rette definite da punti di S_{i-1}, la coppia delle sue coordinate è soluzione di un sistema lineare di due equazioni in due incognite a coefficienti in K_{i-1} e perciò le coordinate di P_i appartengono ancora a K_{i-1} e risulta

$[K_i : K_{i-1}] = 1$. Se P_i è intersezione di una retta e di una circonferenza oppure di due circonferenze definite da punti di S_{i-1}, la coppia delle sue coordinate è soluzione di un sistema formato da una equazione lineare e da una equazione di secondo grado in due incognite a coefficienti in K_{i-1}; in questo caso, pertanto, una delle due coordinate si ottiene risolvendo una equazione di secondo grado a coefficienti in K_{i-1} mentre l'altra coordinata si ottiene come funzione lineare di questa. Ne segue che $[K_i : K_{i-1}] \leq 2$.

Viceversa, supponiamo esista una catena di campi

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$$

tali che $x, y \in K$ e $[K_i : K_{i-1}] \leq 2 \quad$ per $\quad i = 1, 2, \ldots, n$. Per dimostrare che P è costruibile basta far vedere che $K \subseteq \mathcal{C}$. Tenuto conto del Teorema B.4.5, procediamo per induzione su n. Per $n = 0$ si ha $\mathbb{Q} \subseteq \mathcal{C}$ come dimostrato nel Teorema B.4.4. Per $\quad i = 1, 2, \ldots, n$, supposto $K_i \subseteq \mathcal{C}$, poiché $[K_i : K_{i-1}] \leq 2$, per il Teorema B.4.5 si ha $K_i \subseteq \mathcal{C}$. ■

Poiché ogni ampliamento di grado 2 di un campo numerico F è del tipo $F(\sqrt{a}), a \in F$, per il teorema ora dimostrato possiamo anche dire che il punto $P = (x, y)$ è costruibile se e soltanto se è possibile determinare una catena di sottocampi di $\mathbb{R}$

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$$

tali che $x, y \in K$ e $K_i = K_{i-1}(\sqrt{a_i})$, con $a_i \in K_{i-1} \quad$ per $\quad i = 1, 2, \ldots, n$. Ciò significa che P è costruibile se e soltanto se le sue coordinate si possono esprimere in termini di radicali quadratici successivi.

Corollario B.4.7 *Se il punto $P = (x, y)$ è costruibile allora*

$$[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^h, h \geq 0$$

Dimostrazione. Per il Teorema B.4.6, se $P = (x, y)$ è costruibile, esiste una catena finita di campi

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = K$$

tali che $x, y \in K$ e $[K_i : K_{i-1}] \leq 2 \quad$ per $\quad i = 1, 2, \ldots, n$. Poiché $\mathbb{Q} \subseteq \mathbb{Q}(x, y) \subseteq K$ e il grado di K su $\mathbb{Q}$ è uguale a una potenza di 2, anche il grado di $\mathbb{Q}(x, y)$ su $\mathbb{Q}$ è uguale a una potenza di 2 (Teorema B.3.11). ■

Possiamo dunque affermare che *se α è un numero reale costruibile, allora esso appartiene ad un ampliamento di $\mathbb{Q}$ di grado una potenza di* 2. In particolare quindi ogni numero reale costruibile è algebrico.

Questo fatto ci assicura che **nessun numero trascendente è costruibile**, inoltre fornisce un importante criterio di non costruibilità per i numeri algebrici.

Teorema B.4.8 *Se un numero reale α è radice di un polinomio irriducibile di grado n che non è una potenza di 2, allora il numero non è costruibile.*

DIMOSTRAZIONE. Se α soddisfa un polinomio irriducibile di grado n, sappiamo che questo è il suo polinomio minimo e pertanto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n \neq 2^h$. Quindi α non può appartenere ad un ampliamento algebrico di grado una potenza di 2 come dovrebbe essere se α fosse costruibile (Corollario B.4.7). ■

Osservazione B.4.9 Si faccia attenzione che se un numero reale è radice di un polinomio irriducibile di grado una potenza di 2, **non** si può concludere che il numero è costruibile.

B.4.3 Problemi classici non costruibili con riga e compasso

I risultati ottenuti permettono di dimostrare che molte costruzioni classiche dell'antichità non sono costruibili usando solo la riga e il compasso. Fra queste ricordiamo i problemi più noti.

Duplicazione del cubo

Il problema consiste nel *costruire un cubo il cui volume sia uguale al doppio di quello di un cubo assegnato.* Supponendo che il lato del cubo assegnato abbia lunghezza uguale ad 1, per risolvere il problema della duplicazione occorre costruire il numero $\sqrt[3]{2}$. Posto $\alpha = \sqrt[3]{2}$, α soddisfa il polinomio $x^3 - 2$ irriducibile su $\mathbb{Q}$. Poiché il grado di questo polinomio non è una potenza di 2, per il Teorema B.4.8, α non può essere costruibile.

Quadratura del cerchio

Il problema consiste nel *costruire un quadrato che abbia area uguale a quella di un cerchio assegnato.* Possiamo supporre sia 1 il raggio del cerchio, si tratta quindi di costruire un quadrato di lato $\sqrt{\pi}$. Questo è impossibile perché $\sqrt{\pi}$ è trascendente (se fosse algebrico sarebbe algebrico anche π, e non lo è per il teorema di Lindemann).

Rettificazione della circonferenza

Il problema consiste nel *costruire un segmento pari alla lunghezza di una circonferenza.* Supponiamo sia 1 il raggio della circonferenza, si tratta di costruire un segmento di lunghezza 2π. Se ciò fosse possibile, il numero 2π sarebbe algebrico mentre è trascendente.

Trisezione dell'angolo

Il problema consiste nel *costruire la terza parte di un dato angolo* 3ϑ.

Ci sono angoli per i quali questa costruzione si può fare con riga e compasso e ci sono angoli per i quali non si può fare. Poiché costruire un angolo ϑ equivale a costruire il suo coseno, cerchiamo $\cos\vartheta$. Posto $a = \cos 3\vartheta$ e ricordando che

$$\cos 3\vartheta = 4\cos^3\vartheta - 3\cos\vartheta,$$

si ha che $\cos\vartheta$ è radice del polinomio

$$4x^3 - 3x - a.$$

Se questo polinomio è irriducibile nel campo $\mathbb{Q}(a)$, allora $\cos\vartheta$ ha grado 3 su $\mathbb{Q}(a)$ e quindi, per il Corollario B.4.7, non è costruibile con riga e compasso.

▼ Sia ad esempio $3\vartheta = \frac{\pi}{3}$, si tratta di costruire $\frac{\pi}{9}$. Si ha $\cos 3\vartheta = \frac{1}{2}$ e $\cos\vartheta$ è radice del polinomio

$$4x^3 - 3x - \frac{1}{2},$$

che è irriducibile su $\mathbb{Q}$ perché non ha radici razionali. Dunque $\cos\vartheta = \cos\frac{\pi}{9}$ ha grado 3 su $\mathbb{Q}$ quindi $\cos\frac{\pi}{9}$ non è un numero costruibile e $\frac{\pi}{3}$ non è trisecabile.▲

Facciamo ora vedere che certi angoli sono trisecabili con riga e compasso.

▼ Consideriamo, ad esempio, l'angolo $\frac{\pi}{2}$. Si ha che $\cos\frac{\pi}{6}$ è radice del polinomio

$$4\cos^3\frac{\pi}{6} - 3\cos\frac{\pi}{3} - 0$$

ossia, posto $x = \cos\frac{\pi}{6}$, è radice del polinomio $4x^3 - 3x$. Questo polinomio non è irriducibile e il polinomio minimo di $\cos\frac{\pi}{6}$ è il polinomio di secondo grado $4x^2 - 3$. Il numero $\cos\frac{\pi}{6}$ sta quindi in una estensione quadratica di $\mathbb{Q}$ e pertanto è costruibile (d'altra parte $\cos\frac{\pi}{6} = \frac{\sqrt{3}}{2}$ che sappiamo essere costruibile). ▲

B.4.4 Costruibilità dei poligoni regolari e numeri primi di Fermat

A conclusione di questa appendice vogliamo ricordare che la costruibilità con riga e compasso di un poligono regolare dipende dal numero n dei suoi lati.

Sia P_n il poligono regolare di n lati con centro nell'origine O del sistema cartesiano e un vertice in $U = (1, 0)$; indichiamo con $P_{n,k}, k = 0, 1, \ldots, n-1$ i vertici del poligono numerati in senso antiorario in modo tale che $P_{n,0} = U$ e $P_{n,k} = (\cos \frac{2k\pi}{n}, \sin \frac{2k\pi}{n})$, $k = 1, \ldots, n-1$. Costruire il poligono P_n significa costruire i suoi vertici e quindi costruire P_n equivale a costruire le radici n-esime dell'unità[12] e pertanto P_n è costruibile se e solo se è costruibile la radice primitiva[13]

$$\xi_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$$

(poiché per ogni x si ha $\cos^2 x + \sin^2 x = 1$, e la radice quadrata è costruibile con riga e compasso, è sufficiente la costruibilità di una delle due coordinate).

Fin dall'antichità era noto che se si poteva costruire un poligono regolare con m lati allora si potevano costruire anche i poligoni regolari con $2^k\, m$ lati con $k \in \mathbb{N}^*$, questo perché con riga e compasso è sempre possibile bisecare un angolo. La questione della costruibilità di un poligono regolare con n lati fu completamente risolta da Gauss nel 1801 che dimostrò il seguente teorema.[14] Per la dimostrazione si rinvia a Gabelli (2008, pp. 361–362).

Teorema B.4.10 *Un poligono regolare con n lati è costruibile se e soltanto se* $n = 2^k p_1 \ldots p_m$ *dove* $k \geq 0$ *e* $p_1 \ldots p_m$ *sono numeri primi della forma* $2^{2^r} + 1, r \geq 0$.

[12] I polinomi $x^n - 1, n \in \mathbb{N}^*$, sono detti *polinomi ciclotomici* proprio perché strettamente collegati al problema della *ciclotomia*, ossia del "taglio" del cerchio in parti uguali con riga e compasso.

[13] Vedi Sezione B.3.5.

[14] Nel 1796, Gauss, allora studente diciannovenne a Gottinga, dimostrò la formula

$$\cos \frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

che implica la costruibilità del poligono regolare con 17 lati. Successivamente, nell'ultima parte del suo libro *Disquisitiones aritmeticae* del 1801, egli affermò che è possibile costruire un poligono regolare con un numero dispari n di lati se e solo se n è prodotto di numeri primi di Fermat distinti. In realtà, pur avendo dato un risultato corretto, Gauss dimostrò solo la condizione sufficiente tramite lo studio dell'equazione $x^p - 1 = 0, p \geq 3$ primo. La condizione necessaria venne dimostrata in seguito con la teoria di Galois.

Osservazione B.4.11 (Numeri di Fermat) I numeri della forma

$$F_r = 2^{2^r} + 1, \quad r \geq 0$$

sono detti numeri di Fermat.

Nel 1634 Fermat congetturò che tutti i numeri interi della forma F_r fossero primi come in effetti lo sono i seguenti cinque:

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

Ma Eulero (1738) dimostrò la falsità della congettura perché riuscì a dimostrare che F_5 non è primo in quanto

$$F_5 = 4\,294\,976\,297 = 641 \times 6\,700\,417.$$

La scomposizione in fattori primi di numeri di Fermat è estremamente difficile, e gli unici finora completamente fattorizzati sono quelli da F_5 ad F_{11}; ad esempio:

$$F_6 = 18\,446\,744\,073\,709\,551\,617 = 274\,177 \times 67\,280\,421\,310\,721$$

Il problema della ricerca dei numeri di Fermat che siano primi è tuttora aperto. A tutt'oggi i soli numeri primi di Fermat conosciuti rimangono i cinque di Fermat, F_0, F_1, F_2, F_3, F_4, e non è neanche noto se i numeri primi di Fermat siano in numero finito o infinito.[15]

[15] Gli specialisti ritengono altamente improbabile che si possa trovare un ulteriore numero primo di Fermat "F_5" con i metodi computazionali e l' *hardware* attualmente (2012) disponibile. Informazioni aggiornate sullo stato della ricerca sui primi di Fermat (e più in generale sui numeri primi), sono disponibili nel sito della University of Tennessee at Martin: `http://primes.utm.edu` (visitato il 2/4/2012).

Bibliografia

Opere del Settecento o di periodi precedenti

Eulero, L. (1738) Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus, *Comment. Acad. Scient. Petropol.*, 6, pp. 103–107.

Eulero, L. (1740) De summis serierum reciprocarum. *Comment. Acad. Scient. Petropol.*, 7, pp. 123–134.

Eulero, L. (1744a) De fractionibus continuis dissertatio, *Comment. Acad. Scient. Petropol.*, 9, pp. 98–137.

Eulero, L. (1744b) Variae observationes circa series infinitas, *Comment. Acad. Scient. Petropol.*, 9, pp. 160–188.

Eulero, L. (1753) Calcul de la probabilité dans le jeu de rencontre, *Mémoires de l'académie de Berlin*, p. 255–270

Eulero, L. (1768) Remarques sur un beau rapport entre les series des puissances tant directes que reciproques, *Histoire de l'Académie Royale des Sciences et des Belles–Lettres de Berlin*, 17, pp. 83–106.

Eulero, L. (1774) *Elémens d'algèbre traduits de l'allemand, avec des notes et des additions* [di Joseph–Louis Lagrange], Vol. II. Lyon: Bruyset.

Eulero, L. (1797) *Introductio in analysin infinitorum*, Vol. I, Ch. XVIII. Lyon: Bernuset Delamollière Falque & Soc.

Lambert, J.H. (1768) Mémoires sur quelques propriétés remarquables des quantités transcendantes, circulaires et logarithmiques, *Mémoires de l'Académie royale des Sciences et des Belles–Lettres de Berlin*, pp. 265–322.

Legendre, A.–M. (1794) *Éléments de géométrie, avec des notes.* Paris: F. Didot.

Napier, J. [Nepero] (1614) *Mirifici logarithmorum canonis descriptio Ejusque usus, in utraque Trigonometria, ut etiam in omni Logistica Mathematica, Amplissimi, Facillimi & expeditissimi explicatio.* Edinburgi: Andreas Hart.

Napier, J. [Nepero] (1617) *Rabdologiæ seu Numerationis per Virgulas libri duo: Cum Appendice de expeditissimo Multiplicationis promptuario. Quibus accessit & ArithmeticæLocalis Liber unus.* Edinburgi: Andreas Hart.

Oriani B. (1785) De usu fractionum continuarum ad inveniendos ciclos calendarii novi & veteris, *Ephem. Astron. Anni 1786*, Mediolani, pp. 132–154.

Wallis, J. (1656) *Arithmetica Infinitorum.* Oxford: Lichfield.

Opere dell'Ottocento

CANTOR, G. (1878) Ein Beitrag zur Mannigfaltigkeitslehre, *J. Reine Angew. Math.*, 84, pp. 242–258.

CHRYSTAL, G. (1886) *Algebra: an elementary text book for the higher classes of secondary schools and for colleges.* Part I. Edinburgh: Adam and Charles Black.

CHRYSTAL, G. (1889) *Algebra: an elementary text book for the higher classes of secondary schools and for colleges.* Part II. Edinburgh: Adam and Charles Black.

DIRICHLET, G. LEJEUNE (1889) *Werke*, Erster Band. Berlin: Druck und Verlag von Georg Reimer.

HEAT, T.L. (1897) *Th Works of Archimedes.* Cambridge: University Press.

HERMITE, C. (1850) Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objects de la théorie des nombres (Deuxième lettre). *J. Reine Angew. Math.*, 40, pp. 279–290.

HERMITE, C. (1873), Sur la fonction exponentielle, *Comptes Rendus Acad. Sci. Paris*, 77, pp. 18–24. In: *Oeuvres de Charles Hermite*, Vol. III. Paris: Gauthier–Villars (pp. 150–181).

HURWITZ, A. (1894) Über die angenäherte Darstellung der Zahlen durch rationale Brüche, *Math. Ann.,* 44, pp. 2–3, 417–436.

LINDEMANN, F. (1882) Über die Zahl π, *Math. Ann.* 20, pp. 213–225.

LIOUVILLE, J. (1844) Sur les classes très étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébriques, *C.R. Acad. Sci. Paris*, 18, pp. 883–885; 910–911.

LIOUVILLE, J. (1851) Sur les classes très–étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationelles algébriques, *J. Math. Pures Appl.*, I Sér., pp. 133–142.

ZOBOLI, P. (1877) Del Calendario in Generale e in Particolare del *Calendarium perpetuum* del signor Kesselmeyer, *Annuario della Società dei Naturalisti in Modena*, Ser. II, 4, pp. 276–324.

Opere dell'inizio del Novecento

AUDISIO, F. (1930) Calcolo di π in Archimede, *Atti R. Accad. Sci. Torino*, 65, pp. 101–108.

BOREL, E. (1903) Contribution à l'analyse arithmétique du continu, *J. Math. Pures Appl.* 9, pp. 329–375.

COURANT, R. (1937) *Differential and Integral Calculus*, Vol. I–II. London and Glasgow: Blackie & Son Ltd.

GAMOW, G. (1947) *One two three ... infinity*, New York: The Viking Press Inc.

HARDY G.H. (1908) *A course of pure mathematics.* Cambridge: University Press.

Hardy G.H. e Littlewood L.E. (1914) Some problems of diophantine approximation, *Acta Math.–Djursholm*, 37(1), pp. 155–191.

Iwamoto, Y. (1949) A proof that π^2 is irrational, *J. Osaka Inst. Sci. Tech.*, 1(1), pp. 147–148.

Peano, G. (1906) *Formulario Mathematico*, Vol. V. Torino: Fratres Bocca Editores.

Zeuthen, H.G. (1902), *Histoire des mathématiques dans l'antiquité et le moyen âge.* Éd. française, rev. et corr. par l'auteur, traduite par Jean Mascart (prima edizione danese 1893).

Opere di fine Novecento o di epoca attuale

Aigner, M. e Ziegler, G.M. (2004) *Proofs from THE BOOK*, 3nd Ed. Berlin Heidelberg New York: Spinger–Verlag. Trad. it. (2006) a cura di A. Quarteroni, Milano: Springer–Verlag Italia.

Arrigo, G. e D'Amore, B. (1999) "Lo vedo, ma non ci credo". Ostacoli epistemologici e didattici al processo di comprensione di un teorema di Georg Cantor che coinvolge l'infinito attuale, *L'insegnamento della matematica e delle scienze integrate*, 22B(5), pp. 465–494.

Barozzi, G.C. (1996) *I codici crittografici a chiave pubblica*, Atti del Convegno "Il fascino *discreto* della matematica", L'Aquila, 18–20 aprile 1996, pp. 9–22 (a cura di Mauro Cerasoli). L'Aquila: Libreria universitaria Benedetti.

Barozzi, G.C. e Matarasso, S. (1986) *Analisi matematica 1.* Bologna: Zanichelli.

Berggren, L. (1997) Borwein, P.B. e Borwein, J.M. *Pi: A source book.* New York: Springer Verlag.

Baker, A. (1975) *Transcendental Number Theory.* London: Cambridge University Press.

Birkhoff, G. e Mac Lane, S. (1965) *A Survey of Modern Algebra.* New York: The Macmillan Company.

Bombieri, E. (2006) *L'infinito matematico*, conferenza tenuta in occasione delle consegna del Premio Pitagora, Crotone, 20.10.2006. URL: `http://www.math.it/eventi/BOMBIERI.pdf` (sito visitato il 10.04.2012).

Brusadin G. e Invernizzi S. (2011) On the origin of the 97/400 leap years rule in the Gregorian calendar, *Atti Soc. Nat. Mat. Modena*, 141, pp. 261–270.

Cartan, H. (1961) *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes.* Paris: Hermann.

Cecconi, J.P., Piccinini, L.C. e Stampacchia, G. (1979) *Esercizi e problemi di analisi matematica.* Napoli: Liguori Editore.

Cecconi, J.P. e Stampacchia, G. (1974) *Analisi matematica. Vol. 1: Funzioni di una variabile.* Napoli: Liguori Editore.

Coppel, W.A. (2009) *Number Theory. An Introduction to Mathematics*, 2nd Ed. Dordrecht Heildelberg London New York: Springer Science.

D'Amore, B. (2011) *Dante e la Matematica*. Firenze: Giunti.

Doggett, L.E. (1992) *Calendars*. Ch. 12 in *Explanatory Supplement to the Astronomical Almanac* (Ed. P.K. Seidelmann). Mill Valley, CA: University Science Books. URL: `http://astro.nmsu.edu/~lhuber/leaphist.html` (sito visitato il 10.04.2011).

Dikranjan D. e Lucido, M.S. (2007) *Aritmetica e algebra*. Napoli: Liguori.

Fiori, C. e Invernizzi, S. (2009) *Numeri reali*. Bologna: Pitagora Editrice.

Gabelli, S. (2008) *Teoria delle equazioni e teoria di Galois*. Berlin Heidelberg New York: Springer.

Garrity, T. (2001) On periodic sequences for algebraic numbers, *J. of Number Theory*, 88, pp. 86–103.

Giacardi, L., Roero, C.S. e Viola, C. (1995) Sui contributi di Lagrange alla teoria dei numeri, *Rend. Sem. Mat. Univ. Politec. Torino*, 53, pp. 151–181.

Hardy, G.H. e Wright, E.M. (1964) *An Introduction to the Theory of Numbers*, 3rd ed. London: Cambridge University Press.

Khinchin, A.Ya. (1964) *Continued Fractions*. Chicago: The University of Chicago Press.

Khovanskii, A.N. (1963) *The Application of Continued Fractions and their Generalizations to Problems in Approximation Theory*, Groningen: P. Noordhoff.

Martzloff, J.–C. (2006) *A History of Chinese Mathematics*. Berlin Heidelberg: Springer–Verlag.

Niven, I. (1947) A simple proof that π is irrational, *Bull. Amer. Math. Soc.*, 53, p. 506.

Niven, I. (1961) *Numbers: rational and irrational*, New York: Random House. Trad. it.: (1965) *Numeri razionali e numeri irrazionali*. Bologna: Zanichelli.

Niven, I. (1967) *Irrational numbers*, Carus Mathematical Monographs, 3rd ed. Rahway, New Jersey: Quinn & Boden Company, Inc.

Oomes, R.M.Th.E., Tersteeg, J.J.T.M e Top, J. (2000) Het grafschrift van Ludolph van Ceulen, *Nieuw Arch. Wiskd.*, 5/1 (n. 2), pp. 57–62.

Olds, C.D. (1963) *Continued fractions*. New York: Random House. Trad. it.: (1968) *Frazioni continue*. Bologna: Zanichelli.

Olds, C.D. (1970) The Simple Continued Fraction Expansion of e, *The American Mathematical Monthly*, 77(9), pp. 968–974.

Riesel, H. (2012) *Prime Numbers and Computer Methods for Factorization*, Modern Birkhäuser Classics. Boston: Birkhäuser.

Rockett, A.M. e Szüsz, P. (1992) *Continued Fractions*. Singapore: World Scientific Publishing Co.

Roth, K.F. (1955) Rational approximations to algebraic numbers e Corrigendum, *Mathematika*, 2 pp. 1–20 e 168.

Russo, L. (1996) *La rivoluzione dimenticata*, Milano: Feltrinelli.

SCHOEDER, M.R. (2009) *Number Theory in Science and Communication*, 5^{th} Ed., Berlin Heidelberg: Springer–Verlag.

SCIMEMI, B. (1993) *Le frazioni continue rivisitate*, Atti XV Convegno UMI-CIIM, in Notiziario U.M.I., Suppl. n. 5.

SHIDLOVSKII, A.B. (1989) *Transcendental Numbers*, Berlin, New York: Walter de Gruyter.

SLOANE, N. (2010) *The On–Line Encyclopedia of Integer Sequences*, pubblicazione elettronica su: `http://oeis.org`.

STRAFFIN, P.D. (1998) Liu Hui and the First Golden Age of Chinese Mathematics, *Math. Mag.*, 71(3), pp. 163–181.

TIMPANARO CARDINI (1978) *Commento al I libro degli Elementi di Euclide / Proclo; introduzione, traduzione e note a cura di Maria Timpanaro Cardini.* Pisa: Giardini.

VILLANI, V. (2003) *Cominciamo da Zero.* Bologna: Pitagora Editrice.

WEIL, A. (1984) *Number theory, an approach through history from Hammurapi to Legendre.* Boston : Birkhäuser. Trad. it.: (1993) *La Teoria dei numeri. Storia e matematica da Hammurabi a Legendre.* Torino: Einaudi.