Matematica, Cultura e Società

Rivista dell'Unione Matematica Italiana

Nadir Murru

Sulla rappresentazione periodica di irrazionali algebrici

Matematica, Cultura e Società. Rivista dell'Unione Matematica Italiana, Serie 1, Vol. **8** (2023), n.1, p. 79–88.

Unione Matematica Italiana

<http://www.bdim.eu/item?id=RUMI_2023_1_8_1_79_0>

L'utilizzo e la stampa di questo documento digitale è consentito liberamente per motivi di ricerca e studio. Non è consentito l'utilizzo dello stesso per motivi commerciali. Tutte le copie di questo documento devono riportare questo avvertimento.

Articolo digitalizzato nel quadro del programma
bdim (Biblioteca Digitale Italiana di Matematica)
SIMAI & UMI
http://www.bdim.eu/

Matematica, Cultura e Società. Rivista dell'Unione Matematica Italiana, Unione Matematica Italiana, 2023.

Matematica, Cultura e Società – Rivista dell'Unione Matematica Italiana
Serie I, Vol. 8, N. 1, aprile 2023, 79-88

Sulla rappresentazione periodica di irrazionali algebrici

Nadir Murru
Università di Trento
E-mail: nadir.murru@unitn.it

Sommario: *In questo articolo viene presentato il problema della rappresentazione di numeri irrazionali algebrici mediante successioni periodiche di interi. Tale problema fu posto nell'800 da Charles Hermite a Carl Jacobi e rimane tutt'ora un affascinante problema aperto nella teoria dei numeri. Inizieremo introducendo ed esaminando alcune proprietà delle frazioni continue che forniscono una soluzione del problema di Hermite per gli irrazionali quadratici e sono ad oggi gli unici irrazionali algebrici per cui abbiamo una risposta. Analizzeremo poi la risposta dello stesso Jacobi con l'introduzione delle frazioni continue multidimensionali.*

Abstract: *In this article we provide an overview about the problem of representing algebraic numbers by means of periodic sequences of integers. In the 800's, Charles Hermite asked this question to Carl Jacobi and this is still a fascinating open problem in number theory. We start defining and studying some properties of continued fractions that provide an answer to the Hermite's problem for quadratic irrationals and they are, until now, the only algebraic numbers for which we know an answer. Then, we analyze the Jacobi's answer who introduced multidimensional continued fractions.*

1. – Introduzione

"Dio creò i numeri interi, tutto il resto è opera dell'uomo" è la celebre frase del grande matematico Leopold Kronecker con cui esprimeva l'importanza dei numeri interi e del loro ruolo nel mondo al di sopra di tutto il resto. Ritroviamo questa 'visione metafisica' dei numeri già in Sant'Agostino che addirittura nella sua opera 'La città di Dio' scriveva "Sei è un numero perfetto di per sé, e non perché Dio ha creato il mondo in sei giorni; piuttosto è vero il contrario. Dio ha creato il mondo in sei giorni perché questo numero è perfetto, e rimarrebbe perfetto anche se l'opera dei sei giorni non fosse esistita". Questo interesse per i numeri, non solo dal punto di vista matematico, ma anche filosofico e religioso, lo troviamo per la prima volta nell'antica Grecia, con la scuola pitagorica (fondata intorno al 530 a.C.), in cui i numeri, ed in particolare i numeri interi, erano considerati la sostanza delle cose. Secondo i pitagorici tutto poteva essere espresso mediante i numeri interi. Questa concezione filosofica dell'universo entrò in profonda crisi quando Ippaso di Metaponto dimostrò l'irrazionalità di $\sqrt{2}$, ovvero l'esistenza di grandezze non commensurabili, non esprimibili come rapporto tra numeri interi.

Possiamo quindi pensare ai numeri irrazionali come a dei numeri che in un certo senso 'sfuggono' alla nostra razionalità, non possiamo esprimerli come rapporti di numeri interi, hanno un'espansione decimale infinita e non periodica che non possiamo predire. Potremmo dire, in effetti, che non siamo in grado di 'afferrare' questi numeri, quando parliamo ad esempio di $\sqrt{2}$, stiamo riferendoci a quel numero che moltiplicato per se stesso fa 2, ma di che numero si tratta? Per poterlo usare, azzarderei dire per poterlo conoscere, ci serve esprimerlo mediante dei numeri razionali, limitandoci ad usarne delle sue approssimazioni, senza poter usare veramente tale numero nella sua completezza. E così per tutti i numeri irrazionali, se dobbiamo effettuare dei calcoli che li coinvolgono, dobbiamo necessariamente usare dei numeri interi e, in particolare, delle loro appros-

Accettato: il 17 febbraio 2023.

simazioni razionali. Questo è uno dei motivi dell'importanza dell'approssimazione diofantea, che studia le approssimazioni dei numeri reali mediante numeri razionali e deve il proprio nome al matematico Diofanto di Alessandria (III-IV secolo d.C.) che con il suo libro 'Arithmetica', di cui sfortunatamente giungono a noi solo sei dei suoi tredici volumi, formalizza per la prima volta lo studio di equazioni a più incognite le cui soluzioni si ricercano solo tra i numeri interi. Quindi, malgrado la caduta dell'idea pitagorica che tutto fosse esprimibile mediante i numeri interi, rimane di centrale importanza il loro ruolo per poter veramente conoscere le cose.

In quest'ottica le frazioni continue e le loro generalizzazioni, che esploreremo nelle prossime sezioni, inseguono questo desiderio. Le frazioni continue permettono infatti di esprimere tutti i numeri reali mediante successioni di numeri interi (finite o infinite), fornendo le migliori approssimazioni razionali per i numeri irrazionali. Ma è il loro comportamento relativo agli irrazionali quadratici che, a mio parere, le rendono assolutamente affascinanti. Infatti, vedremo che gli irrazionali quadratici sono caratterizzati da sviluppi periodici in frazione continua, mettendo così un po' di ordine, dando un po' di razionalità, a questa classe di irrazionali. Questa particolarità delle frazioni continue affascinò sicuramente anche Hermite, spingendolo a porre a Jacobi un quesito, tuttora irrisolto, per fornire analoghe caratterizzazioni per irrazionali algebrici di gradi superiori, partendo dagli irrazionali cubici.

2. – Frazioni continue e loro definizione

Non è facile datare la nascita delle frazioni continue, esse appaiono già in tempi antichi, come in alcuni lavori del matematico indiano Aryabatha (circa 550 a.C). Inoltre, il loro stretto legame con l'algoritmo di Euclide ci lascia supporre che potessero essere conosciute ed usate anche nell'antica Grecia. Sicuramente ne troviamo traccia nei matematici bolognesi Bombelli (1526-1573) e Cataldi (1548-1626) che forniscono alcune rappresentazioni di irrazionali quadratici mediante frazioni continue, anche se tale argomento verrà introdotto e studiato con sistematicità solo a partire da Eulero (1707-1783). In seguito molti grandi matematici come Lagrange, Jacobi, Galois, Gauss ecc..., si dedicarono allo studio di questi oggetti, contribuendo con i loro risultati allo sviluppo di una teoria strutturata e di notevole spessore. Per un excursus storico sulle frazioni continue si consigliano i lavori di Brezinski [3] e Cretney [5].

Le frazioni continue suscitarono fin dal principio grande interesse in quanto il loro utilizzo permette di risolvere in maniera costruttiva molti problemi, come la risoluzione di vari tipi di equazioni, tra cui l'equazione di Pell. Inoltre, forniscono una rappresentazione assolutamente astratta dei numeri reali, individuandoli univocamente attraverso successioni di numeri interi, a differenza per esempio della notazione decimale, che risulta vincolata alla base numerica prescelta oltre a rappresentare in maniera poco conveniente alcuni numeri razionali che hanno invece uno sviluppo finito in frazione continua. D'altra parte anche la rappresentazione dei numeri tramite le normali frazioni, efficace per i numeri razionali, come detto non risulta esauriente in quanto è ovviamente inutilizzabile per i numeri irrazionali. Ricorrendo invece alle frazioni continue si ottiene un'espressione astratta e soddisfacente per tutti i numeri reali. Un ulteriore spunto di interesse è dato dalle approssimazioni che le frazioni continue forniscono per i numeri irrazionali. Infatti, come descriveremo meglio, le migliori approssimazioni razionali di un numero irrazionale sono fornite dalle frazioni continue. Come già accennato nell'introduzione, sono però le loro proprietà di periodicità a renderle definitivamente interessanti e affascinanti. Inoltre, le frazioni continue possono essere studiate con vari approcci, per via elementare, algebrica o analitica e sono molto studiate anche dal punto di vista combinatoriale, oltre ad avere importanti applicazioni in vari campi come, ad esempio, la crittografia. Alcuni testi che coprono questi vari aspetti delle frazioni continue sono i lavori di Kane [10], Olds [11] (che ne fornisce una panoramica di base di tutte le loro principali proprietà) e Wall [14].

Nella sua forma più generale, una frazione continua è un oggetto del tipo

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ddots}}.$$

dove gli a_i e b_i sono numeri complessi. In questo articolo, saremo interessati alle frazioni continue semplici e aritmetiche (che chiameremo poi solamente frazioni continue per brevità), dove i b_i sono tutti uguali a 1 e gli a_i sono numeri interi chiamati *quozienti parziali*. Indicheremo in breve con $[a_0, a_1, a_2, \ldots]$ una tale frazione continua che potrà essere finita o infinita. Un qualunque numero reale α_0 può essere espresso mediante una frazione continua $[a_0, a_1, a_2, \ldots]$, per opportuni quozienti parziali che si determinano mediante un algoritmo che itera i seguenti passi:

$$\begin{cases} a_i = \lfloor \alpha_i \rfloor \\ \alpha_{i+1} = \dfrac{1}{\alpha_i - a_i}, \quad \text{se } \alpha_i \notin \mathbb{Z}, \end{cases}$$

per ogni $i = 0, 1, \ldots$, dove i numeri reali α_i vengono chiamati *quozienti completi*. Nel caso in cui si abbia $\alpha_i \in \mathbb{Z}$ per qualche i, l'algoritmo si interrompe e lo sviluppo di α_0 è finito. Le precedenti equazioni ricorsive si ottengono facilmente dall'algoritmo di Euclide. Infatti, se $\alpha_0 = \dfrac{x_0}{x_1} \in \mathbb{Q}$, per calcolare il massimo comun divisore tra x_0 e x_1, otteniamo

$$\begin{aligned} x_0 &= a_0 x_1 + x_2, \quad a_0 = \lfloor x_0/x_1 \rfloor \\ x_1 &= a_1 x_2 + x_3, \quad a_1 = \lfloor x_1/x_2 \rfloor \\ &\ldots \\ x_i &= a_i x_{i+1} + x_{i+2}, \quad a_i = \lfloor x_i/x_{i+1} \rfloor \\ &\ldots \end{aligned}$$

da cui ponendo $\alpha_i = \dfrac{x_i}{x_{i+1}}$ si ha

$$\frac{x_i}{x_{i+1}} = a_i + \frac{x_{i+2}}{x_{i+1}} \Rightarrow \alpha_i = a_i + \frac{1}{\alpha_{i+1}}$$

con $a_i = \lfloor \alpha_i \rfloor$. Dunque, l'algoritmo per determinare l'espansione in frazione continua di un numero razionale finirà in un numero finito di passi e viceversa è immediato osservare che una frazione continua finita rappresenta sempre un numero razionale, ottenendo che i numeri razionali sono caratterizzati da espansioni finite in frazioni continue. Possiamo procedere formalmente con l'algoritmo di Euclide anche per un generico numero reale $\alpha_0 \notin \mathbb{Q}$, con la differenza che, in questo caso, l'algoritmo non terminerà e l'espansione di α_0 sarà infinita.

3. – Alcune proprietà delle frazioni continue

Per poter proseguire con l'analisi delle frazioni continue, iniziamo a vedere alcune definizioni e proprietà di base. Dato lo sviluppo in frazione continua di un numero reale $\alpha_0 = [a_0, a_1, a_2, \ldots]$, chiamiamo n-esimo convergente il numero razionale $[a_0, \ldots, a_n] = \dfrac{p_n}{q_n}$. È semplice dimostrare per induzione che i numeratori e denominatori dei convergenti possono essere calcolati mediante

$$\begin{cases} p_n = a_n p_{n-1} + p_{n-2} \\ q_n = a_n q_{n-1} + q_{n-2} \end{cases},$$

per ogni $n \geq 1$, ponendo le condizioni iniziali $p_{-1} = 1, p_0 = a_0$ e $q_{-1} = 0, q_0 = 1$, oppure mediante la seguente identità tra matrici:

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}.$$

Dalla precedente identità matriciale è immediato ottenere la proprietà fondamentale dei convergenti

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$$

e

$$\alpha_0 = \frac{\alpha_{n+1} p_n + p_{n-1}}{\alpha_{n+1} q_n + q_{n-1}}$$

per ogni $n \geq 0$.

I convergenti, nome non casuale in quanto la successione $(p_n/q_n)_{n \geq 0}$ converge appunto al numero reale α_0, svolgono un ruolo centrale nell'approssimazione dei numeri irrazionali. Infatti, i convergenti dello sviluppo in frazione continua di un numero irrazionale α_0 ne forniscono le migliori approssimazioni, nel senso che

$$\left| \alpha_0 - \frac{p_n}{q_n} \right| \leq \left| \alpha_0 - \frac{a}{b} \right|$$

dati qualunque interi a, b tali che $1 \leq b \leq q_n$. È anche semplice dimostrare la seguente disuguaglianza che fornisce un'indicazione sulla qualità di approssimazione dei convergenti:

$$\left| \alpha_0 - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Inoltre, se un numero razionale approssima α_0 con una certa precisione, in particolare se

$$\left|\alpha_0 - \frac{a}{b}\right| < \frac{1}{2b^2},$$

allora coincide necessariamente con uno dei convergenti dello sviluppo in frazione continua di α_0. Quest'ultima proprietà ha anche applicazioni in crittoanalisi, infatti nel 1990 Wiener esibì un attacco al famoso sistema crittografico a chiave pubblica RSA mediante le frazioni continue [15].

ESEMPIO 1 – *Vediamo un esempio di sviluppo in frazione continua di un numero irrazionale e le relative proprietà di approssimazione. Lo sviluppo di π in frazione continua è il seguente*:

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

Ottime approssimazioni di π furono fornite per la prima volta da Archimede di Siracusa (287 a. C.), che considerò come approssimazione per difetto di π, il semiperimetro di un poligono regolare inscritto nella circonferenza di raggio unitario e come valore per eccesso, quello di un poligono regolare circoscritto. Archimede partì considerando gli esagoni regolari e successivamente raddoppiò il numero di lati, considerando poligoni regolari inscritti e circoscritti di 12, 24, 48, e 96 lati (ovvero poligoni di $3 \cdot 2$, $3 \cdot 2^2$, $3 \cdot 2^3$, $3 \cdot 2^4$ e $3 \cdot 2^5$ lati). Con tale metodo arrivò alla celebre, e ottima, approssimazione $\frac{223}{71} < \pi < \frac{22}{7}$, dove $\frac{22}{7}$ è proprio un convergente della frazione continua.

Possiamo infatti calcolare i primi convergenti di π:

$$\frac{p_0}{q_0} = 3, \quad \frac{p_1}{q_1} = \frac{22}{7}, \quad \frac{p_2}{q_2} = \frac{333}{106}, \quad \frac{p_3}{q_3} = \frac{355}{113}$$

Osservando che $\left|\pi - \frac{p_3}{q_3}\right| < \frac{1}{q_3 q_4}$, possiamo aspettarci da p_3/q_3 un'ottima approssimazione di π, dal momento che $a_4 = 292$ è molto grande e la grandezza di q_4 dipende anche da esso.

Se le frazioni continue risultano molto interessanti e utili per rappresentare i numeri reali mediante successioni di interi e nell'ambito dell'approssimazione diofantea, è il loro comportamento rispetto agli irrazionali quadratici (ovvero numeri irrazionali radici di polinomi di secondo grado a coefficienti razionali) a mostrare tutta la loro bellezza. Infatti, ci apprestiamo a vedere come lo sviluppo in frazione continua di α_0 sia periodico se e solo se α_0 è un irrazionale quadratico, ovvero le frazioni continue forniscono una caratterizzazione davvero suggestiva per tali numeri, mediante una rappresentazione periodica di interi.

ESEMPIO 2 – *Se consideriamo $\alpha_0 = \sqrt{2}$, abbiamo immediatamente $a_0 = 1$ e*

$$\alpha_1 = \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1, \quad a_1 = 2,$$

da cui

$$\alpha_2 = \frac{1}{\sqrt{2} - 1} = \alpha_1,$$

ovvero lo sviluppo in frazione continua di $\sqrt{2}$ continuerà a ripetersi uguale, ottenendo

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}} = [1, \overline{2}].$$

Se cerchiamo lo sviluppo in frazione continua della sezione aurea $\varphi = \frac{1 + \sqrt{5}}{2}$, troviamo uno sviluppo veramente elegante:

$$\varphi = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}} = [\overline{1}].$$

Tale sviluppo lo si può ottenere facilmente applicando l'algoritmo che abbiamo visto in precedenza oppure possiamo verificarlo osservando che

$$\varphi = 1 + \frac{1}{\varphi}.$$

La dimostrazione che una qualunque frazione continua periodica rappresenta un irrazionale quadratico è dovuta ad Eulero e non è particolarmente complessa. Se consideriamo una frazione continua puramente periodica $\alpha_0 = [\overline{a_0, \ldots, a_n}]$, possiamo scrivere

$$\alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\alpha_0}}}}$$

e

$$\alpha_0 = \frac{\alpha_0 p_n + p_{n-1}}{\alpha_0 q_n + q_{n-1}}$$

da cui è immediato osservare che α_0 soddisfa un'equazione di secondo grado a coefficienti razionali. A questo punto, per dimostrare che una generica frazione continua periodica rappresenta un irrazionale quadratico è sufficiente osservare che una trasformazione lineare frazionaria di un irrazionale quadratico è ancora un irrazionale quadratico. Infatti, dato $\alpha_0 = [a_0, \ldots, a_k, \overline{a_{k+1}, \ldots, a_{k+t}}]$, si ha

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \beta & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \beta & 1 \\ 1 & 0 \end{pmatrix}$$

da cui $\alpha_0 = \dfrac{a\beta + b}{c\beta + d}$, dove $\beta = [\overline{a_{k+1}, \ldots, a_{k+t}}]$.
La dimostrazione del viceversa, ovvero che dato un irrazionale quadratico allora il suo sviluppo in frazione continua è periodico, è dovuta a Lagrange ed è un po' più elaborata. L'idea, essenzialmente, è di osservare prima di tutto che dato un irrazionale quadratico $\alpha_0 = \dfrac{P_0 + \sqrt{D}}{Q_0}$, i quozienti completi del suo sviluppo in frazione continua sono irrazionali quadratici della forma $\alpha_k = \dfrac{P_k + \sqrt{D}}{Q_k}$ dove i P_k e Q_k sono numeri interi determinabili mediante opportune relazioni ricorsive. Sfruttando tali relazioni e alcune proprietà delle frazioni continue è poi possibile dimostrare che i P_k e Q_k possono assumere solo un numero finito di valori, in particolare $-\sqrt{D} < P_k < \sqrt{D}$ e $0 < Q_k < 2\sqrt{D}$. Pertanto, esistendo solo un numero finito di coppie P_k, Q_k, esisteranno due indici i e j tali che $\alpha_i = \alpha_j$ e quindi lo sviluppo in frazione continua di α_0 risulta periodico.

Lo sviluppo in frazione continua delle radici quadrate di numeri interi positivi (non quadrati) è particolarmente interessante e utile. Il suo sviluppo ha sempre preperiodo di lunghezza uno e l'ultimo termine del periodo è due volte il termine del preperiodo:

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{L-1}, 2a_0}]$$

dove la stringa $a_1, \ldots a_{L-1}$ è palindroma. È abbastanza sorprendente osservare come lo sviluppo in frazione continua di $\sqrt{D}$ fornisca tutte e sole le soluzioni della famosa equazione di Pell

$$x^2 - Dy^2 = 1.$$

Infatti, è possibile dimostrare che la soluzione primitiva dell'equazione di Pell è (p_{L-1}, q_{L-1}) quando L è pari, (p_{2L-1}, q_{2L-1}) quando L è dispari.

Tutte queste interessanti e importanti proprietà delle frazioni continue legate agli irrazionali quadratici ispirarono Hermite per porre un problema a Jacobi sulla rappresentazione periodica di irrazionali algebrici, cercando di generalizzare a irrazionali di gradi maggiori tutte queste buone proprietà. Il problema di Hermite, che esploreremo nel dettaglio nelle prossime sezioni, rimane tuttora un affascinante problema irrisolto nella teoria dei numeri già per gli irrazionali cubici, non siamo ancora riusciti a determinare una generalizzazione delle frazioni continue che permetta di rappresentare ogni irrazionalità cubica con successioni periodiche di interi mediante un algoritmo che funzioni su tutti i numeri reali.

4. – Da due a tre

Prima di introdurre più formalmente il problema di Hermite e vedere la risposta di Jacobi e i successivi sviluppi di questo problema, vorrei sottolineare in questa sezione come il passaggio 'da due a tre' in matematica non sia sempre scontato e, anzi, sia molto spesso insidioso. Un esempio ci viene fornito subito dalle formule risolutive per le equazioni di secondo e terzo grado. Se per il primo caso fu molto

facile determinare la famosa formula risolutiva, e ne abbiamo testimonianze già intorno al 300-400 a.C., ben diversa fu la sorte per le equazioni di terzo grado. Dobbiamo infatti attendere il 1500 per arrivare a tale formula, con molti tentativi e anche affascinanti disfide matematiche che coinvolsero i matematici italiani Cardano, Del Ferro, Del Fiore, Ferrari, Tartaglia. Inoltre, la formula risolutiva può ritenersi non completamente soddisfacente per il suo cosiddetto caso irriducibile. Per risolvere un'equazione di terzo grado della forma $x^3 + px + q$ (si noti che possiamo sempre ricondurre una generica equazione di terzo grado a questa forma), la formula risolutiva ci porta a soluzioni del tipo

$$\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}+\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}.$$

Nel caso in cui $\frac{q^2}{4}+\frac{p^3}{27} < 0$ si parla di caso irriducibile e risulta intrattabile senza passare all'uso dei numeri complessi anche per esprimere la radice reale (sicuramente ne esiste sempre almeno una). Ad esempio per $x^3 - 2x + 1$ si ha come soluzione

$$\sqrt[3]{-\frac{1}{2}+\sqrt{-\frac{5}{108}}}+\sqrt[3]{-\frac{1}{2}-\sqrt{-\frac{5}{108}}}=1$$

e possiamo osservare che per ottenerla tramite la formula occorre usare i numeri complessi.

Un altro esempio, in questo caso dell'impossibilità di portare al caso tre ciò che vale nel caso due, è dato dalla trisezione dell'angolo. Sappiamo bene che siamo in grado di dividere in due parti uguali un angolo mediante una costruzione con riga e compasso, mentre questo risulta impossibile (a meno di casi particolari) nel caso della trisezione. Possiamo anche pensare al celebre ultimo teorema di Fermat. Se l'equazione diofantea $x^2 + y^2 = z^2$ ammette soluzioni intere non banali (le terne pitagoriche), invece le analoghe equazioni di grado superiore, a partire da $x^3 + y^3 = z^3$, non ne hanno come ha dimostrato solamente negli anni '90 il grande matematico Andrew Wiles, ponendo fine a una congettura che resisteva da secoli.

Concludo questa sezione con un ultimo esempio relativo ai cammini casuali. Nel 1921, Polya dimostrò che in due dimensioni un cammino casuale tornerà al punto di partenza con probabilità 1, mentre nelle tre dimensioni questa probabilità si riduce a circa 0.34. È molto divertente la descrizione di questo risultato da parte del matematico giapponese Kakutani: 'una persona ubriaca troverà la via di casa, ma un uccello ubriaco rischia di perdersi per sempre'.

5. – Il problema di Hermite

Nel 1839, Hermite pose a Jacobi il problema di estendere la costruzione delle frazioni continue in modo da ottenere un algoritmo che fornisse rappresentazioni periodiche mediante successioni di interi per irrazionalità algebriche, così come le frazioni continue lo fanno per le irrazionalità quadratiche. Un enunciato conciso di questo problema è proposto da Thomas Garrity: '*Find methods for writing numbers that reflect special algebraic properties*', [7]. Troviamo traccia del problema originale posto da Hermite in alcuni estratti delle sue lettere a Jacobi: '*Mais permettez-moi, Monsieur, de revenir un instant sur les circonstances remarquables, auxquelles donne lieu la reduction des formes dont les coefficients dependent de racines d'equations algebriques à coefficients entiers Peutetre parviendra-t-on à deduire de là, un systeme complet de caracteres pour chaque espece de ce genre de quantites,* ***analogue par example à cuex' que donne la theorie des fractions continues pour les racines des equations du second degrè***', [8].

Jacobi propose una sua soluzione al problema introducendo un nuovo algoritmo e definendo così delle nuove frazioni continue che chiameremo multidimensionali. A differenza del classico algoritmo per le frazioni continue, che prende in input un numero reale e vi associa una successione di interi, l'algoritmo di Jacobi prende come input una coppia di numeri reali (α_0, β_0) e vi associa una coppia di successioni di interi $(a_i)_{i\geq 0}, (b_i)_{i\geq 0}$:

$$\begin{cases} a_k = \lfloor \alpha_k \rfloor \\ b_k = \lfloor \beta_k \rfloor \\ \alpha_{k+1} = \dfrac{1}{\beta_k - b_k} \\ \beta_{k+1} = \dfrac{\alpha_k - a_k}{\beta_k - b_k} \end{cases}.$$

Scriveremo in breve

$$(\alpha_0, \beta_0) = [(a_0, a_1, a_2, ...), (b_0, b_1, b_2, ...)],$$

dove gli interi a_i, b_i verranno ancora chiamati quozienti parziali e i numeri reali α_i, β_i quozienti completi.

Questa generalizzazione dell'algoritmo per le frazioni continue che può sembrare a prima vista strana, visto che si passa dal cercare lo sviluppo di un numero reale all'usare insieme coppie di numeri reali, risulta invece naturale se si pensa al legame con l'algoritmo di Euclide. Infatti, l'algoritmo di Jacobi si può derivare da un metodo per determinare il massimo comun divisore tra tre numeri. Se prendiamo due numeri razionali $\alpha_0 = \dfrac{x_0}{z_0}$ e $\beta_0 = \dfrac{y_0}{z_0}$, per calcolare $\mathrm{MCD}(x_0, y_0, z_0)$ si può considerare

$$x_0 = a_0 z_0 + y_1, \quad y_0 = b_0 z_0 + z_1$$

con $a_0 = \lfloor \alpha_0 \rfloor$, $b_0 = \lfloor \beta_0 \rfloor$ e proseguire considerando la terna $(x_1 = z_0, y_1, z_1)$. In questo modo si ha

$$\alpha_1 = \frac{x_1}{z_1} = \frac{z_0}{y_0 - b_0 z_0} = \frac{1}{y_0/z_0 - b_0} = \frac{1}{\beta_0 - b_0}$$

e

$$\beta_1 = \frac{y_1}{z_1} = \frac{x_0 - a_0 z_0}{y_0 - b_0 z_0} = \frac{\alpha_0 - a_0}{\beta_0 - b_0},$$

ovvero si deriva l'algoritmo proposto da Jacobi [9]. Analogamente al caso delle classiche frazioni continue, possiamo formalmente usare la stessa idea nel caso di due numeri reali α_0 e β_0. Tale algoritmo può essere in realtà modificato in vari modi, modificando il metodo di aggiornamento delle terne (x_i, y_i, z_i), esistono infatti altri algoritmi proposti, ad esempio, da Poincaré [13] e Brun [4].

L'algoritmo di Jacobi, come vedremo, si comporta bene sugli irrazionali cubici, ma non abbastanza da risolvere il problema di Hermite, che rimane tuttora un bellissimo problema ancora aperto della matematica. Successivamente, nel 1906, Perron [12] estese l'algoritmo di Jacobi in modo da cercare di trattare la rappresentazione di ogni irrazionale algebrico. In questo caso si considera una m–upla di numeri reali $\alpha_0^{(1)}, ..., \alpha_0^{(m)}$ e viene associata ad essa una m-upla di successioni di interi $\left(a_k^{(1)}\right)_{k\geq 0}$, ..., $\left(a_k^{(m)}\right)_{k\geq 0}$ calcolati per mezzo delle seguenti equazioni:

$$\begin{cases} a_k^{(i)} = [\alpha_k^{(i)}], \quad i = 1, ..., m \\ \alpha_{k+1}^{(1)} = \dfrac{1}{\alpha_k^{(m)} - a_k^{(m)}} \\ \alpha_{k+1}^{(i)} = \dfrac{\alpha_k^{(i-1)} - a_k^{(i-1)}}{\alpha_k^{(m)} - a_k^{(m)}} \quad i = 2, ..., m \end{cases}.$$

Per una panoramica completa sulle proprietà e nozioni di base dell'algoritmo di Jacobi-Perron si veda [2]. Nella prossima sezione ci concentreremo solamente sull'originale algoritmo di Jacobi e sulle frazioni continue multidimensionali che ne derivano.

6. – Frazioni continue multidimensionali

Manipolando le equazioni che definiscono l'algoritmo di Jacobi è abbastanza semplice ottenere

$$\alpha_i = a_i + \frac{\beta_{i+1}}{\alpha_{i+1}}, \quad \beta_i = b_i + \frac{1}{\alpha_{i+1}}$$

per ogni $i \geq 0$, da cui si ottiene che le successioni dei quozienti parziali rappresentano i due numeri reali di partenza (α_0, β_0) nel seguente modo:

$$\alpha_0 = a_0 + \cfrac{1}{b_1 + \cfrac{1}{b_3 + \cfrac{1}{\ddots}}} \cfrac{}{a_2 + \cfrac{}{\ddots}} \cfrac{}{a_3 + \cfrac{}{\ddots}} \cfrac{}{\ddots} \cfrac{1}{b_2 + \cfrac{1}{\ddots}} \cfrac{}{a_3 + \cfrac{}{\ddots}} \cfrac{}{a_1 + \cfrac{}{\ddots}} \cfrac{1}{b_3 + \cfrac{1}{\ddots}} \cfrac{}{a_2 + \cfrac{}{\ddots}} \cfrac{}{a_3 + \cfrac{}{\ddots}}$$

e

$$\beta_0 = b_0 + \cfrac{1}{b_2 + \cfrac{1}{\ddots \; a_3 + \cfrac{\ddots}{\ddots \; a_1 + \cfrac{\ddots}{\ddots \; b_3 + \cfrac{1}{\ddots \; a_2 + \cfrac{\ddots}{\ddots \; a_3 + \cfrac{\ddots}{\ddots}}}}}}}.$$

Analogamente al caso classico una frazione continua multidimensionale finita rappresenta sempre una coppia di numeri razionali e, per quanto osservato nella precedente sezione, se $\alpha_0, \beta_0 \in \mathbb{Q}$ l'algoritmo termina in un numero finito di passi. Nel caso delle frazioni continue multidimensionali possiamo però osservare che anche nel caso in cui $\alpha_0, \beta_0 \notin \mathbb{Q}$ ma siano tra loro algebricamente dipendenti, allora l'algoritmo termina in un numero finito di passi, ma la frazione continua multidimensionale ottenuta non converge ai due numeri reali di partenza.

Le frazioni continue multidimensionali derivate dall'algoritmo di Jacobi offrono molte analogie con le classiche frazioni continue. Possiamo prima di tutto definire i convergenti di $(\alpha_0, \beta_0) = [(a_0, a_1, \ldots), (b_0, b_1, \ldots)]$ come

$$[\{a_0, a_1, ..., a_n\}, \{b_0, b_1, ..., b_n\}] = \left(\frac{A_n}{C_n}, \frac{B_n}{C_n}\right),$$

per ogni $n \geq 0$ dove

$$\begin{cases} A_n = a_n A_{n-1} + b_n A_{n-2} + A_{n-3} \\ B_n = a_n B_{n-1} + b_n B_{n-2} + B_{n-3} \\ C_n = a_n C_{n-1} + b_n C_{n-2} + C_{n-3} \end{cases}, \ \forall n \geq 1$$

e

$$\begin{pmatrix} a_0 & 1 & 0 \\ b_0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_n & 1 & 0 \\ b_n & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} A_n & A_{n-1} & A_{n-2} \\ B_n & B_{n-1} & B_{n-2} \\ C_n & C_{n-1} & C_{n-2} \end{pmatrix}$$

Dal punto di vista della periodicità possiamo osservare che frazioni continue multidimensionali periodiche convergono a irrazionali cubici. Infatti, Se consideriamo $(\alpha_0, \beta_0) = [\{\overline{a_0, \ldots, a_{N-1}}\}, \{\overline{b_0, \ldots, b_{N-1}}\}]$ si ha

$$\alpha_0 = \frac{\alpha_0 A_{N-1} + \beta_0 A_{N-2} + A_{N-3}}{\alpha_0 C_{N-1} + \beta_0 C_{N-2} + C_{N-3}}$$

e

$$\beta_0 = \frac{\alpha_0 B_{N-1} + \beta_0 B_{N-2} + B_{N-3}}{\alpha_0 C_{N-1} + \beta_0 C_{N-2} + C_{N-3}}$$

da cui si ottiene che α_0 e β_0 soddisfano un'equazione di terzo grado. A partire da ciò, è poi semplice mostrare il risultato anche per una generica frazione continua multidimensionale periodica. Sfortunatamente non è mai stato provato il viceversa. Ovvero non è mai stato dimostrato che data un irrazionale cubico α_0, esiste sempre un numero reale β_0 tale che l'algoritmo di Jacobi applicato a (α_0, β_0) fornisca un'espansione periodica. Si osservi che nel caso dell'algoritmo di Jacobi, la difficoltà nel dimostrare proprietà di periodicità, ma non solo, risulta maggiore anche per il fatto che non è predeterminata la scelta della coppia α_0, β_0, nel senso che dato α_0 non è scontata la scelta di β_0 in modo da ottenere buone proprietà, ad esempio in termini di periodicità, per il loro sviluppo in frazione continua multidimensionale.

Esistono alcuni risultati parziali sulla periodicità dell'algoritmo di Jacobi, per esempio è noto che $(\sqrt[3]{m^2}, \sqrt[3]{m})$, con $m = a^6 + 3a^3 + 3$ e a intero positivo tale che m non contenga cubi, ha uno sviluppo periodico.

ESEMPIO 3 – *Possiamo osservare che anche l'ordine con cui vengono presi i numeri reali nell'algoritmo di Jacobi è importante. Per esempio si ha*

$$\left(\sqrt[3]{2}, (\sqrt[3]{2^2}) = [(1, \overline{1,2}), (\overline{1,0})\right],$$

mentre

$$\left(\sqrt[3]{2^2}, (\sqrt[3]{2}) = [(1, \overline{3}), (1,2, \overline{3})\right].$$

Talvolta, il risultato può essere drasticamente diverso. Infatti possiamo vedere che

$$\left(\sqrt[3]{3}, (\sqrt[3]{3^2}) = [(1, 12, 1, 1, 1, 13, \ldots), (2, 5, 0, 0, 0, 0, \ldots)\right]$$

sembra non fornire uno sviluppo periodico, mentre invertendo l'ordine si ottiene

$$(\sqrt[3]{3^2}, \sqrt[3]{3}) = [(2, \overline{2, 5}), (1, 0, \overline{1})].$$

Concludiamo questo esempio con una bella analogia con la sezione aurea. La sezione aurea sappiamo essere la radice maggiore in modulo di $x^2 - x - 1$ *ed è limite del rapporto di termini consecutivi della successione di Fibonacci. Il suo analogo cubico è il numero di Tribonacci* μ*, ovvero la radice reale di* $x^3 - x^2 - x - 1$ *ed anch'esso è il limite di* $\left(\frac{T_{n+1}}{T_n}\right)_{n\geq 0}$ *con* $(T_n)_{n\geq 0}$ *successione di Tribonacci definita da*

$$\begin{cases} T_0 = 0, T_1 = 0, T_2 = 1 \\ T_n = T_{n-1} + T_{n-2} + T_{n-3} \end{cases}, \quad n \geq 3.$$

Il numero di Tribonacci μ *ha una rappresentazione particolarmente elegante in frazione continua multidimensionale:*

$$(\mu, 1/\mu) = [(\overline{1}), (0, \overline{1})]$$

oppure

$$(\mu, 1 + 1/\mu) = [(\overline{1}), (\overline{1})].$$

Le frazioni continue multidimensionali hanno anche un'applicazione interessante all'equazione cubica di Pell, così come le classiche frazioni continue ci permettono di risolvere l'equazione di Pell $x^2 - Dy^2 = 1$. Si potrebbe pensare che l'analogo cubico dell'equazione di Pell sia l'equazione diofantea $x^3 - Dy^3 = 1$. Tuttavia, se si osserva che il primo membro dell'equazione di Pell non è nient'altro che la norma di un elemento in $\mathbb{Q}[t]/(t^2 - D)$, risulta più naturale pensare all'equazione cubica di Pell come a

$$x^3 + Dy^3 + D^2z^3 - 3Dxyz = 1$$

dove il primo membro è la norma di un elemento in $\mathbb{Q}[\sqrt[3]{D}] \simeq \mathbb{Q}[t]/(t^3 - D)$, con D intero non cubo. L'equazione cubica di Pell risolta tuttora irrisolta, non abbiamo un metodo per generarne una soluzione primitiva a partire dalla quale ottenere tutte le sue soluzioni intere. Per approfondimenti si veda il libro di Barbeau interamente dedicato all'equazione di Pell e sue estensioni [1].

Il problema della risoluzione dell'equazione cubica di Pell è intrinsecamente legato alla periodicità dell'algoritmo di Jacobi. Infatti, Daus [6] dimostrò che se l'espansione di $(\sqrt[3]{D}, \sqrt[3]{D^2})$ è periodica, allora numeratori e denominatori dei convergenti, per opportuni indici, forniscono le soluzioni dell'equazione cubica di Pell.

Il problema di ottenere un analogo del teorema di Lagrange per le frazioni continue multidimensionali risulta quindi molto difficile da risolvere (si noti che al momento non sappiamo dire se sia vero o falso) ed è stato affrontato anche con l'ideazione di modifiche all'algoritmo di Jacobi, con la speranza di ottenere delle nuove frazioni continue multidimensionali per cui si riuscisse a dimostrare essere vero il teorema di Lagrange. Molti di questi tentativi prevedono di cambiare la mappa di costruzione dei quozienti completi. Possiamo infatti osservare che l'algoritmo di Jacobi si basa sulla seguente mappa di coppie di numeri reali per aggiornare i quozienti completi:

$$(\alpha, \beta) \mapsto \left(\frac{1}{\beta - \lfloor\beta\rfloor}, \frac{\alpha - \lfloor\alpha\rfloor}{\beta - \lfloor\beta\rfloor}\right).$$

Alcune lavori hanno proposto l'uso di mappe diverse come

$$(\alpha, \beta) \mapsto \left(\frac{1}{\alpha} - \left[\frac{1}{\alpha}\right], \frac{\beta}{\alpha} - \left[\frac{\beta}{\alpha}\right]\right)$$

e

$$(\alpha, \beta) \mapsto \left(\frac{\beta}{\alpha}, \frac{1 - \alpha - k\beta}{\alpha}\right)$$

con k numero intero calcolato in maniera dipendente da α e β. Tuttavia, tutti questi tentativi e molti altri, per quanto di notevole interesse, si sono rivelati infruttuosi. Ciò che si può ottenere, mediante un approccio puramente elementare, è però una scrittura periodica per ogni irrazionalità cubica. In particolare, dato $D \in \mathbb{Z}$ non cubo, si ha che lo sviluppo in frazione continua multidimensionale di $(\sqrt[3]{D^2}, \sqrt[3]{D})$ è

$$\left[\left(z, \frac{2z}{D}, \overline{\frac{3Dz}{z^3 + D^2}, 3z, \frac{3z}{D}}\right), \left(0, -\frac{z^2}{D}, \overline{-\frac{3z^2}{z^3 + D^2}, -\frac{3Dz^2}{z^3 + D^2}, -\frac{3z^2}{D}}\right)\right]$$

per ogni intero $z \neq 0$. Tale scrittura può poi essere generalizzata ad ogni irrazionale cubico. Si osservi

prima di tutto che la frazione continua multidimensionale periodica contiene quozienti parziali razionali, ma essa può essere trasformata in una con quozienti parziali interi. Il problema principale di questa scrittura periodica è che non possibile ottenerla mediante un algoritmo che lavori su un qualunque numero reale, non fornendo quindi una risposta completa al problema di Hermite. Ciò che si desidera con la risoluzione del problema di Hermite è un algoritmo che sia in grado di determinare certe proprietà algebriche dei numeri reali, in particolare indicare che un dato numero reale è o non è un irrazionale cubico mediante la periodicità o meno dell'algoritmo ad esso applicato.

Ringraziamenti

Desidero ringraziare Livia Giacardi per lo stimolo alla realizzazione di questo articolo. Ringrazio inoltre Stefano Barbero e Umberto Cerruti per le molte discussioni sugli argomenti di questo articolo e le idee da cui trae notevole ispirazione.

RIFERIMENTI BIBLIOGRAFICI

[1] E. J. Barbeau, Pell's equation, Problem Books in Mathematics, Springer, 2003.

[2] L. Bernstein, The Jacobi-Perron algorithm – its theory and application, Lecture Notes in Mathematics, Vol. 207, Springer-Verlag, Berlin-New York, 1971.

[3] C. Brezinski, History of continued fractions and Padé approximants, Springer Series in Computational Mathematics, Vol. 12, 1991.

[4] V. Brun, En generalisation av kjedebroken, Skrifter utgit av Videnskapsselskapet i Kristiania I, Matematisk-Naturvidenskabelig, 1920. Klasse

[5] R. Cretney, The origins of Euler's early work on continued fractions, Historia Mathematica, Vol. 41 (2014), 139-156.

[6] P. H. Daus, Normal ternary continued fraction expansions for the cube roots of integers, American Journal of Mathematics, Vol. 44 (1922), 279-296.

[7] T. Garrity, On periodic sequences for algebraic numbers, Journal of Number Theory, Vol. 88 (2001), 86-103.

[8] C. Hermite, Extraits de lettres de M. Ch. Hermite a M. Jacobi sur differents objets de la theorie des nombres, Journal für die reine und angewandte Mathematik, Vol. 40 (1850), 286.

[9] K. G. J. Jacobi, Allgemeine theorie der kettenbruchs algorithmen, in welchen jede zahl aus drei vorhergehenden gebildet wird, Journal für die reine und angewandte Mathematik, Vol. 69 (1868), 29-64.

[10] A. M. Kane, On the use of continued fractions for stream ciphers, Proceedings of the 2009 International Conference on Security and Management, (2009), 583-589.

[11] C. D. Olds, Continued fractions, Random House, 1963.

[12] O. Perron, Grundlagen fur eine theorie des Jacobischen kettenbruchalgorithmus, Mathematische Annalen, Vol. 64 (1907), 1-76.

[13] H. Poincaré, Sur une generalization des fractions continues, C. R. Acad. Sci. Paris. Ser. 1, Vol. 99 (1884), 1014-1016

[14] H. S. Wall, Analytic theory of continued fractions, D. Van Nostrand Company Inc. London, 1948.

[15] M. J. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Transaction on Information Theory, Vol. 36 (1990), 553-558.

Nadir Murru

Professore Associato di Algebra dal 2020 presso l'Università degli Studi di Trento, dove è membro del Laboratorio di Matematica Industriale e Crittografia. In precedenza ha ricoperto ruoli di ricerca presso Università e Politecnico di Torino, CNR di Pisa, Istituto Nazionale di Ricerca Metrologica. La sua ricerca si concentra sulla teoria dei numeri e la crittografia, con particolare interesse alla teoria delle successioni ricorrenti in anelli, frazioni continue e loro generalizzazioni, crittografia a chiave pubblica. è membro dell'Unione Matematica Italiana (UMI), Gruppo Crittografia e Codici, e dell'associazione di promozione sociale De Componendis Cifris.