Frazioni continue e equazioni di Pell

Rudy Cesaretto

Sommario

Questa tesi é essenzialmente un lavoro di approfondimento di alcuni argomenti inerenti le frazioni continue, trattati nel corso di Matematiche Complementari. Il lavoro si articola essenzialmente in tre sezioni principali.
Nella prima parte introduttiva, vengono richiamati alcuni concetti riguardanti le frazioni continue, sotto un punto di vista alternativo e con l'utilizzo di strumenti diversi (esempio: la notazione di Eulero); in particolare verranno trattate le frazioni continue periodiche. Nella seconda parte viene discussa l'equazione di Pell ed i suoi legami con i campi quadratici. Infine nell'ultima parte si sono considerati alcuni aspetti probabilistici delle frazioni continue.
Mentre nelle prime sezioni di questa tesi tutti i risultati vengono giustificati, nel capitolo 11 verranno soltanto enunciati teoremi complessi per la cui dimostrazione si rimanda ai testi indicati in bibliografia.

Indice

1 Introduzione

L'algoritmo di Euclide per la ricerca del massimo comun divisore tra due numeri naturali, puó essere formulato in un'altro modo, per effetto del quale il quoziente di quei due numeri viene rappresentato come frazione continua.

Esempio: Applichiamo l'algoritmo di Euclide ai numeri 67 e 24:

$$67 = 2 \times 24 + 19,$$
$$24 = 1 \times 19 + 5,$$
$$19 = 3 \times 5 + 4,$$
$$5 = 1 \times 4 + 1,$$
$$4 = 4 \times 1 + 0.$$

MCD(67,24)=1.
Scriviamo ora ciascuna equazione in forma frazionaria:

$$\frac{67}{24} = 2 + \frac{19}{24},$$
$$\frac{24}{19} = 1 + \frac{5}{19},$$
$$\frac{19}{5} = 3 + \frac{4}{5},$$
$$\frac{5}{4} = 1 + \frac{1}{4},$$

L'ultima frazione in ciascuna equazione é la reciproca della prima frazione nell'equazione successiva. Possiamo quindi eliminare tutte le frazioni intermedie ed esprimere quella originale $\frac{67}{24}$ nella forma

$$2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{4}}}}$$

Una tale espressione é detta *frazione continua finita*. Per convenienza sia tipografica che di notazione, si adotta la forma:

$$2 + \frac{1}{1+}\frac{1}{3+}\frac{1}{1+}\frac{1}{4}.$$

I numeri 2, 1, 3, 1, 4 sono detti *termini* della frazione continua o *quozienti parziali*. Un' altro tipo di notazione per la frazione continua in questione é la seguente:

$$\{2;\ 1,\ 3,\ 1,\ 4\}\ .$$

Mentre i numeri

$$\frac{67}{24}\ ;\quad \frac{24}{19}\ ;\quad \frac{19}{5}\ ;\quad \frac{5}{4}\ ;$$

sono detti *quozienti completi*.
Possiamo quindi dare una definizione piú generale di frazione continua ovvero: se $a_0,\ a_1,\ a_2,\ a_3,\ \ldots a_n$ sono indeterminate, definiremo la $frazione\ continua$ $\{a_0,\ a_1,\ a_2,\ a_3,\ \ldots a_n\ \}$ per ricorrenza, ponendo:

$$\{a_0;\}\ =\ a_0\ ;\quad \{a_0;\ a_1\ \}\ =\ a_0\ +\ \frac{1}{a_1}\ ;\quad \{a_0;\ a_1,\ a_2\ \}\ =\ a_0\ +\ \frac{1}{a_1\ +\ \frac{1}{a_2}}\ ;$$

$$\ldots\qquad \{a_0;\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ \}\ =\ a_0\ +\ \frac{1}{a_1\ +\ \frac{1}{a_2\ +\ \frac{1}{\ldots\ +\ \frac{1}{a_{n-1}\ +\ \frac{1}{a_n}}}}}\ ;$$

si tratta dunque di quozienti di polinomi nelle a_i che si puó scrivere:

$$a_0\ +\ \frac{1}{a_1\ +\ \frac{1}{a_2\ +\ \frac{1}{\ldots\ +\ \frac{1}{a_{n-1}\ +\ \frac{1}{a_n}}}}}\ ;$$

Se in una frazione continua si arresta la somma al termine a_i si ottiene la sua *convergente* (*o ridotta*) *i-esima* $\{a_0;\ a_1,\ a_2,\ \ldots,\ a_{i-1},\ a_i\ \} = \frac{p_i}{q_i}$.

Le frazioni continue semplici sono quelle in cui gli a_i sono numeri interi, con $a_i > 0$ per ogni $i > 0$.

Come si é visto, l'algoritmo di Euclide prova che ogni numero razionale si puó esprimere (in modo essenzialmente unico) come frazione continua finita. Se si sostituisce la n-upla $a_0, a_1, \ldots, a_n$ con la successione $a_0, a_1, \ldots, a_n, \ldots$ e si introducono le serie

$$\{a_0, a_1, \ldots, a_n, \ldots\} =\ a_0\ +\ \frac{1}{a_1\ +\ \frac{1}{a_2\ +\ \frac{1}{\ldots\ +\ \frac{1}{a_{n-1}\ +\ \frac{1}{a_n}\ldots}}}}$$

cioé le frazioni continue infinite, si prova che :
"*ogni numero reale non razionale si rappresenta in modo unico come frazione continua semplice infinita*" (vedi capitolo 4).

2 Regola di Eulero

Le frazioni continue hanno diversi tipi di notazione e di trattazione, e una delle piú efficaci é rappresentata dalla regola di Eulero. Vediamo ora in che cosa consiste tale regola e come puó essere applicata alle frazioni continue.

Definizione 1 *Se* $a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n$ *sono indeterminate, il simbolo* $[\ a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ ]$ *indicherá il polinomio ottenuto sommando i seguenti monomi:*

1. *il prodotto di tutti gli* $n+1$ *fattori* $a_0,\ a_1,\ a_2,\ a_3,\ \ldots a_n$*;*
2. *i prodotti di* $n-1$ *fattori ottenuti dal precedente prodotto* 1) *omettendo (in tutti i modi possibili) un paio di fattori contigui del tipo* $a_0a_1,\ a_1a_2,\ a_2a_3,\ \ldots,\ a_{n-1}a_n$*. Questo contributo alla somma é dunque:*

$$a_2a_3a_4\ldots a_{n-1}a_n\ +\ a_0a_3a_4\ldots a_{n-1}a_n\ +\ a_0a_1a_4\ldots a_{n-1}a_n\ +$$
$$+\ a_0a_1a_2\ldots a_{n-3}a_n\ +\ a_0a_1a_2\ldots a_{n-2}\ ;$$

3. *i prodotti di* $n-3$ *fattori, ottenuti dal precedente prodotto* 1) *omettendo (in tutti i modi possibili) due paia disgiunte di fattori contigui come* a_0a_1 *e* a_2a_3*,* a_0a_1 *e* a_3a_4*, ... ,* a_0a_1 *e* $a_{n-1}a_n$*, ... ,* a_1a_2 *e* a_3a_4*, ... ,*$a_{n-3}a_{n-2}$ *e* $a_{n-1}a_n$*. Questo contributo alla somma é dunque:*

$$a_4a_5\ldots a_{n-1}a_n+\ a_2a_5\ldots a_{n-1}a_n+\ a_2a_3a_6\ldots a_{n-1}a_n+\ \ldots+\ a_0a_1\ldots a_{n-4}\ ,$$

e cosí via.

4. *Quando* $n-1$ *é pari l'ultimo contributo é 1.*

Esempi:

$[\,]\ =\ 1;\ \ [a_0]=\ a_0;\ \ [a_0,\ a_1]\ =\ a_0a_1+1;\ \ [a_0,\ a_1,\ a_2]\ =\ a_0a_1a_2+a_2+a_0;$

$[a_0,\ \ a_1,\ \ a_2,\ \ a_3]\ \ =\ \ a_0a_1a_2a_3\ \ +\ \ a_2a_3\ \ +\ \ a_0a_3\ \ +\ \ a_0a_1\ \ +\ \ 1;$

$$[a_0,\ a_1,\ a_2,\ a_3,\ a_4]\ =\ a_0a_1a_2a_3a_4\ \ +\ \ a_2a_3a_4\ +\ a_0a_3a_4\ +\ a_0a_1a_4\ +$$
$$a_0a_1a_2\ \ +\ \ a_4\ +\ a_2\ +\ a_0;$$

e cosí via.

Lemma 1 *Sono valide le seguenti uguaglianze:*

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

$$\begin{aligned} ii)\ [\ a_0,\ a_1,\ldots,\ a_{n-1},\ a_n\ ] &= a_0[\ a_1,\ a_2,\ldots,\ a_{n-1},\ a_n\ ] + [\ a_2,\ a_3,\ldots,\ a_{n-1},\ a_n\ ] \\ &= [\ a_0,\ a_1,\ldots,\ a_{n-2},\ a_{n-1}\ ]a_n + [\ a_0,\ a_1,\ldots,a_{n-2}\ ] \end{aligned} \tag{2}$$

Dimostrazione
i) La definizione é combinatoria e la proprietá di due termini, di non essere contigui, si conserva quando si inverte l'ordine dei simboli a_i.

ii) Dobbiamo mostrare che

$$[\,a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\,] \ =\ a_0[\,a_1,\ a_2,\ a_3,\ \ldots,\ a_{n-1},\ a_n\,] + [\,a_2,\ a_3,\ \ldots,\ a_{n-1},\ a_n\,].$$

Ora considerando il secondo membro di tale uguaglianza, l'addendo $a_0[a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\,]$ contiene tutti e soli gli addendi di $[\ a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ ]$ in cui é presente il paio a_0, a_1.
Invece $[a_2,\ a_3,\ \ldots,\ a_{n-1},\ a_n\,]$ contiene tutti e soli gli addendi di $[\,a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\,]$ in cui il paio a_0, a_1 non é ammesso.
Pertanto il valore al secondo membro é esattamente il valore al primo membro.
La successiva uguaglianza é analoga, ma si ottiene scambiando a_0 con a_n, a_1 con a_{n-1}, a_2 con a_{n-2}, e cosí via. □

3 Frazione continua generale e suoi convergenti

Vediamo ora come si puó usare la regola di Eulero per esprimere lo sviluppo in frazioni continue.
Se le a_i sono indeterminate, continuano ad avere significato (non numerico, ma di quozienti di polinomi $\frac{p_i}{q_i}$) le espressioni del capitolo 1. Scriveremo cioé:

$$\{a_0; a_1, a_2, \ldots, a_n\} = \; a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\ldots\frac{1}{a_n} \; .$$

Se n=1

$$\{a_0, a_1\} = \; a_0 + \frac{1}{a_1} \; = \; \frac{a_0a_1+1}{a_1} \; ;$$

Se n=2

$$\{a_0, a_1, a_2\} = \; a_0 + \frac{1}{a_1+}\frac{1}{a_2} \; = \; \frac{a_0a_1a_2+a_0+a_2}{a_1a_2+1} \; ;$$

e cosí via.
Proviamo che in generale vale il seguente teorema:

Teorema 1 *Per le convergenti* $\frac{p_n}{q_n}$ *della frazione continua* $\{a_0;\ a_1,\ a_2,\ a_3,\ \ldots a_n\}$ *risulta:*

$$\begin{aligned} i)\ p_n = [\ a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n\ ] &= a_n[\ a_0,\ \ldots,\ a_{n-1}\ ] + [\ a_0, \ldots, a_{n-2}] = \\ &= a_np_{n-1} + p_{n-2} \end{aligned} \tag{3}$$

$$\begin{aligned} ii)\ q_n = [\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ ] &= a_n[\ a_1,\ \ldots,\ a_{n-1}\ ] + [\ a_1, \ldots, a_{n-2}] = \\ &= a_nq_{n-1} + q_{n-2} \end{aligned} \tag{4}$$

Dimostrazione
i) e ii) Per i valori iniziali si ha che:

$$p_0 = [a_0] = a_0 \; ; \qquad p_1 = [\ a_0, a_1\ ] = a_0a_1 + 1 \; ;$$

$$q_0 = [\ ] = 1 \; ; \qquad q_1 = [\ a_1\ ] = a_1 \; ;$$

Per induzione sia $p_i = [\ a_0,\ a_1,\ \ldots,\ a_{i-1},\ a_i\ ]$ e $q_i = [\ a_1,\ \ldots,\ a_{i-1},\ a_i\ ]$ per ogni $i < n$.

Dalla definizione di frazione continua si ha che:

$$\begin{aligned}
\frac{p_n}{q_n} &= \{\, a_0; a_1, a_2, \ldots, a_n\} = a_0 + \frac{1}{\{a_1; a_2, \ldots, a_n\}} = \\
&= a_0 + \frac{1}{\frac{[\ a_1,\ a_2,\ \ldots,\ a_n\ ]}{[\ a_2,\ a_3,\ \ldots,\ a_n\ ]}} = a_0 + \frac{[\ a_2,\ a_3,\ \ldots,\ a_n\ ]}{[\ a_1,\ a_2,\ \ldots,\ a_n\ ]} = \\
&= \frac{a_0[\ a_1,\ a_2,\ \ldots,\ a_n\ ] + [\ a_2,\ a_3,\ \ldots,\ a_n\ ]}{[\ a_1,\ a_2,\ \ldots,\ a_n\ ]} = \\
&= \frac{[\ a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n\ ]}{[\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ ]}
\end{aligned}$$

La frazione continua generale ha dunque un valore dato da:

$$\frac{p_n}{q_n} = \{a_0; a_1, \ldots, a_n\} = a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots \frac{1}{a_n} = \frac{[\ a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n\ ]}{[\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ ]} \quad (5)$$

Tornando alla penultima uguaglianza si ha che:

$$\begin{aligned}
\frac{p_n}{q_n} &= \frac{a_0[\ a_1,\ a_2,\ \ldots,\ a_n\ ] + [\ a_2,\ a_3,\ \ldots,\ a_n\ ]}{[\ a_1,\ a_2,\ \ldots,\ a_n\ ]} = \\
&= \frac{a_n[\ a_{n-1},\ a_{n-2},\ \ldots,\ a_0\ ] + [\ a_{n-2},\ a_{n-3},\ \ldots,\ a_0\ ]}{[\ a_n,\ a_{n-1},\ \ldots,\ a_1\ ]} = \\
&= \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}}\ .
\end{aligned}$$

□

Nella frazione continua generale $\frac{[\ a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n\ ]}{[\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ ]}$ nulla si puó semplificare.
che primi Si dimostra che numeratore e denominatore sono polinomi *irriducibili* nelle indeterminate $a_0, a_1, \ldots, a_n$.

Proposizione 1 *Qualsiasi coppia di convergenti consecutive, nello sviluppo in frazioni continue di un numero, soddisfa la relazione:*

$$p_m q_{m-1} - p_{m-1} q_m = (-1)^{m-1} \quad (6)$$

Dimostrazione Sia m=1 allora:

$$p_0 = [a_0] = a_0\ ; \qquad p_1 = [\ a_0, a_1\ ] = a_0 a_1 + 1\ ;$$

$$q_0 = [\ ] = 1\ ; \qquad\qquad q_1 = [\ a_1\ ] = a_1\ ;$$

Pertanto

$$p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) \cdot 1\ -\ a_0 a_1 = 1$$

Usando le relazioni (3) e (4) si ottiene che:

$$\begin{aligned} p_m q_{m-1}\ &-\ p_{m-1} q_m = \\ &= (a_m p_{m-1} + p_{m-2}) q_{m-1} - p_{m-1}(a_m q_{m-1} + q_{m-2}) \\ &= -(p_{m-1} q_{m-2} - p_{m-2} q_{m-1})\ . \end{aligned}$$

Pertanto se chiamo il primo membro della relazione (6) Δ_m si ha che:

$$\Delta_m = -\Delta_{m-1}$$

e continuando

$$\Delta_m = -\Delta_{m-1} = +\Delta_{m-2} = \ldots = \pm\Delta_1$$

ma, come visto sopra, $\Delta_1 = 1$, perció

$$\Delta_m = (-1)^{m-1}$$

□

Come conseguenza si ha che p_m e q_m sono primi tra loro poiché ogni eventuale fattore comune deve dividere 1. Pertanto la frazione $\frac{p_m}{q_m}$ che rappresenta una convergente generica é ridotta ai minimi termini. In particolare prendendo $m = n$ ció é vero per la formula (5) sul valore di una frazione continua generica. Abbiamo cosí dimostrato che nella frazione continua generale nulla si puó semplificare tra numeratore e denominatore.

4 Sviluppo in frazioni continue di un numero reale

$\frac{a}{b}$ $\frac{a}{b}$, Per una frazione continua semplice, in cui gli a_i sono interi positivi, si possono stabilire relazioni relative all'ordinamento naturale dei numeri razionali. Infatti partendo dalla (6) e dividendo per $q_{m-1}q_m$ si ottiene:

$$\frac{p_m}{q_m} - \frac{p_{m-1}}{q_{m-1}} = \frac{(-1)^{m-1}}{q_m q_{m-1}} \tag{7}$$

La differenza al primo membro é positiva se m é dispari, e negativa se m é pari. Poiché $q_0, q_1, q_2, \ldots$ crescono costantemente, tale differenza decresce al crescere di m.
Pertanto:

$$\frac{p_1}{q_1} > \frac{p_0}{q_0}$$

$$\frac{p_2}{q_2} < \frac{p_1}{q_1} \qquad ma \qquad \frac{p_0}{q_0} < \frac{p_2}{q_2}$$

$$\frac{p_3}{q_3} > \frac{p_2}{q_2} \qquad ma \qquad \frac{p_1}{q_1} > \frac{p_3}{q_3}$$

e cosí via.
Alla fine segue che tutti i convergenti pari ($\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \ldots$) sono minori di ogni convergente dispari, mentre tutti i convergenti dispari ($\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \ldots$) sono maggiori di ogni convergente pari.

Con l'algoritmo di Euclide abbiamo trovato l'espressione dei numeri razionali in frazioni continue. Cosí come si é anticipato al capitolo 1 é anche possibile rappresentare un numero irrazionale con le frazioni continue, pur di sostituire le somme con le serie.
Sia γ un numero irrazionale arbtrario. Allora

$$\gamma = a_0 + \frac{1}{\gamma_1} \qquad \text{ove } a_0 = [\gamma] \qquad (\ a_0 = \text{parte intera di } \gamma)$$

$$\text{e } 0 < \frac{1}{\gamma_1} < 1 \qquad (\ \frac{1}{\gamma_1} = \text{ parte frazionaria di } \gamma)$$

Ora $\gamma_1 > 1$ perció:

$$\gamma_1 = a_1 + \frac{1}{\gamma_2} \qquad \text{ove } a_1 = [\gamma_1] \qquad (\ a_1 = \text{parte intera di } \gamma_1)$$

$$\text{e } 0 < \frac{1}{\gamma_2} < 1 \qquad (\ \frac{1}{\gamma_2} = \text{ parte frazionaria di } \gamma_1)$$

Iterando il processo si ottiene:

$$\gamma_n = a_n + \frac{1}{\gamma_{n+1}} \qquad \text{ove } a_n = [\gamma_n] \qquad (\ a_n = \text{parte intera di } \gamma_n)$$
$$\text{e } 0 < \frac{1}{\gamma_{n+1}} < 1 \qquad (\ \frac{1}{\gamma_{n+1}} = \text{ parte frazionaria di } \gamma_n)$$

e quindi:

$$\gamma = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n+}\frac{1}{\gamma_{n+1}} \tag{8}$$

ove $a_1, a_2, \ldots, a_n \in \mathbb{N}$ (notiamo che a_0 puó essere positivo, negativo o nullo, se $\gamma > 1$ allora $a_0 > 0$). Utilizzando la regola di Eulero, valida anche per numeri reali qualsiasi, si ottiene:

$$\gamma = \frac{[\ a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n,\ \gamma_{n+1}\ ]}{[\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n,\ \gamma_{n+1}\ ]}$$

ove

$$\begin{aligned}[\ a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n,\ \gamma_{n+1}\ ] &= \gamma_{n+1}[\ a_0,\ a_1,\ \ldots,\ a_{n-1},\ a_n\ ] + [\ a_0,\ a_1,\ \ldots,\ a_{n-1}\ ] \\ &= \gamma_{n+1}p_n + p_{n-1}\end{aligned}$$

e

$$\begin{aligned}[\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n,\ \gamma_{n+1}\ ] &= \gamma_{n+1}[\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n\ ] + [\ a_1,\ a_2,\ \ldots,\ a_{n-1}\ ] \\ &= \gamma_{n+1}q_n + q_{n-1}\end{aligned}$$

Quindi

$$\gamma = \frac{\gamma_{n+1}p_n + p_{n-1}}{\gamma_{n+1}q_n + q_{n-1}}\ . \tag{9}$$

A questo punto é opportuno mostrare che la convergente $\frac{p_n}{q_n}$ effettivamente tende ad γ per $n \to \infty$.

Proposizione 2 *Mostriamo che*

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \gamma$$

o il che é equivalente

$$\lim_{n\to\infty} \left|\gamma - \frac{p_n}{q_n}\right| = 0$$

Dimostrazione

$$\begin{aligned}\left|\gamma - \frac{p_n}{q_n}\right| &= \left|\frac{\gamma_{n+1}p_n + p_{n-1}}{\gamma_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n}\right| \\ &= \left|\frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(\gamma_{n+1}q_n + q_{n-1})}\right| \\ &= \frac{1}{q_n(\gamma_{n+1}q_n + q_{n-1})} \qquad \text{per la (6) .}\end{aligned}$$

Ora poiché $\gamma_{n+1} > a_{n+1}$ si ottiene che:

$$\left|\gamma - \frac{p_n}{q_n}\right| < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_n q_{n+1}} \tag{10}$$

ma essendo $q_0, q_1, \ldots, q_n$ naturali strettamente crescenti si ha che:

$$\frac{1}{q_n q_{n+1}} \to 0 \qquad \text{per } n \to \infty$$

quindi

$$\left|\gamma - \frac{p_n}{q_n}\right| \to 0 \qquad \text{per } n \to \infty$$

cioé $\frac{p_n}{q_n}$ converge ad γ per $n \to \infty$. □

Abbiamo visto che ogni numero reale γ si puó scrivere come frazione continua. Sorge ora naturale chiedersi: *"data una sequenza qualunque di numeri interi positivi (eccetto il primo) $a_0, a_1, \ldots, a_n, \ldots$ la frazione continua $\{a_0; a_1, \ldots, a_n, \ldots\}$ ha significato, cioé la serie converge?"*
La risposta é sí, infatti proviamo che la successione delle convergenti ha un limite.
Considerando la successione delle convergenti pari $(\frac{p_0}{q_0}, \frac{p_2}{q_2}, \frac{p_4}{q_4}, \ldots)$ sappiamo che essa é crescente e superiormente limitata da $\frac{p_1}{q_1}$. Dunque la successione ammete limite.
Analogamente la successione delle convergenti dispari $(\frac{p_1}{q_1}, \frac{p_3}{q_3}, \frac{p_5}{q_5}, \ldots)$ é decrescente e inferiormente limitata da $\frac{p_0}{q_0}$. Dunque la successione ammette limite.
Ora questi due limiti concidono perché per la (7) la differenza tra due convergenti tende a zero per n che tende ad infinito.
Pertanto é possibile attribuire un significato numerico a qualsiasi frazione continua semplice, anche infinita.

"Ma la scrittura in frazione continue é unica anche per gli sviluppi infiniti?"
Anche in questo caso la risposta é si. Infatti se γ é il limite di cui prima si parlava allora

$$\gamma = a_0 + \frac{1}{\gamma_1} \qquad \text{ove } a_0 = [\gamma] \qquad (\ a_0 = \text{parte intera di } \gamma)$$
$$\text{e } 0 < \frac{1}{\gamma_1} < 1 \qquad (\ \frac{1}{\gamma_1} = \text{ parte frazionaria di } \gamma)$$

analogamente

$$\gamma_1 = a_1 + \frac{1}{\gamma_2} \qquad \text{ove } a_1 = [\gamma_1] \qquad (\ a_1 = \text{parte intera di } \gamma_1)$$
$$\text{e } 0 < \frac{1}{\gamma_2} < 1 \qquad (\ \frac{1}{\gamma_2} = \text{ parte frazionaria di } \gamma_1)$$

e cosí via. Perció la frazione continua é unica.

Osservazione 1 *Le frazioni continue forniscono un mezzo per costruire numeri irrazionali, e anzi stabiliscono una corrispondenza biunivoca tra gli irrazionali maggiori di 1 e le sequenze infinite di numeri naturali* $(a_0, a_1, \dots, a_n, \dots)$.

5 Irrazionali quadratici

I numeri irrazionali che sono zeri di polinomi irriducibili quadratici a coefficienti razionali si dicono *irrazionali quadratici*. In particolare la radice quadrata di un qualsiasi naturale N che non sia un quadrato perfetto é un irrazionale quadratico, in quanto soluzione dell'equazione $x^2 - N = 0$.

Lagrange dimostró che un numero é un irrazionale quadratico se e solo se si rappresenta come frazione continua periodica, cioé da un certo indice r in poi, gli interi a_i si ripetono periodicamente. In tale caso scriveremo:

$$\gamma = \{a_0; a_1, a_2, \ldots, \underbrace{a_r, a_{r+1}, \ldots, a_{r+k}}, \underbrace{a_r, a_{r+1}, \ldots, a_{r+k}}, \ldots\}$$

che scriveremo con il simbolo

$$\gamma = \{a_0; a_1, a_2, \ldots, \overline{a_r, a_{r+1}, \ldots, a_{r+k}}\}$$

Esempio 1:

$$\gamma = \sqrt{2} = 1 + (\sqrt{2} - 1) \qquad \text{ove } a_0 = 1 \qquad \text{e } \sqrt{2} - 1 = \frac{1}{\gamma_1} \ ;$$

$$\gamma_1 = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{2 - 1} = 2 + (\sqrt{2} - 1) \qquad \text{ove } a_1 = 2 \qquad \text{e } \sqrt{2} - 1 = \frac{1}{\gamma_2} \ ;$$

$$\gamma_2 = \frac{1}{\sqrt{2} - 1} = \frac{\sqrt{2} + 1}{2 - 1} = 2 + (\sqrt{2} - 1) \qquad \text{ove } a_2 = 2 \qquad \text{e } \sqrt{2} - 1 = \frac{1}{\gamma_3} \ ;$$

e cosí via. Perció si ha che:

$$\gamma = \sqrt{2} = 1 + \frac{1}{2+}\frac{1}{2+}\frac{1}{2+}\ldots = \{1; \overline{2}\} \ .$$

Esempio 2:

$$\gamma = \frac{24-\sqrt{15}}{17} = 1 + \left(\frac{7-\sqrt{15}}{17}\right) \qquad \text{ove } a_0 = 1 \qquad \text{e } \frac{7-\sqrt{15}}{17} = \frac{1}{\gamma_1} \ ;$$

$$\gamma_1 = \frac{17}{7-\sqrt{15}} = \frac{17(7+\sqrt{15})}{49-15} = 5 + \frac{\sqrt{15}-3}{2} \qquad \text{ove } a_1 = 5 \qquad \text{e } \frac{\sqrt{15}-3}{2} = \frac{1}{\gamma_2} \ ;$$

$$\gamma_2 = \frac{2}{\sqrt{15}-3} = \frac{2(\sqrt{15}+3)}{15-9} = 2 + \frac{\sqrt{15}-3}{3} \qquad \text{ove } a_2 = 2 \qquad \text{e } \frac{\sqrt{15}-3}{3} = \frac{1}{\gamma_3} \ ;$$

$$\gamma_3 = \frac{3}{\sqrt{15}-3} = \frac{3(\sqrt{15}+3)}{15-9} = 3 + \frac{\sqrt{15}-3}{2} \qquad \text{ove } a_3 = 3 \qquad \text{e } \frac{\sqrt{15}-3}{2} = \frac{1}{\gamma_4} \ ;$$

$$\gamma_4 = \frac{2}{\sqrt{15}-3} = \frac{2(\sqrt{15}+3)}{15-9} = 2 + \frac{\sqrt{15}-3}{3} \qquad \text{ove } a_4 = 2 \qquad \text{e } \frac{\sqrt{15}-3}{3} = \frac{1}{\gamma_5} \ ;$$

e cosí via. Perció si ha che:

$$\gamma = \frac{24-\sqrt{15}}{17} = 1 + \frac{1}{5+}\frac{1}{2+}\frac{1}{3+}\frac{1}{2+}\ldots = \{1; 5, \overline{2,3}\} \ .$$

5.1 Frazioni continue puramente periodiche

Iniziamo ora a trattare frazioni continue che sono periodiche fin dall'inizio, ovvero il cui periodo inizia con a_0.
Esempio:
Sia γ il seguente numero reale:

$$\begin{aligned}\gamma &= 4+\frac{1}{1+}\frac{1}{3+}\frac{1}{4+}\frac{1}{1+}\frac{1}{3+}\frac{1}{4+}\dots \\ \gamma &= 4+\frac{1}{1+}\frac{1}{3+}\frac{1}{\gamma} = 4+\frac{1}{1+\frac{1}{3+\frac{1}{\gamma}}} = \{4;1,3,\gamma\}\end{aligned}$$

da cui si ottiene la seguente equazione quadratica verificata da γ :

$$\gamma = \frac{19\gamma+5}{4\gamma+1} \qquad \Longleftrightarrow \qquad 4\gamma^2-18\gamma-5=0 \tag{11}$$

Consideriamo le prime convergenti di γ:

$$\frac{p_0}{q_0}=\frac{4}{1}\,; \qquad \frac{p_1}{q_1}=\frac{5}{1}\,; \qquad \frac{p_2}{q_2}=\frac{19}{4}\,;$$

Sia ora β il numero definito allo stesso modo di γ ma con il periodo rovesciato:

$$\begin{aligned}\beta &= 3+\frac{1}{1+}\frac{1}{4+}\frac{1}{3+}\frac{1}{1+}\frac{1}{4+}\frac{1}{3+}\dots \\ \beta &= 3+\frac{1}{1+}\frac{1}{4+}\frac{1}{\beta} = 3+\frac{1}{1+\frac{1}{4+\frac{1}{\beta}}} = \{3;1,4,\beta\}\end{aligned}$$

da cui si ottiene la seguente equazione quadratica verificata da β :

$$\beta = \frac{19\beta+4}{5\beta+1} \qquad \Longleftrightarrow \qquad 5\beta^2-18\beta-4=0 \tag{12}$$

Consideriamo le prime convergenti di β:

$$\frac{p_0}{q_0}=\frac{3}{1}\,; \qquad \frac{p_1}{q_1}=\frac{4}{1}\,; \qquad \frac{p_2}{q_2}=\frac{19}{5}\,;$$

L'equazione (12) é strettamente legata all'equazione (11). Infatti ponendo $-\frac{1}{\beta} = \gamma$, l'equazione (12) si trasforma nella (11).
Notiamo che $-\frac{1}{\beta} \neq \gamma$ in quanto γ e β sono entrambi positivi mentre $-\frac{1}{\beta}$ é negativo. Pertanto esso é la seconda radice dell'equazione (11).

Riassumendo, le due radici dell'equazione (11) sono rispettivamente γ e $-\frac{1}{\beta}$. Quest'ultimo numero é denominato *coniugato algebrico di* γ e lo si denoterá come γ' .

Si puó a questo punto enunciare il seguente teorema attribuito a Galois (1828):

Teorema 2 *Una frazione continua semplice é puramente periodica se e solo se:*

i) γ *é un numero reale algebrico di grado 2 su* $\mathbb{Q}$ *;*

ii) $\gamma > 1$ *;*

iii) il coniugato di γ *soddisfa alla disuguaglianza* $-1 < \gamma' < 0$.

In particolare se γ *soddisfa alle i), ii), iii)* γ *si dice* ridotto.

Dimostrazione " $\Longrightarrow$" Sia $\gamma = \{\overline{a_0; a_1, a_2, \ldots, a_n}\}$.
Se il periodo inizia con a_0 allora $a_0 = a_{n+1} \geq 1$, e cioé $\gamma > 1$ (ii).
Inoltre dall'equazione generale

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

segue che

$$q_n \gamma^2 - (p_n - q_{n-1})\gamma - p_{n-1} = 0$$

essendo $\gamma_{n+1} = \gamma$. Il polinomio di secondo grado

$$f(x) = q_n x^2 - (p_n - q_{n-1})x - p_{n-1}$$

é irriducibile in $\mathbb{Q}[x]$, perché la frazione continua non é finita e in quanto tale rappresenta un irrazionale (i).
Infine per la regola di Eulero si ha:

$$p_n = [a_0, a_1, \ldots, a_n] \qquad\qquad q_n = [a_1, a_2, \ldots, a_n]$$

Consideriamo ora la frazione continua che si ottiene da γ rovesciando il periodo:

$$\beta = \{\overline{a_n; a_{n-1}, \ldots, a_0}\}$$

Notiamo che β é maggiore di 1 essendo $a_n \geq 1$ e dall'equazione generale si ha:

$$\beta = \frac{\beta_{n+1}p_n + q_n}{\beta_{n+1}p_{n-1} + p_{n-1}} = \frac{\beta p_n + q_n}{\beta p_{n-1} + p_{n-1}}$$

da cui

$$p_{n-1}\beta^2 - (p_n - q_{n-1})\beta - q_n = 0$$

che é equivalente all'equazione:

$$q_n\left(-\frac{1}{\beta}\right)^2 - (p_n - q_{n-1})\left(-\frac{1}{\beta}\right) - p_{n-1} = 0$$

Allora $-\frac{1}{\beta}$ é zero di $f(x)$ diverso da γ e poiché $\beta > 1$ si ha che $-1 < -\frac{1}{\beta} < 0$, cioé $-\frac{1}{\beta}(= \gamma')$ soddisfa la iii).

" $\Longleftarrow$" Sia γ zero reale positivo del polinomio $f(x) = ax^2 + bx + c$ irriducibile in $\mathbb{Z}[x]$; sia poi γ' l'altro zero di $f(x)$ e si supponga che $-1 < \gamma' < 0$. Quindi

$$\begin{aligned} \gamma &= \frac{-b + \sqrt{b^2 - 4ac}}{2a} = \frac{P + \sqrt{D}}{Q} \\ \gamma' &= \frac{-b - \sqrt{b^2 - 4ac}}{2a} = \frac{P - \sqrt{D}}{Q} \end{aligned}$$

ove $P, Q \in \mathbb{Z}$ e D intero positivo (non quadrato).
Per ipotesi γ é ridotto, allora $\gamma > 1$ e $-1 < \gamma' < 0$, pertanto:

1. $\gamma - \gamma' > 0 \quad \Longrightarrow \quad \frac{2\sqrt{D}}{Q} > 0 \quad \Longrightarrow \quad Q > 0$
2. $\gamma + \gamma' > 0 \quad \Longrightarrow \quad \frac{2P}{Q} > 0 \quad \Longrightarrow \quad P > 0$
3. $\gamma' < 0 \quad \Longrightarrow \quad \frac{P - \sqrt{D}}{Q} < 0 \quad \Longrightarrow \quad P < \sqrt{D}$
4. $\gamma > 1 \quad \Longrightarrow \quad \frac{P + \sqrt{D}}{Q} > 1 \quad \Longrightarrow \quad P + \sqrt{D} > Q$

Riassumendo:

$$0 < \quad P \quad < \sqrt{D} \tag{13}$$
$$0 < \quad Q \quad < 2\sqrt{D} \tag{14}$$

Inoltre poiché $Q = \pm 2a$ e $P^2 - D = (-b)^2 - (b^2 - 4ac)$ si ha che:

$$Q \mid P^2 - D \tag{15}$$

E ricordando le proprieta' dei coniugati:

$$(a_1+a_2)' = a_1'+a_2' \; ; \; (a_1-a_2)' = a_1'-a_2' \; ; \; (a_1a_2)' = a_1'a_2' \; ; \; \left(\frac{a_1}{a_2}\right)' = \frac{a_1'}{a_2'} \quad (16)$$

Possiamo ora procedere con la dimostrazione. Sia $\gamma = a_0 + \frac{1}{\gamma_1}$ ove $a_0(\geq 1)$ é la parte intera di γ e $\frac{1}{\gamma_1}$ é la parte frazionaria di γ (con $\gamma_1 > 1$).
Anche γ_1 é un irrazionale quadratico ridotto applicando a γ le proprietá dei coniugati (16) si ottiene:

$$\begin{aligned} \left(\gamma \right. &= \left. a_0 + \frac{1}{\gamma_1}\right)' \\ \gamma' &= a_0 + \frac{1}{\gamma_1'} \end{aligned}$$

da cui

$$\gamma_1' = -\frac{1}{a_0 - \gamma'} \qquad \text{ove } -1 < \gamma' < 0$$

dunque $-1 < \gamma_1' < 0$, cioé γ_1 é ridotto.
Analogamente anche $\gamma_2, \gamma_3, \ldots, \gamma_n, \ldots$ sono irrazionali quadratici ridotti.
Si nota che:

$$\frac{1}{\gamma_1} = \gamma - a_0 = \frac{P+\sqrt{D}}{Q} - a_0 = \frac{P - Qa_0 + \sqrt{D}}{Q}$$

da cui

$$\gamma_1 = \frac{Q}{P - Qa_0 + \sqrt{D}}$$

Ora poniamo

$$P_1 = -P + Qa_0 \quad (17)$$

pertanto

$$\begin{aligned} \gamma_1 &= \frac{Q}{-P_1 + \sqrt{D}} \\ &= \frac{Q(\sqrt{D} + P_1)}{D - P_1^2} \end{aligned}$$

Ora poniamo

$$Q_1 = \frac{D - P_1^2}{Q} \quad (18)$$

da cui si ottiene

$$\gamma_1 = \frac{P_1 + \sqrt{D}}{Q_1} \tag{19}$$

Prestiamo ora attenzione al seguente ragionamento:

per la (17): $P_1 \equiv -P \ (mod\ Q)$ ma per la (15): $Q \mid P^2 - D \quad \Longrightarrow \quad Q \mid (-P_1)^2 - D$

$$\Longrightarrow \quad Q \mid D - P_1^2$$

P_1 é intero e anche Q_1 lo é poiché $Q \mid D - P_1^2$.

Riassumendo γ_1 é ridotto allora gli interi P_1 e Q_1 sono positivi e soddisfano le condizioni (13) e (14). Inoltre per la (18): $Q_1 \mid P_1^2 - D$.
Quindi possiamo ripetere il ragionamento fatto finora partendo con γ_1 al posto di γ e tutto funziona.
In generale ogni quoziente completo ha la forma:

$$\gamma_n = \frac{P_n + \sqrt{D}}{Q_n}$$

ove P_n e Q_n sono interi positivi che soddisfano le condizioni (13) e (14), e $Q_n \mid P_n^2 - D$.
Dopo al piú $2D$ passi si ottiene una ripetizione della coppia$(P_r, Q_r) = (P_{r+n+1}, Q_{r+n+1})$ e quindi la periodicitá $\gamma_r = \gamma_{r+n+1}$.

Rimane da dimostrare che il periodo é puro (cioé $r = 0$). Introduciamo, per ogni i, il numero:

$$\beta_i = -\frac{1}{\gamma_i'} \qquad (-1 < \gamma_i' < 0 \Longrightarrow -\frac{1}{\gamma_i'} = \beta_i > 1)$$

e coniugando γ_i si ottiene:

$$\left(\gamma_i \ = \ a_i + \frac{1}{\gamma_{i+1}}\right)'$$

$$\gamma_i' \ = \ a_i + \frac{1}{\gamma_{i+1}'} \tag{20}$$

che si riscrive:

$$-\frac{1}{\beta_i} \ = \ a_i - \beta_{i+1}$$

$$\beta_{i+1} \ = \ a_i + \frac{1}{\beta i} \tag{21}$$

Osservando le relazioni (20) e (21) notiamo che:

parte intera di γ_i' cioé $[\gamma_i'] = a_i = [\beta_{i+1}]$

essendo $\gamma_r = \gamma_{r+n+1} \implies \gamma_r' = \gamma_{r+n+1}' \implies \beta_r = \beta_{r+n+1}$

ma ($[\beta_r] = a_{r-1}$ e $[\beta_{r+n+1}] = a_{r-1+n+1}$) $\implies$ $a_{r-1} = a_{r+n}$.

Ora ($a_{r-1} = a_{r+n}$ e $\gamma_r = \gamma_{r+n+1}$) $\implies$ $\gamma_{r-1} = \gamma_{r-1+n+1}$

$\left(\text{ poiché } \quad \gamma_{r-1} = a_{r-1} + \dfrac{1}{\gamma_r} \text{ e } \gamma_{r-1+n+1} = a_{r-1+n+1} + \dfrac{1}{\gamma_{r+n+1}} \right)$

Iterando il procedimento si trova che: $\gamma_0 = \gamma_{n+1}$ come si voleva.

Quindi γ é puramente periodico.

□

Osservazione 2 *Le frazioni continue puramente periodiche rappresentano tutti e soli gli irrazionali quadratici ridotti.*

5.2 Teorema di Lagrange

In questa sezione enunceremo il teorema di Lagrange sulle frazioni continue e ne daremo una dimostrazione diversa da quelle usuali (che potete trovare nei testi [2] e [3] indicati in bibliografia).

Teorema 3 *Lo sviluppo in frazioni continue di un numero reale γ é periodico se e solo se γ é algebrico su $\mathbb{Q}$ di grado 2.*

Dimostrazione "$\Longrightarrow$" Mostriamo che se una frazione continua é periodica allora definisce un reale algebrico su $\mathbb{Q}$ di grado 2.
Se $\gamma = \{a_0; a_1, a_2, \ldots, \overline{a_r, \ldots, a_{r+n}}\}$ é periodico allora si ha che $\gamma_{r+n+1} = \gamma_r$ pertanto :

$$\gamma = \frac{\gamma_r p_{r-1} + p_{r-2}}{\gamma_r q_{r-1} + q_{r-2}} = \frac{\gamma_{r+n+1} p_{r+n} + p_{r+n-1}}{\gamma_{r+n+1} q_{r+n} + q_{r+n-1}}$$

da cui si ha che γ_r é zero di un polinomio di grado 2 su $\mathbb{Z}[x]$. Supponiamo che tale polinomio sia:

$$f(x) = ax^2 + bx + c \ .$$

Ora scrivendo γ_r in funzione di γ (cioé $\gamma_r(\gamma)$) e andandolo a sostiture in $f(x)$ si ottiene:

$$f(\gamma_r(\gamma)) = a(\gamma_r(\gamma))^2 + b(\gamma_r(\gamma)) + c = 0$$

da cui si ha che anche γ é zero di un polinomio di grado 2 su $\mathbb{Q}[x]$, pertanto é algebrico di grado 2 su $\mathbb{Q}$.

"$\Longleftarrow$" Mostriamo ora che ogni irrazionale quadratico ha uno sviluppo in frazioni continue che diventa periodico da un certo punto in poi.
Per mostrare ció sará sufficiente mostrare che, quando un qualsiasi irrazionale γ é sviluppato in frazioni continue, si raggiungerá prima o poi un quoziente completo γ_n che sia un irrazionale quadratico ridotto; infatti in tale caso la frazione continua si ripeterá da quel punto.
noi sappiamo che:

$$\gamma = \frac{\gamma_{n+1} p_n + p_{n-1}}{\gamma_{n+1} q_n + q_{n-1}} \qquad \text{con } p_n, p_{n-1}, q_n, q_{n-1} \in \mathbb{N}$$

essendo γ e γ_{n+1} irrazionali quadratici allora la stessa relazione sussiste tra:

$$\gamma' = \frac{\gamma'_{n+1} p_n + p_{n-1}}{\gamma'_{n+1} q_n + q_{n-1}} \qquad \text{con } p_n, p_{n-1}, q_n, q_{n-1} \in \mathbb{N}$$

quindi

$$\gamma'_{n+1} = -\frac{q_{n-1}\gamma' - p_{n-1}}{q_n\gamma' - p_n} = -\frac{q_{n-1}}{q_n}\left(\frac{\gamma' - \frac{p_{n-1}}{q_{n-1}}}{\gamma' - \frac{p_n}{q_n}}\right) \quad .$$

Per $n \to \infty$, $\frac{p_n}{q_n}$ e $\frac{p_{n-1}}{q_{n-1}}$ tendono a γ pertanto il valore tra parentesi tende a 1, cioé $\gamma'_{n+1} \to -\frac{q_{n-1}}{q_n}$.

Peró $q_{n-1}, q_n \in \mathbb{N}$ cioé sono positivi quindi γ'_{n+1} sará negativo.
Inoltre i numeri $\frac{p_n}{q_n}$ sono alternativamente piú grandi e piú piccoli di γ, e dunque la frazione fra parentesi é alternativamente appena minore o appena maggiore di 1. Scegliendo un valore di n per cui essa é piú piccola di 1, e osservando che $q_{n-1} < q_n$, si vede che $-1 < \gamma'_{n+1} < 0$.
Per un tale valore di n, il numero γ_{n+1} é un irrazionale quadratico ridotto. Conseguentemente la frazione continua sará puramente periodica da quel punto in poi. □

Non esistono molti irrazionali, oltre ai quadratici, di cui si conosca qualche aspetto di regolarita'.
Esempi:

$\frac{e-1}{e+1} = \{0; 2, 6, 10, 14, \dots\}$ ove i termini formano una progressione aritmetica;

e piú in generale se $k \in \mathbb{Z}^+$:

$\frac{e^{\frac{2}{k}} - 1}{e^{\frac{2}{k}} + 1} = \{0; k, 3k, 5k, 7k, \dots\}$ ove i termini formano una progressione aritmetica

ove lo sviluppo di e é il seguente:

$e = \{2; 1, 2, 1, 1, 4, 1, 1, 6, \dots\}$ ove i numeri 2, 4, 6, ... sono separati ogni volta da due 1;

Per il numero $\sqrt[3]{2}$, radice del polinomio $x^3 - 2$, non si sa se i termini della sua frazione continua, il cui inizio é:

$$\sqrt[3]{2} = \{1; 3, 1, 5, 1, 1, 4, 1, \dots\}$$

siano limitati o no, e non si conosce alcun modo per attaccare tale problema.

5.3 Radici quadrate dei razionali come frazioni continue

Consideriamo ora gli sviluppi in frazioni continue delle radici quadrate irrazionali, dei numeri razionali.
Esempi:

$$\sqrt{2} = \{1;\overline{2}\} \ ;$$

$$\sqrt{54} = \{7;\overline{2,1,6,1,2,14}\} \ ;$$

$$\sqrt{53} = \{7;\overline{3,1,1,3,14}\} \ .$$

Teorema 4 *Le radici quadrate irrazionali γ, dei numeri razionali maggiori di 1 (che non siano quadrati di razionali, cioé: $\gamma^2 \in \mathbb{Q}$, e $\gamma \in \mathbb{Q}$) sono tutte e sole le frazioni continue semplici del tipo:*

$$\gamma = \{a_0;\overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}\} \tag{22}$$

(ove gli $a_i \in \mathbb{N}$, il periodo comincia dopo il ; e consiste di una parte palindroma seguita da $2a_0$).
Inoltre γ é radice quadrata di:

$$\frac{[a_0, a_1, a_2, \ldots, a_1, a_0]}{[a_1, a_2, a_3, \ldots, a_2, a_1]}$$

Dimostrazione "$\Longleftarrow$" Vogliamo mostrare che se γ ha una frazione continua come quella indicata nella (22) allora é una radice quadrata irrazionale, e cioé $\gamma = -\gamma'$ (in quanto se γ é radice quadrata allora é soluzione dell'equazione $x^2 - \gamma^2 = 0$ cioé $x = \pm\gamma$ perció una radice é γ e l'altra é $\gamma' = -\gamma$).
Sappiamo che se γ ha uno sviluppo di quel tipo allora é un irrazionale quadratico maggiore di 1 (Lagrange).

Consideriamo ora il numero

$$\gamma + a_0 = \{\overline{2a_0; a_1, a_2, \ldots, a_2, a_1}\}$$

che é periodico puro.
Consideriamo poi il numero β, definito dalla frazione continua con il periodo rovesciato rispetto a $\gamma + a_0$ cioé:

$$\beta = \{\overline{a_1; a_2, \ldots, a_2, a_1, 2a_0}\}$$

Noi sappiamo che:

$$(\gamma + a_0)' = \gamma' + a_0 = -\frac{1}{\beta}$$

quindi

$$\beta = -\frac{1}{\gamma' + a_0} = \{\overline{a_1; a_2, \ldots, a_2, a_1, 2a_0}\} \quad .$$

Notiamo anche che essendo

$$\gamma + a_0 = \{\overline{2a_0; a_1, a_2, \ldots, a_2, a_1}\} = 2a_0 \; + \; \cfrac{1}{a_1 \; + \; \cfrac{1}{a_2 \; + \; \cfrac{1}{\ldots \; + \; \cfrac{1}{a_1 \; + \; \cfrac{1}{2a_0} \ldots}}}} \; ;$$

allora si ha che:

$$\gamma + a_0 - 2a_0 = \cfrac{1}{a_1 \; + \; \cfrac{1}{a_2 \; + \; \cfrac{1}{\ldots \; + \; \cfrac{1}{a_1 \; + \; \cfrac{1}{2a_0} \ldots}}}} \; ;$$

per cui

$$\frac{1}{\gamma + a_0 - 2a_0} = a_1 \; + \; \cfrac{1}{a_2 \; + \; \cfrac{1}{\ldots \; + \; \cfrac{1}{a_1 \; + \; \cfrac{1}{2a_0}}}} = \{\overline{a_1; a_2, \ldots, a_2, a_1, 2a_0}\}.$$

Confrontando $-\frac{1}{\gamma' + a_0}$ e $\frac{1}{\gamma + a_0 - 2a_0}$ notiamo che sono uguali, pertanto:

$$\beta = -\frac{1}{\gamma' + a_0} = \frac{1}{\gamma + a_0 - 2a_0} = \frac{1}{\gamma - a_0}$$

per cui

$$\gamma = -\gamma'$$

come si voleva dimostrare.

In particolare dall'equazione generale di γ:

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

e poiché

$$\gamma + a_0 = 2a_0 \; + \; \cfrac{1}{a_1 \; + \; \cfrac{1}{a_2 \; + \; \cfrac{1}{\ldots \; + \; \cfrac{1}{a_1 \; + \; \cfrac{1}{\gamma + a_0} \ldots}}}} \; ;$$

si ottiene che:

$$\begin{aligned}\gamma + a_0 &= \frac{(\gamma + a_0)p_n + p_{n-1}}{(\gamma + a_0)q_n + q_{n-1}} \\ \gamma + a_0 &= \frac{(\gamma + a_0)[2a_0, a_1, a_2, \ldots, a_2, a_1] + [2a_0, a_1, a_2, \ldots, a_2]}{(\gamma + a_0)[a_1, a_2, \ldots, a_2, a_1] + [a_1, a_2, \ldots, a_2]}\end{aligned}$$

da cui:

$$\begin{aligned}(\gamma + a_0)\{(\gamma + a_0)[a_1, a_2, \ldots, a_2, a_1] &+ [a_1, a_2, \ldots, a_2]\} = \\ &= (\gamma + a_0)[2a_0, a_1, a_2, \ldots, a_2, a_1] + [2a_0, a_1, a_2, \ldots, a_2]\end{aligned}$$

Sviluppando i calcoli:

$$\begin{aligned}(\gamma &+ a_0)^2[a_1, a_2, \ldots, a_2, a_1] + (\gamma + a_0)[a_1, a_2, \ldots, a_2] = \\ &= \gamma[2a_0, a_1, a_2, \ldots, a_2, a_1] + a_0[2a_0, a_1, a_2, \ldots, a_2, a_1] + [2a_0, a_1, a_2, \ldots, a_2]\end{aligned}$$

$$\begin{aligned}\gamma^2 &\quad [a_1, a_2, \ldots, a_2, a_1] + a_0^2[a_1, a_2, \ldots, a_2, a_1] + a_0[a_1, a_2, \ldots, a_2] = \\ a_0 &\quad [2a_0, a_1, a_2, \ldots, a_2, a_1] + [2a_0, a_1, a_2, \ldots, a_2]\end{aligned}$$

Isolando il termine con γ^2 al primo membro si ottiene:

$$\begin{aligned}\gamma^2 &\quad [a_1, a_2, \ldots, a_2, a_1] = \\ a_0 &\quad [2a_0, a_1, a_2, \ldots, a_2, a_1] + 2a_0[a_1, a_2, \ldots, a_2] + [a_2, \ldots, a_2] - a_0^2[a_1, \ldots, a_1] - a_0[a_1, \ldots, a_2] = \\ a_0 &\quad [2a_0, a_1, a_2, \ldots, a_2, a_1] + a_0[a_1, a_2, \ldots, a_2] + [a_2, \ldots, a_2] - a_0^2[a_1, \ldots, a_1] = \\ 2a_0^2 &\quad [a_1, a_2, \ldots, a_2, a_1] + a_0[a_1, a_2, \ldots, a_2] + a_0[a_1, a_2, \ldots, a_2] + [a_2, \ldots, a_2] - a_0^2[a_1, \ldots, a_1] = \\ a_0^2 &\quad [a_1, a_2, \ldots, a_2, a_1] + 2a_0[a_1, a_2, \ldots, a_2] + [a_2, \ldots, a_2] = \\ a_0 &\quad \big(a_0[a_1, a_2, \ldots, a_2, a_1] + 2[a_1, a_2, \ldots, a_2]\big) + [a_2, \ldots, a_2] = \\ a_0 &\quad \big(a_0[a_1, a_2, \ldots, a_2, a_1] + [a_1, a_2, \ldots, a_2] + [a_1, a_2, \ldots, a_2]\big) + [a_2, \ldots, a_2] = \\ a_0 &\quad \big([a_0, a_1, a_2, \ldots, a_2, a_1] + [a_1, a_2, \ldots, a_2]\big) + [a_2, \ldots, a_2] = \\ a_0 &\quad [a_0, a_1, a_2, \ldots, a_2, a_1] + a_0[a_1, a_2, \ldots, a_2] + [a_2, \ldots, a_2] = \\ a_0 &\quad [a_0, a_1, a_2, \ldots, a_2, a_1] + [a_0, a_1, a_2, \ldots, a_2] = \\ = &\quad [a_0, a_1, a_2, \ldots, a_2, a_1, a_0]\end{aligned}$$

Perció

$$\gamma^2 = \frac{[a_0, a_1, a_2, \ldots, a_2, a_1, a_0]}{[a_1, a_2, \ldots, a_2, a_1]}$$

"$\Longrightarrow$" Se

$$\gamma = \{a_0; \overline{a_1, a_2, \ldots, a_n}\}$$

é la radice irrazionale di un razionale maggiore di 1 allora:

$$a_0 \geq 1 \qquad \text{e} \qquad \gamma' = -\gamma \ .$$

Ora essendo $a_0 \geq 1 \Longrightarrow \gamma + a_0 > 1$. Il suo coniugato sará:

$$\big(\gamma + a_0\big)' = \gamma' + a_0 = -\gamma + a_0$$

e notiamo che tale coniugato é compreso tra -1 e 0, e cioé $\gamma + a_0 = \{\overline{2a_0; a_1, a_2, \ldots, a_n}\}$ é periodico puro.
Rovesciando il periodo si ha:

$$\{\overline{a_n; a_{n-1}, \ldots, a_2, a_1, 2a_0}\} = -\frac{1}{\gamma' + a_0} = \frac{1}{\gamma - a_0} = \frac{1}{(\gamma + a_0) - 2a_0} = \{\overline{a_1; a_2, \ldots, a_{n-1}, a_n, 2a_0}\}$$

per l'unicitá della rappresentazione (nell'ipotesi che l'ultimo termine della frazione continua non venga spezzato in $a_r = (a_r - 1) + \frac{1}{1}$) si ha che:

$a_n = a_1$; $\quad a_{n-1} = a_2$; $\quad \ldots \quad a_2 = a_{n-1}$; $\quad a_1 = a_n$; $\quad 2a_0 = 2a_0$

cioé il periodo é palindromo e

$$\gamma = \{a_0; \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}\}$$

come volevasi dimostrare. □

Corollario 1 *i) Le radici dei numeri naturali, che non siano quadrati perfetti, hanno uno sviluppo in frazioni continue del tipo:*

$$\sqrt{N} = \{a_0; \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}\}$$

ii) Se un numero ha uno sviluppo con questa forma:

$$\{a_0; \overline{a_1, a_2, a_3, \ldots, a_3, a_2, a_1, 2a_0}\}$$

esso é la radice di un numero naturale se e solo se

$$[a_1, a_2, \ldots, a_2, a_1] \mid [a_0, a_1, a_2, \ldots, a_2, a_1, a_0]$$

ossia

$$[a_1, a_2, \ldots, a_2, a_1] \mid 2a_0[a_1, a_2, \ldots, a_2] + [a_2, \ldots, a_2] \ .$$

La dimostrazione di questo corollario si ottiene direttamente dal teorema precedente (teorema 4).

6 Frazioni continue periodiche e somma di 2 quadrati

Consideriamo in questa sezione frazioni continue palindrome finite e non.

Lemma 2 *Una frazione continua semplice finita é palindroma di lunghezza pari, cioé del tipo:*

$$\gamma = \{a_0; a_1, a_2, \ldots, a_{m-1}, a_m, a_m, a_{m-1}, \ldots, a_2, a_1, a_0\} \tag{23}$$

se e solo se rappresenta un numero razionale $\frac{p}{q}$ *con* $p, q \in \mathbb{Z}$ *(e* $q \neq 0$*) tale che:*

i) $p > q$*;*

ii) $p \mid (q^2 + 1)$*.*

Dimostrazione Notiamo che il numero di termini della frazione continua é $2m + 2$, e se indichiamo la prima convergente a γ con $\frac{p_0}{q_0}$ allora l'ultima convergente che rappresenterá γ stesso sará $\frac{p_{2m+1}}{q_{2m+1}}$.

"$\Longrightarrow$" Sia γ della forma indicata in (23), allora

$$p_{2m} = [a_0, a_1, \ldots, a_m, a_m, \ldots, a_1] = [a_1, \ldots, a_m, a_m, \ldots, a_1, a_0] = q_{2m+1} \ .$$

Ponendo

$$p = p_{2m+1}; \qquad q = q_{2m+1} = p_{2m}; \qquad h = q_{2m};$$

risulterá che

$$\gamma = \frac{p_{2m+1}}{q_{2m+1}} = \frac{p}{q} = \frac{p_{2m+1}}{p_{2m}} \ .$$

Ora

$$q = p_{2m} < p_{2m+1} = p \qquad \text{cioé} \qquad p > q \qquad \text{(i)} \ .$$

Dall'equazione (6) del capitolo 3 si ha che:

$$p_{2m+1}q_{2m} - p_{2m}q_{2m+1} = (-1)^{2m} = 1$$

cioé

$$ph - qq = 1 \qquad \Longleftrightarrow \qquad ph = q^2 + 1 \qquad \Longleftrightarrow \qquad p \mid q^2 + 1 \qquad \text{(ii)}$$

"$\Longleftarrow$" Sia ora $\gamma = \frac{p}{q}$ con $p, q \in \mathbb{Z}$ e tali che

$$p > q \qquad \text{e} \qquad p \mid q^2 + 1 \quad \text{cioé} \quad ph = q^2 + 1 \quad (\exists h \in \mathbb{Z})$$

Svilippando γ come frazione continua di lunghezza pari (eventualmente scomponendo l'ultimo termine a_n in 2 termini: $a_n - 1$ e 1) si ottiene:

$$\gamma = \frac{p}{q} = \{a_0; a_1, a_2, \ldots, a_{m-1}, a_m, a_m^*, a_{m-1}^*, \ldots, a_2^*, a_1^*, a_0^*\}$$

Ora $p = p_{2m+1}$ e $q = q_{2m+1}$. Per ipotesi $ph = q^2 + 1$ il che equivale a:

$$p_{2m+1}h - q_{2m+1}^2 = 1$$

Dall'equazione (6) si ha ancora

$$p_{2m+1}q_{2m} - p_{2m}q_{2m+1} = 1$$

sottranendo queste ultime due relazioni si ottiene:

$$p_{2m+1}(h - q_{2m}) = q_{2m+1}(q_{2m+1} - p_{2m})$$

Essendo p_{2m+1} e q_{2m+1} coprimi si ottiene che

$$p_{2m+1} \mid (q_{2m+1} - p_{2m})$$

Inoltre

$$p_{2m+1} = p > q > q - p_{2m} = q_{2m+1} - p_{2m} \qquad \text{cioé} \qquad p > q_{2m+1} - p_{2m}$$

Ora noi siamo in questa situazione:

$$p_{2m+1} \mid (q_{2m+1} - p_{2m}) \qquad \text{e} \qquad p > q_{2m+1} - p_{2m}$$

allora dovrá per forza essere che $q = q_{2m+1} = p_{2m}$.
Questo si puó scrivere cosí:

$$[a_0, a_1, a_2, \ldots, a_{m-1}, a_m, a_m^*, a_{m-1}^*, \ldots, a_2^*, a_1^*, a_0^*] = [a_1, a_2, \ldots, a_{m-1}, a_m, a_m^*, a_{m-1}^*, \ldots, a_2^*, a_1^*, a_0^*]$$

allora

$$\{a_0; a_1, \ldots, a_m, a_m^*, \ldots, a_1^*, a_0^*\} = \frac{p_{2m+1}}{q_{2m+1}} = \frac{p_{2m+1}}{p_{2m}} =$$

$$= \frac{[a_0, a_1, \ldots, a_m, a_m^*, \ldots, a_1^*, a_0^*]}{[a_0, a_1, \ldots, a_m, a_m^*, \ldots, a_1^*]} = \frac{[a_0^*, a_1^*, \ldots, a_m^*, a_m, \ldots, a_1, a_0]}{[a_1^*, \ldots, a_m^*, a_m, \ldots, a_1, a_0]} =$$

$$= \{a_0^*; a_1^*, \ldots, a_m^*, a_m, \ldots, a_1, a_0\}$$

Per l'unicitá della rappresentazione risulta:

$$a_0 = a_0^*; \qquad a_1 = a_1^*; \qquad \dots \qquad a_{m-1} = a_{m-1}^*; \qquad a_m = a_m^*$$

come volevasi dimostrare. □

Se io sostituisco il quoziente completo

$$\gamma_{m+1} = \frac{[a_m, a_{m-1}, \dots, a_1, a_0]}{[a_{m-1}, \dots, a_1, a_0]}$$

nell'equazione generale

$$\gamma = \frac{p}{q} = \frac{\gamma_{m+1} p_m + p_{m-1}}{\gamma_{m+1} q_m + q_{m-1}}$$

dopo semplici calcoli si ottiene che

$$\gamma = \frac{p_m^2 + p_{m-1}^2}{p_m q_m + p_{m-1} q_{m-1}}$$

Notiamo che la frazione é ridotta, infatti scrivendo

$$(p_m^2 + p_{m-1}^2) q_m - (p_m q_m + p_{m-1} q_{m-1}) p_m = \pm p_{m-1}$$

si vede che un fattore primo di p_{m-1} dividerebbe anche p_m, il che é assurdo. Allora $p = p_m^2 + p_{m-1}^2$.

Abbiamo cosí ottenuto il Corollario di Serret:

Corollario 2 *(COROLLARIO DI SERRET)*
Sia p divisore di q^2+1 con $p > q$, allora p é somma di 2 quadrati ($p = x^2+y^2$ con $(x, y) = 1$) e anzi x, y si calcolano sviluppando $\frac{p}{q}$ come frazione continua di lunghezza pari. Cioé

$$\frac{p}{q} = \{a_0; a_1, a_2, \dots, a_{m-1}, a_m, a_m, a_{m-1}, \dots, a_2, a_1, a_0\}$$

dove

$$p = x^2 + y^2 \qquad \textit{ponendo} \qquad x = p_{m-1} \quad y = p_m \ .$$

Esempio 1:

$p = 41 \; ; \quad q = 9 \; ; \quad p > q \; ;$

$q^2 + 1 = 9^2 + 1 = 41 \cdot 2 = p \cdot h \; ;$

$\frac{p}{q} = \frac{41}{9} = \{4; 1, 1, 4\}$ i cui convergenti sono: $\quad \frac{4}{1} \; ; \frac{5}{1} \; ; \frac{9}{2} \; ; \frac{41}{9} \; ;$

in tale caso $m = 1$ perció le soluzioni sono: $x = p_{m-1} = p_0 = 4 \quad y = p_m = p_1 = 5$

infatti: $p = 41 = x^2 + y^2 = 4^2 + 5^2$.

Esempio 2:

$p = 65 \; ; \quad q = 18 \; ; \quad p > q \; ;$

$q^2 + 1 = 18^2 + 1 = 65 \cdot 5 = p \cdot h \; ;$

$\frac{p}{q} = \frac{65}{18} = \{3; 1, 1, 1, 1, 3\}$ i cui convergenti sono: $\quad \frac{3}{1} \; ; \frac{4}{1} \; ; \frac{7}{2} \; ; \frac{11}{3} \; ; \frac{18}{5} \; ; \frac{65}{18} \; ;$

in tale caso $m = 2$ perció le soluzioni sono: $x = p_{m-1} = p_1 = 4 \quad y = p_m = p_2 = 7$

infatti: $p = 65 = x^2 + y^2 = 4^2 + 7^2$.

Viceversa scegliendo comunque i numeri $a_0, a_1, \ldots, a_{m-1}, a_m$, e calcolando I convergenti:

$$\frac{p_0}{q_0} \; ; \frac{p_0}{q_0} \; ; \ldots \frac{x}{q_{m-1}} \; ; \frac{y}{q_m} \; ; \ldots \frac{q}{h} \; ; \frac{p}{q} \; ;$$

si ottengono le relazioni: $p \cdot h = q^2 + 1 \; ; \qquad p = x^2 + y^2.$

Esempio 3:

Sia $\gamma = \{1; 2, 3, 4, 5, 5, 4, 3, 2, 1\}$.

Le sue convergenti sono:

$$\frac{1}{1} ; \frac{3}{2} ; \frac{10}{7} ; \frac{43}{30} ; \frac{225}{157} ; \frac{1168}{815} ; \frac{4897}{3417} ; \frac{15859}{11066} ; \frac{36615}{25549} ; \frac{52474}{36615} ;$$

essendo $m = 5$ allora considero $x = p_{m-1} = p_4 = 43$ e $y = p_m = p_5 = 225$, mentre $p = 52474$ e $q = 36615$.

Allora $p > q$ inoltre

$$q^2 + 1 = 36615^2 + 1 = 52474 \cdot 25549 = p \cdot h$$

e concludendo:

$$p = 52474 = 43^2 + 225^2 = x^2 + y^2$$

Esempio 4:

Sia $\gamma = \{1; 2, 1, 1, 8, 2, 1, \ 1, 2, 8, 1, 1, 2, 1\}$.

Le sue convergenti sono:

$$\frac{1}{\dots} ; \frac{3}{\dots} ; \frac{4}{\dots} ; \frac{7}{\dots} ; \frac{60}{\dots} ; \frac{127}{\dots} ; \frac{187}{\dots} ; \dots ; \frac{51098}{36615}$$

essendo $m = 6$ allora considero $x = p_{m-1} = p_5 = 127$ e $y = p_m = p_6 = 187$, mentre $p = 51098$ e $q = 36615$.

Allora $p > q$ inoltre

$$q^2 + 1 = 36615^2 + 1 = 51098 \cdot 26237 = p \cdot h$$

e concludendo:

$$p = 51098 = 127^2 + 187^2 = x^2 + y^2$$

Consideriamo infine frazioni continue semplici, periodiche e palindrome.

Teorema 5 *Si consideri la frazione continua semplice periodica*

$$\gamma = \{a_0; \overline{a_1, a_2, \ldots, a_{m-1}, a_m, a_m, a_{m-1}, \ldots, a_2, a_1, 2a_0}\}$$

dove la parentesi contiene $1 + n$ *termini.*
Sia poi $\frac{p_n}{q_n}$ *la convergente n-esima di*

$$\delta = \{a_0; a_1, a_2, \ldots, a_{m-1}, a_m, a_m, a_{m-1}, \ldots, a_2, a_1, a_0\}$$

allora:

i)

$$p_{n-1} = q_n \ ;$$

ii)

$$\gamma = \sqrt{\frac{p_n}{q_{n-1}}} = \sqrt{\frac{[a_0, a_1, \ldots, a_m, a_m, a_1, a_0]}{[a_1, \ldots, a_m, a_m, a_1]}} \ .$$

Dimostrazione Tutto ció é giá stato dimostrato precedentemente, ossia i) al Lemma 2 del capitolo 6 mentre ii) al teorema 4 del capitolo 5.

7 Interpretazione geometrica delle frazioni continue

Una sorprendente interpretazione geometrica della frazione continua di un numero irrazionale fu proposta da Klein nel 1895. Supponiamo che γ sia un irrazionale positivo. Consideriamo tutti i punti del piano le cui coordinate sono interi positivi, e immaginiamo di piantare nel piano dei pioli in corrispondenza di tutti questi punti. La retta $y = \gamma x$ non passa per nessuno di essi. Immaginiamo un filo teso lungo tale retta e avente un'estremitá fissata a un punto della retta infinitamente distante. Se l'altro capo del filo, nell'origine, viene spostato dalla retta, il filo si appoggerá a certi pioli; se verrá trascinato via dall'altra parte della retta, il filo si appoggerá a certi altri pioli. I pioli in uno di questi insiemi (quelli sotto alla retta) saranno associati ai punti con coordinate $(q_0, p_0); (q_2, p_2); (q_4, p_4); \dots$ corrispondenti ai punti con coordinate minori di γ. I pioli nell'altro insieme (quelli sopra alla retta) saranno associati ai punti di coordinate $(q_1, p_1); (q_3, p_3); (q_5, p_5); \dots$ corrispondenti ai convergenti maggiori di γ. Il filo in ciascuna delle due posizioni formerá una poligonale che si avvicinerá alla retta $y = \gamma x$.

La figura 1, che si trova nel file allegato "*figura 1.doc*[1]", illustra il caso

$$\gamma = \frac{1+\sqrt{5}}{2} = \{1; 1, 1, 1, 1, \dots\}$$

ovvero la sezione aurea.
Ora i convergenti sono:

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \dots$$

I pioli sotto la retta staranno sui punti:

$$(1,1);\ (2,3);\ (5,8);\ \dots$$

e quelli sopra la retta sui punti

$$(1,2);\ (3,5);\ (8,13);\ \dots$$

La maggior parte dei teoremi elementari sulle frazioni continue ammette semplici interpretazioni geometriche. Se P_n denota il punto (q_n, p_n), allora le relazioni di ricorrenza (3) e (4) affermano che il vettore $\overrightarrow{P_{n-2}P_n}$ é un multiplo del vettore $\overrightarrow{OP_{n-1}}$. La relazione (6) puó essere interpretata dicendo che l'area del triangolo O, P_{n-1}, P_n é sempre $\frac{1}{2}$. Infatti non ci sono punti con coordinate intere all'interno del triangolo, oltre ai vertici, pertanto un triangolo con tale proprietá ha area $\frac{1}{2}$.

[1] tutte le figure indicate nell'elaborato si possono consultare nei file allegati di tipo *doc*

8 Equazione di Pell

Si chiama equazione di Pell l'equazione diofantea:

$$x^2 - Ny^2 = 1 \qquad \text{o} \qquad x^2 = Ny^2 + 1 \tag{24}$$

ove N é un naturale che non sia un quadrato perfetto[2].

É notevole che l'equazione di Pell ammetta sempre soluzione in numeri naturali, e che tali soluzioni siano infinite. Riferimenti a singoli casi dell'equazione di Pell si trovano sparsi attraverso tutta la storia della Matematica. La piú curiosa di queste apparizioni avviene nel cosidetto "*problema del bestiame*" di Archimede.
Tale problema contiene 8 incognite (numeri di capi di bestiame di vario tipo) che soddisfano 7 equazioni lineari, assieme a 2 condizioni che asseriscono che certi numeri son quadrati perfetti.
Dopo un pó di algebra elementare, il problema si riduce a risolvere l'equazione:

$$x^2 - 4729494y^2 = 1$$

la cui soluzione minima x é un numero di 41 cifre (soluzione esibita da Amthor nel 1880).
Non vi é evidenza che gli antichi sapessero risolvere il problema, ma il solo fatto che l'avessero proposto suggerisce che essi potessero ben aver qualche nozione sll'equazione di Pell che sia poi andata smarrita.

Nei tempi moderni, il primo metodo sistematico per risolvere l'equazione fu esibito da Lord Brouncker nel 1657. Si tratta essenzialmente di sviluppare $\sqrt{N}$ come frazione continua, come verra' spiegato in seguito. Quasi contemporaneamente, Frenicle de Bessy tabuló soluzioni della (24) per tutti i valori di N fino a 150, e sfidó Brouncker a risolvere l'equazione $x^2 - 313y^2 = 1$. Brouncker, in risposta, produsse una soluzione (in cui x ha sessanta cifre), che disse di aver trovato col proprio metodo in una o due ore. Sia Wallis che Fermat, affermarono di aver dimostrato che l'equazione é sempre risolubile. Fermat sembra essere stato il primo ad enunciare categoricamente che le soluzioni sono infinite. La prima dimostrazione pubblicata si deve a Lagrange, ed apparí intorno al 1766. Il nome di Pell fu associato all'equazione da Eulero per errore; egli pensó che il metodo di soluzione esibito da Wallis fosse dovuto o John Pell, un matematico inglese dello stesso periodo.

[2]La differenza di 2 quadrati non puó mai essere uguale a 1, tranne nel caso $1^2 - 0^2$.

8.1 Soluzioni dell'equazione di Pell

Vediamo ora come trovare le soluzioni dell'equazione (24).

Proposizione 3 *Se* (x_1, y_1) *é una soluzione di*

$$x^2 - Ny^2 = \pm 1 \tag{25}$$

allora $\frac{x_1}{y_1}$ *é una convergente dello sviluppo in frazioni continue di* $\sqrt{N}$ *cioé* $\frac{x_1}{y_1} = \frac{p_i}{q_i}$ *per qualche* i.

Dimostrazione Per ipotesi si ha che:

$$x_1^2 - Ny_1^2 = \pm 1$$

cioé

$$(x_1 + y_1\sqrt{N})(x_1 - y_1\sqrt{N}) = \pm 1$$

moltiplico entrambi i membri per $\frac{1}{x_1+y_1\sqrt{N}}$ ed ottengo:

$$\begin{aligned}(x_1 - y_1\sqrt{N}) &= \pm\frac{1}{(x_1 + y_1\sqrt{N})} \\ y_1\left(\frac{x_1}{y_1} - \sqrt{N}\right) &= \pm\frac{1}{y_1\left(\frac{x_1}{y_1} + \sqrt{N}\right)}\end{aligned}$$

divido ancora entrambi i membri per y_1 ed ottengo:

$$\left| \frac{x_1}{y_1} - \sqrt{N} \right| = \frac{1}{y_1^2\left(\frac{x_1}{y_1} + \sqrt{N}\right)} < \frac{1}{2\sqrt{N}y_1^2} < \frac{1}{2y_1^2} \quad ;$$

perció

$$\left| \frac{x_1}{y_1} - \sqrt{N} \right| < \frac{1}{2y_1^2}$$

che consente di applicare un noto teorema di approssimazione diofantea secondo il quale h, k in se un numero razionale $\frac{p}{q}$ soddisfa tale disuguaglianza, allora esso é un convergente a $\sqrt{N}$. □

Ma quali i portano a soluzioni?

Considero la frazione continua per

$$\sqrt{N} = \{a_0; \overline{a_1, a_2, \ldots, 2a_0}\} = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n+}\frac{1}{2a_0+}\frac{1}{a_1+}\cdots$$

Sia ora

$$\begin{aligned}\frac{p_{n-1}}{q_{n-1}} &= a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\dots\frac{1}{a_{n-1}} \\ \frac{p_n}{q_n} &= a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\dots\frac{1}{a_{n-1}+}\frac{1}{a_n}\end{aligned}$$

e il quoziente completo

$$\gamma_{n+1} = 2a_0 + \frac{1}{a_2+}\dots\frac{1}{a_{n-1}+}\frac{1}{a_n+}\frac{1}{2a_0+}\frac{1}{a_1+}\dots = \sqrt{N} + a_0$$

Dall' equazione generale si ha:

$$\sqrt{N} = \frac{\gamma_{n+1}p_n + p_{n-1}}{\gamma_{n+1}q_n + q_{n-1}} = \frac{(\sqrt{N}+a_0)p_n + p_{n-1}}{(\sqrt{N}+a_0)q_n + q_{n-1}}$$

da cui:

$$\begin{aligned}\sqrt{N}\big((\sqrt{N}+a_0)q_n + q_{n-1}\big) &= (\sqrt{N}+a_0)p_n + p_{n-1} \\ Nq_n + (a_0q_n + q_{n-1})\sqrt{N} &= (a_0p_n + p_{n-1}) + p_n\sqrt{N}\end{aligned}$$

Quest'ultima é una equazione del tipo $a + b\sqrt{N} = c + d\sqrt{N}$ ove $a, b, c, d \in \mathbb{Z}$ e $\sqrt{N}$ é irrazionale. Perció si avrá che $a = c$ e $b = d$, cioé:

$$\begin{cases} Nq_n = a_0p_n + p_{n-1} \\ a_0q_n + q_{n-1} = p_n \end{cases}$$

Risolvendo per p_{n-1} e q_{n-1} si ha:

$$\begin{cases} p_{n-1} = Nq_n - a_0p_n \\ q_{n-1} = p_n - a_0q_n \end{cases}$$

Noi sappiamo dalla (6) che:

$$p_mq_{m-1} - p_{m-1}q_m = (-1)^{m-1}$$

quindi sostituendo:

$$p_n(p_n - a_0q_n) - (Nq_n - a_0p_n)q_n = (-1)^{n-1}$$

da cui si ottiene l'equazione:

$$p_n^2 - Nq_n^2 = (-1)^{n-1} \tag{26}$$

A questo punto si verificano 2 casi:

1. Se $n-1$ é pari, cioé n é dispari $\quad\Longrightarrow\quad p_n^2 - Nq_n^2 = 1$
2. Se $n-1$ é dispari, cioé n é pari $\quad\Longrightarrow\quad p_n^2 - Nq_n^2 = -1$

Nel primo caso (n dispari) abbiamo una soluzione dell'equazione di Pell (24) e cioé:

$$x = p_n \qquad y = q_n$$

ove $\frac{p_n}{q_n}$ sono i convergenti nello sviluppo in frazioni continue di $\sqrt{N}$ arrestati prima del termine $2a_0$.

Nel secondo caso (n pari) abbiamo una soluzione dell'equazione

$$x^2 - Ny^2 = -1 \tag{27}$$

Poiché

$$\begin{aligned}\sqrt{N} &= a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n+}\frac{1}{2a_0+}\frac{1}{a_1+} \quad \cdots\cdots \quad \frac{1}{a_n+}\frac{1}{2a_0+}\frac{1}{a_1+}\cdots \\ &= a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n+}\frac{1}{a_{n+1}+}\frac{1}{a_{n+2}+}\cdots\frac{1}{a_{2n+1}+}\frac{1}{a_{2n+2}+}\frac{1}{a_{2n+3}+}\cdots\%\end{aligned}$$

applicando tutto il ragionamento fatto finora, ai 2 convergenti, alla fine del periodo successivo, vediamo che il termine a_n appare per la seconda volta come a_{2n+1}, perció sostituiró n con $2n+1$ nell'equazione (26):

$$p_{2n+1}^2 - Nq_{2n+1}^2 = (-1)^{2n} = 1$$

ottenendo cosí una soluzione dell'equazione di Pell (24) e cioé:

$$x = p_{2n+1} \qquad y = q_{2n+1}$$

ove p_{2n+1} e q_{2n+1} sono i quozienti completi nello sviluppo in frazioni continue di $\sqrt{N}$ arrestati prima del termine $2a_0$ che incontro per la seconda volta.

Esempio 1:

Cerchiamo le soluzioni di $x^2 - 21y^2 = 1$.

$$\sqrt{21} = \{4; \overline{1, 1, 2, 1, 1, 8}\} = \{a_0; \overline{a_1, a_2, a_3, a_4, a_5, 2a_0}\}$$

cioé $n = 5$ quindi:

$$p_5^2 - 21q_5^2 = (-1)^{5-1} = 1$$

I convergenti sono:

$$\frac{4}{1}\ ;\frac{5}{1}\ ;\frac{9}{2}\ ;\frac{23}{5}\ ;\frac{32}{7}\ ;\frac{55}{12}\ ;\dots$$

perció $x = p_5 = 55$ e $y = q_5 = 12$ sono le soluzioni dell'equazione. Infatti:

$$55^2 - 21 \cdot 12^2 = 3025 - 3024 = 1$$

Esempio 2:

Cerchiamo le soluzioni di $x^2 - 29y^2 = 1$.

$$\sqrt{29} = \{5; \overline{2, 1, 1, 2, 10}\} = \{a_0; \overline{a_1, a_2, a_3, a_4, 2a_0}\}$$

cioé $n = 4$ quindi:

$$p_4^2 - 21q_4^2 = (-1)^{4-1} = -1$$

I convergenti sono:

$$\frac{5}{1}\ ;\frac{11}{2}\ ;\frac{16}{3}\ ;\frac{27}{5}\ ;\frac{70}{13}\ ;\dots$$

perció $x = p_4 = 70$ e $y = q_4 = 13$ sono le soluzioni dell'equazione $x^2 - 29y^2 = -1$.

Consideriamo pertanto i convergenti successivi fino ad arrivare a $2n + 1 = 9$, cioé cerchiamo $\frac{p_9}{q_9}$:

$$\frac{727}{135}\ ;\frac{1524}{283}\ ;\frac{2251}{418}\ ;\frac{3775}{701}\ ;\frac{9801}{1820} = \frac{p_9}{q_9}\ ;\dots$$

ora $x = p_9 = 9801$ e $y = q_9 = 1820$ sono le soluzioni dell'equazione. Infatti:

$$9801^2 - 29 \cdot 1820^2 = 96059601 - 96059600 = 1$$

Le piú piccole soluzioni di $x^2 - Ny^2 = \pm 1$ sono elencate nella figura 2, fino ad $N = 50$.

In definitiva per mostrare che l'equazione di Pell ha infinite soluzioni e che queste sono ottenute a partire da convergenti che corrispondono ai termini a_n alla fine di ogni periodo, si procede nel seguente modo:

1. se n é dispari (cioé la frazione continua ha un termine centrale) tutte queste sono soluzioni dell'equazione di Pell (24);

2. se n é pari (cioé la frazione continua non ha un termine centrale) i convergenti forniscono alternativamente soluzioni dell'equazione con -1 (27) e dell'equazione con 1 (24).

Pertanto le soluzioni sono infinite.
Nel caso in cui il periodo di $\{a_0; \overline{a_1, \ldots, a_2, a_1, 2a_0}\}$ ha lunghezza $n+1$ pari, n é dispari (cioé il palindromo $a_1, a_2, \ldots, a_2, a_1$ ha un elemento centrale) allora la (27) non ha soluzioni, mentre la (24) é risolta dalle coppie

$$(p_n, q_n); \qquad (p_{2n}, q_{2n}); \qquad (p_{3n}, q_{3n}); \qquad \ldots$$

Nel caso in cui il periodo di $\{a_0; \overline{a_1, \ldots, a_2, a_1, 2a_0}\}$ ha lunghezza $n+1$ dispari, n é pari (cioé il palindromo $a_1, a_2, \ldots, a_2, a_1$ non ha un elemento centrale) allora la (27) é risolta dalle coppie

$$(p_n, q_n); \qquad (p_{2n}, q_{2n}); \qquad (p_{3n}, q_{3n}); \qquad \ldots$$

mentre la (24) é risolta dalle coppie

$$(p_{2n+1}, q_{2n+1}); \qquad (p_{4n+3}, q_{4n+3}); \qquad (p_{6n+5}, q_{6n+5}); \qquad \ldots$$

Concludendo l'equazione di Pell (24) puó sempre essere risolta, mentre l'equazione (27) non é sempre risolubile.

La distinzione dei casi in cui n é dispari o pari solleva problemi ai quali non si é finora data risposta completa. Infatti non é ancora noto il modo di caratterizzare i numeri N per cui n é pari.

Seguiamo il seguente ragionamento. Se l'equazione (27)

$$x^2 - Ny^2 = -1$$

é risolubile, allora é risolubile la congruenza

$$x^2 + 1 \equiv 0 \ (mod\ N) \qquad \Longleftrightarrow \qquad x^2 \equiv -1 \ (mod\ N)$$

Questo significa che -1 é un quadrato in $\mathbb{Z}/N\mathbb{Z}$.

Se p é un numero primo diverso da 2, andiamo allora a considerare il simbolo di Legendre:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se -1 é un quadrato in } \mathbb{Z}/p\mathbb{Z} \text{ (cioé } p \equiv 1 \ (mod\ 4) \text{)} \\ -1 & \text{se -1 non é un quadrato in } \mathbb{Z}/p\mathbb{Z} \text{ (cioé } p \equiv 3 \ (mod\ 4) \text{)} \end{cases}$$

Nel nostro caso, se $p|N$ da $x^2 \equiv -1 \ (mod\ N)$ segue

$$x^2 \equiv -1 \ (mod\ p) \qquad \Longleftrightarrow \qquad \left(\frac{-1}{p}\right) = 1 \qquad \Longleftrightarrow \qquad p \equiv 1 \ (mod\ 4)$$

Cosí N non é divisibile per 4 (se lo fosse non sarebbe piú valida la congruenza indicata sopra) e non puó essere diviso per alcun primo della forma $4k + 3$. Peró questa é una condizione necessaria per la risolubilitá della (27) ma non sufficiente.
Per esempio

$$N = 34 = 17 \cdot 2$$

ma si puó verificare che l'equazione $x^2 - 34y^2 = -1$ non é risolubile.

Si puó dimostrare invece che se $D = p$ ove pé un primo e $p \equiv 1(\mod 4)$ allora l'equazione $x^2 - py^2 = -1$ ammette soluzioni. Infatti sia (x_1, y_1) la piú piccola soluzione dell'equazione:

$$x^2 - py^2 = 1$$

(allora $y_1 \equiv 0 (\mod 2)$ e $x_1 \equiv 1 (\mod 2)$).
Poiché (x_1, y_1) é soluzione allora:

$$x_1^2 - py_1^2 = 1$$

da cui:

$$x_1^2 - 1 = py_1^2$$

dividiamo entrambi i membri per 4 ed otteniamo:

$$\frac{x_1 + 1}{2} \cdot \frac{x_1 - 1}{2} = p\left(\frac{y_1}{2}\right)^2$$

Ora si possono verificare 2 casi:

1. $$\frac{x_1+1}{2} = pa^2 \ ; \qquad \frac{x_1-1}{2} = b^2 \ ;$$

2. $$\frac{x_1+1}{2} = a^2 \ ; \qquad \frac{x_1-1}{2} = pb^2 \ ;$$

ove $a, b \in \mathbb{Z}$.
Nel secondo caso si ottiene $a^2 - pb^2 = 1$, contro il fatto che (x_1, y_1) é la piú piccola soluzione dell'equazione $x^2 - py^2 = 1$.
Nel primo caso si ottiene $b^2 - pa^2 = -1$. Allora tutte le altre infinite soluzioni dell'equazione $x^2 - py^2 = -1$ si ottengono cosí:

$$X + Y\sqrt{p} = (b + a\sqrt{p})^{2n+1}$$

ove n é un intero arbitrario.
Mentre la soluzione fondamentale e data da:

$$x_1 + y_1\sqrt{p} = (b + a\sqrt{p})^2$$

8.2 Genesi moltiplicativa delle soluzioni dell'equazione di Pell

Continuiamo a vedere come ottenere soluzioni dell'equazione

$$x^2 - Ny^2 = \pm 1$$

Teorema 6 *Se (x_1, y_1) é la piú piccola soluzione positiva dell'equazione (24), $x^2 - Ny^2 = 1$, (cioé la soluzione per cui é minimo il numero $x_1 + y_1\sqrt{N}$) allora tutte le altre soluzioni positive (x_n, y_n) possono essere ottenute dall'equazione:*

$$x_n + y_n\sqrt{N} = (x_1 + y_1\sqrt{N})^n \qquad ove\ n = 1, 2, 3, \ldots \tag{28}$$

Dimostrazione Dimostriamo che le (x_n, y_n) sono soluzioni. Per esempio se (x_1, y_1) é la piú piccola soluzione positiva della (26) la successiva soluzione (x_2, y_2) é data da

$$x_2 + y_2\sqrt{N} = (x_1 + y_1\sqrt{N})^2 = x_1^2 + Ny_1^2 + 2x_1y_1\sqrt{N}$$

cioé

$$x_2 = x_1^2 + Ny_1^2\ ; \qquad y_2 = 2x_1y_1\ .$$

Mostriamo che effettivamente (x_2, y_2) é soluzione:

$$\begin{aligned} x_2^2 - Ny_2^2 &= (x_1^2 + Ny_1^2)^2 - N(2x_1y_1)^2 \\ &= x_1^4 - 2Nx_1^2y_1^2 + N^2y_1^4 \\ &= (x_1^2 - Ny_1^2)^2 = (1)^2 = 1 \end{aligned}$$

É semplice mostrare che se (x_n, y_n) sono calcolate tramite l'equazione (28) allora $x_n^2 - Ny_n^2 = 1$. Dalla (28) si ha che

$$x_n + y_n\sqrt{N} = \underbrace{(x_1 + y_1\sqrt{N})(x_1 + y_1\sqrt{N})\ldots(x_1 + y_1\sqrt{N})}_{n}$$

Coniugando si ottiene:

$$x_n - y_n\sqrt{N} = \underbrace{(x_1 - y_1\sqrt{N})(x_1 - y_1\sqrt{N})\ldots(x_1 - y_1\sqrt{N})}_{n}$$

e cioé

$$x_n - y_n\sqrt{N} = (x_1 - y_1\sqrt{N})^n\ .$$

Concludendo:

$$\begin{aligned} x_n^2 - Ny_n^2 &= (x_n + y_n\sqrt{N})(x_n - y_n\sqrt{N}) \\ &= (x_1 + y_1\sqrt{N})^n (x_1 - y_1\sqrt{N})^n \\ &= (x_1^2 - Ny_1^2)^n = (1)^n = 1 \end{aligned}$$

Pertanto x_n e y_n sono soluzioni dell'equazione (26).

Proviamo ora, che le soluzioni sono tutte di questo tipo.
Supponiamo per assurdo che (a, b) sia una soluzione positiva dell'equazione $x^2 - Ny^2 = 1$ non ottenuta dall'equazione (28).
Allora per certi interi positivi n si ha che:

$$\left(x_1 + y_1\sqrt{N}\right)^n < a + b\sqrt{N} < \left(x_1 + y_1\sqrt{N}\right)^{n+1}$$

Allora dividendo per $x_1 + y_1\sqrt{N}$:

$$1 < \left(a + b\sqrt{N}\right)\left(x_1 - y_1\sqrt{N}\right) < x_1 + y_1\sqrt{N}$$

Poniamo $\left(a + b\sqrt{N}\right)\left(x_1 - y_1\sqrt{N}\right) = X + Y\sqrt{N}$.

Si nota che $X + Y\sqrt{N} < x_1 + y_1\sqrt{N}$ e che $X^2 - NY^2 = 1$.

Ora dal fatto che $X + Y\sqrt{N} > 1$ e $0 < X - Y\sqrt{N} < 1$ si ottiene che $X > 0$; $Y > 0$. Questo peró va contro il fatto che (x_1, y_1) sia la piú piccola soluzione positiva di $x^2 - Ny^2 = 1$.

Pertanto tutte le soluzione sono date dell'equazione (28). □

Teorema 7 *Assumendo che l'equazione (27), $x^2 - Ny^2 = -1$, sia risolubile, e sia (x_1, y_1) é la piú piccola soluzione positiva (cioé la soluzione per cui é minimo il numero $x_1 + y_1\sqrt{N}$) allora tutte le altre soluzioni positive (x_n, y_n) possono essere ottenute dall'equazione:*

$$x_n + y_n\sqrt{N} = (x_1 + y_1\sqrt{N})^n \qquad \textit{ove } n = 1, 3, 5, 7, \ldots \tag{29}$$

D'altra parte usando lo stesso valore (x_1, y_1) si possono ottenere le soluzioni positive di $x^2 - Ny^2 = 1$ che sono data dall'equazione:

$$x_n + y_n\sqrt{N} = (x_1 + y_1\sqrt{N})^n \qquad \textit{ove } n = 2, 4, 6, 8, \ldots \tag{30}$$

La dimostrazione di questo fatto sará conseguenza della struttura (essenzialmente) ciclica del gruppo delle unitá dell'anello degli interi algebrici di $\mathbb{Q}(\sqrt{N})$, ció che é argomento del prossimo paragrafo.

9 Unitá dei campi quadratici ed equazione di Pell

Con riferimento all'equazione di Pell (25) (chiamiamo anch'essa equazione di Pell anche se non sarebbe corretto) nel campo reale ($\mathbb{R}$) consideriamo il sottoanello $\mathbb{Z}[\sqrt{N}] = \{a + b\sqrt{N} \mid a, b \in \mathbb{Z}\}$ e studiamo il gruppo U dei suoi elementi invertibili, utilizzando la moltiplicativitá della norma.
Ora

$$N(a + b\sqrt{N}) = (a + b\sqrt{N})(a - b\sqrt{N}) = a^2 - Nb^2 \ .$$

Per definizione $a + b\sqrt{N} \in U(\mathbb{Z}[\sqrt{N}])$ se e solo se esiste $c + d\sqrt{N} \in \mathbb{Z}[\sqrt{N}]$ tale che:

$$(a + b\sqrt{N})(c + d\sqrt{N}) = 1$$

e usando la norma

$$\begin{aligned} N\big((a + b\sqrt{N})(c + d\sqrt{N})\big) &= N(1) \\ N(a + b\sqrt{N}) \ \ N(c + d\sqrt{N}) &= 1 \\ (a^2 - Nb^2)(c^2 - Nd^2) &= 1 \end{aligned}$$

Ora a, b, c, d sono interi, N é naturale (non quadrato), allora $a^2 - Nb^2$ e $c^2 - Nd^2$ sono interi perció quest'ultima equazione é vera se e solo se i 2 fattori sono entrambi 1 o -1.

Riassumendo $a + b\sqrt{N}$ é invertibile se e solo se la sua norma vale ± 1 (gli inversi sono del tipo $\pm a \pm b\sqrt{N}$). Infatti basta usare il seguente teorema:

Teorema 8 *α é un unitá di $R(\theta)$ (ove R é un campo) se e solo se* $N(\alpha) = \pm 1$.

Dimostrazione "$\Longrightarrow$" α é un unitá se e solo se $\alpha \mid 1$.
Se $\alpha \mid 1 \Longrightarrow N(\alpha) \mid N(1) \Longrightarrow N(\alpha) \mid 1 \Longrightarrow N(\alpha) = \pm 1$.

"$\Longleftarrow$" Se $N(\alpha) = \pm 1 \Longrightarrow \alpha_1\alpha_2 \ldots \alpha_n = \pm 1$ ove gli α_i sono i coniugati di α. Allora $\alpha_1 \mid 1;\ \alpha_2 \mid 1; \ldots \alpha_n \mid 1; \Longrightarrow \alpha \mid 1$. Pertanto α é unitá. □

Ma dire che la sua norma vale ± 1, equivale a dire che $a^2 - Nb^2 = \pm 1$.

Quindi $a + b\sqrt{N}$ é invertibile se e solo se (a, b) risolve l'equazione di Pell (24) o l'equazione (27).

Se esiste una soluzione (a, b) della (27) allora:
- le potenze dispari di $a + b\sqrt{N}$ sono soluzioni della (27);
- le potenze pari danno invece soluzioni della (24).

Se invece (a, b) é una soluzione della (24) allora:
- tutte le potenze di $a + b\sqrt{N}$ danno soluzioni della (24).

9.1 Interi algebrici e interi dei campi quadratici

Andiamo ad analizzare piú a fondo la questione, cominciando con alcune definizioni e teoremi di teoria algebrica dei numeri.

Definizione 2 *θ é un* numero algebrico *su un campo F se esiste un polinomio non nullo a coefficienti in F, di cui θ é uno zero, cioé:*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad con\ a_i \in F$$

tale che $p(\theta) = 0$.

Definizione 3 *θ si dice* semplicemente algebrico *se é algebrico su $\mathbb{Q}$ cioé é zero di un polinomio a coefficienti in $\mathbb{Q}$.*

Definizione 4 *I* coniugati di *θ sono tutte le altre radici del polinomio minimo*[3] *di θ su F.*

Definizione 5 *Un numero algebrico α si dice* intero algebrico *se il suo polinomio minimo ha la forma:*

$$p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \qquad con\ a_i \in \mathbb{Z}\ .$$

Definizione 6 *Un* campo quadratico *é un campo di grado 2 sui razionali. Esso é della forma $\mathbb{Q}(\theta)$, ove θ é radice di un polinomio di grado 2 irriducibile su $\mathbb{Q}$.*

Lemma 3 *Se α é zero di qualche polinomio $f(x)$ monico a coefficienti in $\mathbb{Z}$, allora α é intero algebrico.*

Teorema 9 *Se α é zero di qualche polinomio $f(x)$ monico che ha come coefficienti interi algebrici, cioé:*

$$p(x) = x^n + \gamma_{n-1}x^{n-1} + \ldots + \gamma_1 x + \gamma_0 \qquad con\ \gamma_i\ interi\ algebrici$$

allora α é intero algebrico.

[3]Per polinomio minimo si intende il polinomio monico di grado minimo di cui θ é radice.

Teorema 10 *Se θ é un numero algebrico esiste sempre $r \in \mathbb{Z}$ tale che $r\theta$ é un intero algebrico.*

Dimostrazione Se θ soddisfa l'equazione:

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0$$

ove gli a_i sono interi. Allora $a_n\theta$ soddisfa l'equazione:

$$x^n + a_{n-1} x^{n-1} + a_n a_{n-2} x^{n-2} + a_n^2 a_{n-3} x^{n-3} + \ldots + a_n^{n-1} a_0 = 0$$

perció $a_n\theta$ é un intero algebrico. □

Teorema 11 *Sia F un campo e θ algebrico su F. Ogni elemento α di $F(\theta)$ si puó scrivere in modo unico nel seguente modo:*

$$\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$$

ove $a_i \in F$ e n é il grado di θ su F.

Ora mostriamo che forma ha $\mathbb{Q}(\theta)$ e quali sono gli interi (algebrici) di $\mathbb{Q}(\theta)$.

Teorema 12 *Ogni campo quadratico é della forma $\mathbb{Q}(\sqrt{D})$ ove D é un intero libero da quadrati.*
Gli interi algebrici di tale campo sono:

i) tutti i numeri della forma

$$l + m\sqrt{D} \qquad \text{ove } l, m \text{ sono interi;}$$

ii) nel caso in cui $D \equiv 1 \pmod 4$, occorre aggiungere anche tutti i numeri della forma:

$$\frac{l + m\sqrt{D}}{2} \qquad \text{ove } l, m \text{ sono interi dispari.}$$

Dimostrazione Quanto al primo enunciato, per il teorema 10 possiamo assumere che θ é un intero algebrico, perché per ogni $r \in \mathbb{Z}$ risulta

$$\mathbb{Q}\left(\frac{\theta}{r}\right) = \mathbb{Q}(\theta)$$

Ora supponiamo che θ soddisfi l'equazione

$$x^2 + 2ax + b = 0 \qquad \text{con } a, b \in \mathbb{Q}$$

allora

$$\theta = -a \pm \sqrt{a^2 - b}\ .$$

Se prendo a, b in mdo che $a^2 - b = s^2 D$ ove $D \in \mathbb{Z}$ e D sia libero da quadrati allora si ha:

$$\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{D})\ .$$

Pertanto ogni campo quadratico é della forma $\mathbb{Q}(\sqrt{D})$ ove D é un intero libero da quadrati.

Ora in base al teorema 11 i numeri $(1, \sqrt{D})$ formano una base per $\mathbb{Q}(\sqrt{D})$, perció ogni suo elemento é della forma

$$\frac{l + m\sqrt{D}}{n}$$

ove l, m, n sono interi coprimi[4] ed n é positivo.
Per definizione $\frac{l+m\sqrt{D}}{n}$ é intero algebrico se e solo se soddisfa un equazione del tipo:

$$x^2 + bx + c = 0 \qquad \text{con } b, c \in \mathbb{Z}$$

vale a dire che:

$$\left(\frac{l + m\sqrt{D}}{n}\right)^2 + b\left(\frac{l + m\sqrt{D}}{n}\right) + c = 0$$

il che equivale all'equazione:

$$\left(l + m\sqrt{D}\right)^2 + bn\left(l + m\sqrt{D}\right) + cn^2 = 0 \tag{31}$$

Continuando otteniamo un'equazione di questo tipo:

$$(l^2 + m^2 D + bnl + cn^2) + (2lm + bmn)\sqrt{D} = 0$$

che equivale a risolvere il seguente sistema:

$$\begin{cases} l^2 + m^2 D + bnl + cn^2 = 0 \\ \\ 2lm + bmn = 0 \end{cases} \tag{32}$$

Consideriamo la seconda equazione di questo sistema ed otteniamo:

$$m(2l + bn) = 0\ .$$

[4]Si intende che non ci sono primi che dividono simultaneamente l, m, n; in particolare se $m = 0$ allora l, n sono coprimi nel senso usuale.

Se $m = 0$ allora $\frac{l+m\sqrt{D}}{n} = \frac{l}{n}$ che é intero se e solo se $n \mid l$. Per ipotesi l, m, n sono coprimi quindi $n = \pm 1$.
Perció $\frac{l}{n} = \pm l \in \mathbb{Z}$ come ci aspettavamo, cioé gli elementi appartenenti a $\mathbb{Z}$, sono interi anche in $\mathbb{Q}(\sqrt{D})$.

Se $m \neq 0$ allora deve essere che

$$-2l = bn$$

Sostituendolo nella prima equazione del sistema (32) si ottiene:

$$m^2 D = l^2 - cn^2$$

Supponiamo ora che $(l, n) = d$, allora $l = dl_1$ e $n = dn_1$ con $l_1, n_1 \in \mathbb{Z}$. Quindi:

$$m^2 D = d^2(l_1^2 - cn_1^2)$$

da cui si ha che $d^2 \mid m^2 D$, ma D é libero da quadrati allora $d \mid m^2$.
Se ci fosse un primo p tale che $p|d$ allora $p|m$ ma per definizione $d = (l, n)$, pertanto $p|d$ implica anche $p|l$ e $p|n$. Perció $d = 1$. Dall'equazione $-2l = bn$ allora si ha che $l \mid b$, cioé $b = lk$ $(\exists k \in \mathbb{Z})$ e quindi:

$$-2l = lkn \qquad \Longleftrightarrow \qquad -2 = kn$$

ed essendo k, n interi ed in particolare n é positivo si avrá che n potrá essere uguale a:

$$n = \begin{cases} 1 \\ \\ 2 \end{cases}$$

Consideriamo i due casi separatamente.

Se $n = 1 \qquad \Longrightarrow \qquad l + m\sqrt{D}$ é un intero algebrico infatti esso soddisfa l'equazione (31).

Se $n = 2 \qquad \Longrightarrow \qquad \frac{l+m\sqrt{D}}{2}$ soddisfa l'equazione

$$x^2 - lx + \frac{l^2 - Dm^2}{4} = 0$$

quindi rappresenta un intero algebrico se e solo se $\frac{l^2-Dm^2}{4} \in \mathbb{Z}$ (cioé $4 \mid l^2 - Dm^2$) il che equivale a risolvere la seguente congruenza:

$$l^2 \equiv m^2 D \ (mod\ 4) \tag{33}$$

Poiché $(l, n) = (l, 2) = 1$, per ipotesi, allora l é dispari ($l = 2t + 1 \quad \exists t \in \mathbb{Z}$); pertanto la (33) diventa:

$$1 \equiv m^2 D \ (mod\ 4)$$

Ora D essendo libero da quadrati puó essere congruo a $1, 2, 3\ mod(4)$. Consideriamo i vari casi separatamnete.

1. Se $D \equiv 3\ (mod\ 4)$ allora la (33) diventa:

   $$1 \equiv 3m^2$$

   - se m é pari ottengo che $1 \equiv 0\ (mod\ 4)$ il che é impossibile;
   - se m é dispari ottengo che $1 \equiv 3\ (mod\ 4)$ il che é impossibile.

   Perció se $D \equiv 3\ (mod\ 4)$, $\frac{l+m\sqrt{D}}{2}$ non é un intero algebrico.

2. Se $D \equiv 2\ (mod\ 4)$ allora la (33) diventa:

   $$1 \equiv 2m^2$$

   - se m é pari ottengo che $1 \equiv 0\ (mod\ 4)$ il che é impossibile;
   - se m é dispari ottengo che $1 \equiv 2\ (mod\ 4)$ il che é impossibile.

   Perció se $D \equiv 2\ (mod\ 4)$, $\frac{l+m\sqrt{D}}{2}$ non é un intero algebrico.

3. Se $D \equiv 1\ (mod\ 4)$ allora la (33) diventa:

   $$1 \equiv m^2$$

   - se m é pari ottengo che $1 \equiv 0\ (mod\ 4)$ il che é impossibile;
   - se m é dispari ottengo che $1 \equiv 1\ (mod\ 4)$ il che é vero.

   Perció se $D \equiv 1\ (mod\ 4)$, $\frac{l+m\sqrt{D}}{2}$ é un intero algebrico se e solo se l, m sono entrambi dispari.

Concludendo, gli interi algebrici di $\mathbb{Q}(\sqrt{D})$ sono:

i) tutti i numeri della forma

$$l + m\sqrt{D} \qquad \text{con } l, m \in \mathbb{Z}\ ;$$

ii) inoltre, nel caso in cui $D \equiv 1\ (mod\ 4)$ occorre aggiungere anche i numeri del tipo

$$\frac{l + m\sqrt{D}}{2} \qquad \text{ove } l, m \text{ sono interi dispari.}$$

□

9.2 Unitá dei campi quadratici e legame con l'equazione di Pell

Una volta individuato quali sono gli interi di un campo quadratico, cerchiamo di determinare le sue unitá. Addentrandoci in tale studio vedremo come questo problema sia legato all'equazione di Pell.

Sia $\alpha = a + b\sqrt{D}$ (con $a, b \in \mathbb{Q}$) un intero algebrico di $\mathbb{Q}(\sqrt{D})$. La sua norma é data, come giá visto:

$$N(\alpha) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2 \ .$$

In base al teorema 8 possiamo dire che $\alpha = a + b\sqrt{D}$ é unitá se e solo se $a^2 - Db^2 = \pm 1$. Pertanto trovare le unitá di $Q\sqrt{D}$ equivale a risolvere l'equazione di Pell (24) o l'equazione (27).
Proseguiamo con lo studio, considerando i possibili valori di D.

1. Se D non é congruo a 1 $(mod\ 4)$ allora gli interi algebrici di $\mathbb{Q}(\sqrt{D})$ sono della forma $l+m\sqrt{D}$ con $l, m \in \mathbb{Z}$. quindi trovare le unitá equivale a risolvere le equazioni (24) e (27)

$$l^2 - Dm^2 = \pm 1 \qquad \text{con } l, m \in \mathbb{Z} \ . \tag{34}$$

2. Se $D \equiv 1\ (mod\ 4)$ allora agli interi algebrici di $\mathbb{Q}(\sqrt{D})$ appena visti occorre aggiungere i numeri della forma $\frac{l+m\sqrt{D}}{2}$ con $l, m \in \mathbb{Z}$ ed entrambi dispari.
   Quindi trovare le unitá tra questi numeri equivale a risolvere l'equazione:

$$l^2 - Dm^2 = \pm 4 \qquad \text{con } l, m \text{ interi dispari.} \tag{35}$$

   Questa é una forma piú generale dell'equazione di Pell.

A questo punto vediamo quali sono le unitá di $\mathbb{Q}(\sqrt{D})$. Prima di tutto consideriamo il caso in cui $D < 0$, in tali casi $\mathbb{Q}(\sqrt{D})$ é detto *immaginario.*

Teorema 13 *Per trovare le unitá di* $\mathbb{Q}(\sqrt{D})$ *nel caso in cui* $D < 0$ *occorre fare una distinzione:*

i) se $D \neq -1$ *e* $D \neq -3$ *allora le unitá sono* ± 1*;*

ii) se $D = -1$ *allora le unitá di* $\mathbb{Q}(\sqrt{-1})$ *sono* ± 1 *e* $\pm i$*;*

iii) se $D = -3$ *allora le unitá di* $\mathbb{Q}(\sqrt{-3})$ *sono* ± 1 *e* $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

Dimostrazione Nelle equazioni (34) e (35) il primo membro risulta essere positivo, perció basterá considerare solo le equazioni con il secondo membro positivo.

Se $D \equiv 2 \ (mod\ 4)$ o $D \equiv 3 \ (mod\ 4)$ sappiamo che gli interi algebrici sono della forma $l + m\sqrt{D}$ con $l, m \in \mathbb{Z}$. Si tratta allora di risolvere l'equazione $l^2 - Dm^2 = 1$, le cui uniche soluzioni intere sono:

$$l = \pm 1 \ ; \qquad m = 0 \ ;$$

tranne quando $D = -1$ perché ad esse occorre aggiungere anche:

$$l = 0 \ ; \qquad m = \pm 1 \ .$$

Riassumendo se $D \equiv 2 \ (mod\ 4)$ o se $D \equiv 3 \ (mod\ 4)$ allora le unitá sono ± 1 tranne quando $D = -1$, in tale caso occorre aggiungere anche $\pm i$.

Se $D \equiv 1 \ (mod\ 4)$ oltre a quelli visti gli interi algebrici di $\mathbb{Q}(\sqrt{D})$ sono della forma $\frac{l+m\sqrt{D}}{2}$ ove l, m sono interi dispari. Si tratta allora di risolvere l'equazione $l^2 - Dm^2 = 4$, e se $D \neq -3$ le uniche soluzioni intere sono:

$$l = \pm 2 \ ; \qquad m = 0 \ ;$$

perció si ottiene che le unitá sono:

$$\frac{l}{2} = \frac{\pm 2}{2} = \pm 1$$

come giá sapevamo.
Peró nel caso in cui $D = -3$ l'equazione (35) diventa:

$$l^2 + 3m^2 = 4$$

che ha come soluzioni:

$$l = \pm 1 \ ; \qquad m = \pm 1 \ .$$

Riassumendo se $D \equiv 1 \ (mod \ 4)$ allora le unitá sono ± 1, peró nel caso in cui $D = -3$ devo anche aggiungere $\frac{\pm 1 \pm \sqrt{-3}}{2}$.

Andiamo ora a considerare il caso in cui $D > 0$. Prima di andare avanti é opportuno dare i segenti teoremi e lemmi.

Teorema 14 *Sia c un numero reale positivo, e sia K un campo di numeri algebrici. Allora esiste solo un numero finito di interi algebrici x in K tali che $|x^{(i)}| \leq c$ ove gli $x^{(i)}$ sono tutti i coniugati di x.*

Dimostrazione Sia $[K : \mathbb{Q}] = n$ e siano $\sigma_1, \sigma_2, \ldots, \sigma_n$ i polinomi simmetrici elementari.
Sia c' un numero reale sufficientemente grande, per esempio:

$$c' = max \left\{ nc, \binom{n}{2} c, \ldots, \binom{n}{k} c^k, \ldots, c^n \right\}$$

Sia poi F l'insieme di tutti i polinomi monici di grado al massimo n i cui coefficienti siano interi a tali che $|a| \leq c'$. Tale F é un insieme finito.
Sia S l'insieme degli elementi di K che sono radici di un polinomio di F. Anche S é un insieme finito.
Se $|x^{(i)}| \leq c$ per tutti i coniugati di $x \in K$ allora

$$\sigma_k(x^{(1)}, \ldots, x^{(n)}) \leq c'$$

$\big($perché $\sigma_k = (-1)^k \frac{a_{n-k}}{a_n}$ ove a_{n-k}, a_n sono i coefficienti del polinomio $a_n x^n + \ldots + a_0$ a cui si riferisce l'insieme S, ma $|a| \leq c'$ allora $\sigma_k(x^{(1)}, \ldots, x^{(n)}) \leq c' \ \big)$.

Poiché x é un intero algebrico allora $\sigma_k(x^{(1)}, \ldots, x^{(n)}) \in \mathbb{Z}$ e pertanto il polinomio:

$$\prod_{i=1}^{n} \left(X - x^{(i)} \right)$$

appartiene ad F, allora $x \in S$.

Cosí abbiamo trovato un insieme finito S (che dipende dalla costante c) per il quale abbiamo provato che se x é intero algebrico su K tale che $|x^{(i)}| \leq c$ per tutti i coniugati di x allora $x \in S$. □

Teorema 15 *x é radice di un unitá in $R(\theta)$ (ove R é un campo) se e solo se x é un intero algebrico tale che $|x^i| = 1$ per tutti i coniugati x^i di x.*

Dimostrazione "$\Longrightarrow$" Se x é radice dell'unitá allora lo sono anche tutti i suoi coniugati. Da $x^m = 1$ segue che x é intero algebrico di K e inoltre:

$$x^m = 1 \quad \Longrightarrow \quad |x|^m = 1 \quad \Longrightarrow \quad |x| = 1 \quad \Longrightarrow \quad |x^{(i)}| = 1 \ \ \forall\, x^{(i)} \ .$$

"$\Longleftarrow$ " Per il teorema 15 c'é solo un numero finito di interi algebrici $x \in K$ tali che $|x^{(i)}| = 1 \ \ \forall\, x^{(i)}$.
Ora $x, x^2, x^3, \ldots$ hanno tutti tale proprietá, allora esistono interi r, s con $r < s$ tali che $x^r = x^s$. Allora $x^{r-s} = 1$, cioé x é radice dell'unitá. □

Teorema 16 *Il gruppo W delle radici dell'unitá di $R(\theta)$ é un gruppo ciclico moltiplicativo finito.*

Dimostrazione Usando i teoremi 15 e 16 si ha che W é finito.
Sia poi h il massimo degli ordini degli elementi di W. Ora l'ordine di ogni elemento di W divide h, quindi W é contenuto nel gruppo delle radici h-esime dell'unitá. Quest'ultimo gruppo é ciclico e pertanto anche W é ciclico. Pertanto W é un gruppo ciclico finito. □

Lemma 4 *Se α é un numero irrazionale, allora per ogni intero $m > 0$ esistono a, b interi (non entrambi nulli) tali che:*

i) $|a| \leq m$ *e* $|b| \leq m$;

ii) $|a + \alpha b| \leq \frac{1+\alpha}{m}$.

Dimostrazione Sia $f = X + \alpha Y$ e consideriamo l'insieme S dei valori $f(a, b) = a + \alpha b$ quando $0 \leq a \leq m$ e $\leq b \leq m$. Poiché α é irrazionale se $(a, b) \neq (a', b')$ allora $f(a, b) \neq f(a', b')$. Perció $|S| = (m + 1)^2$.
Tutti gli elementi di S appartengono all'intervallo $[0 \ , \ m + \alpha m]$. Dividiamo tale intervallo in m^2 parti uguali, cioé:

$$\left[0 \ , \ \frac{1+\alpha}{m}\right] ; \quad \left[\frac{1+\alpha}{m} \ , \ 2\frac{(1+\alpha)}{m}\right] ; \quad \ldots$$

Sicuramente esistono almeno 2 elementi di S che appartengono allo stesso sottointervallo, cioé:

$$\frac{r(1+\alpha)}{m} \leq a_1 + \alpha b_1 < a_2 + \alpha b_2 \leq \frac{(r+1)(1+\alpha)}{m}$$

Pertanto ponendo $a = a_2 - a_1$ e $b = b_2 - b_1$ noi otteniamo che:

$$|a + \alpha b| \leq \frac{1 + \alpha}{m}$$

con a, b non entrambi nulli e $|a| \leq m$ e $|b| \leq m$. □

Per concludere, ricordiamo che stiamo considerando il caso in cui $D > 0$. In tale caso $\mathbb{Q}(\sqrt{D})$ é contenuto nel campo dei reali. Pertanto le uniche radici dell'unitá sono ± 1.
Vogliamo mostrare che ci sono altre unitá in $\mathbb{Q}(\sqrt{D})$.

Teorema 17 *Se D é un intero positivo libero da quadrati allora il gruppo U delle unitá di $\mathbb{Q}(\sqrt{D})$ é:*

$$U \simeq \{-1, 1\} \times C$$

ove C é un gruppo ciclico moltiplicativo infinito.

Dimostrazione Abbiamo giá visto che il gruppo delle radici dell'unitá in $\mathbb{Q}(\sqrt{D})$ é

$$W = \{-1, 1\} \ .$$

Per mostrare che esistono altre unitá in $\mathbb{Q}(\sqrt{D})$ usiamo il lemma 4, con $\alpha = \sqrt{D}$.
Per ogni m, sia S_m l'insieme delle coppie (a, b) con a, b interi non entrambi nulli e tali che $|a| \leq m$, $|b| \leq m$ e $|a + b\sqrt{D}| \leq \frac{1+\sqrt{D}}{m}$.
Per il lemma 4 ciascun insieme S_m é non vuoto. Scrivendo S nel seguente modo:

$$S = S_m^+ \cup S_m^- \cup S_m^0$$

ove

$$\begin{aligned} S_m^+ &= \{(a, b) \in S_m \ | \ a > 0\} \ ; \\ S_m^- &= \{(a, b) \in S_m \ | \ a < 0\} \ ; \\ S_m^0 &= \{(a, b) \in S_m \ | \ a = 0\} \ . \end{aligned}$$

Se $(a, b) \in S_m^+$ allora $-(a, b) = (-a, -b) \in S_m^-$ e viceversa.
Inoltre se $m = 1 \quad S_1^0 = \{(0, 1); \ (0, -1)\}$.
Se $m \geq 2 \quad S_m^0 = \emptyset$ infatti deve essere che

$$|a + b\sqrt{D}| \leq \frac{1 + \sqrt{D}}{m}$$

allora

$$|b\sqrt{D}| \leq \frac{1+\sqrt{D}}{m} \quad \Longrightarrow \quad |b| \leq \frac{1}{m}\left(\frac{1}{\sqrt{D}}+1\right) \leq \frac{1}{2}\left(1+\frac{1}{\sqrt{D}}\right) < 1$$

cioé $|b| < 1$ il che é impossibile perché b non puó essere zero essendo $a = 0$.

Supponiamo per assurdo che $\bigcup_{m\geq 1} S_m$ sia un insieme finito. Allora esiste un m_0 tale che $\frac{1}{m_0} < |a + b\sqrt{D}|$ per ogni $(a, b) \in \bigcup_{m\leq 1} S_m$.
D'altra parte se m é abbastanza grande e se $(a, b) \in S_m$.
Allora:

$$|a + b\sqrt{D}| < \frac{1+\sqrt{D}}{m} \leq \frac{1}{m_0}$$

il che é assurdo.
Allora $\bigcup_{m\geq 1} S_m$ é un insieme infinito, ed anche $\bigcup_{m\geq 1} S_m^+$ é infinito (altrimenti $|S_m^-| = |S_m^+|$ per ogni m da cui segue che $\bigcup_{m\geq 1} S_m$ é finito, il che é un assurdo).
Da $|a| \leq m$ e $|b| \leq m$ segue che

$$|a - b\sqrt{D}| \leq |a| + |b|\sqrt{D} \leq m(1+\sqrt{D})$$

quindi

$$0 \neq |a^2 - Db^2| = |a - b\sqrt{D}||a + b\sqrt{D}| \leq m(1+\sqrt{D})\frac{1+\sqrt{D}}{m} = (1+\sqrt{D})^2$$

per ogni $(a, b) \in \bigcup_{m\geq 1} S_m$ (e di conseguenza anche per ogni coppia $(a, b) \in \bigcup_{m\geq 1} S_m^+$).
Quindi esiste un intero $n \qquad 0 < |n| \leq (1+\sqrt{D})^2$ tale che:

$$a^2 - Db^2 = n$$

per infinite coppie di interi (a, b) ove $a > 0$.

Consideriamo $n^2 + 1$ di queste coppie. Poi definiamo la seguente relazione di equivalenza:

$$(a_1, b_1) \equiv (a_2, b_2) \quad \Longleftrightarrow \quad \big(a_1 \equiv_n a_2 \;\; e \;\; b_1 \equiv_n b_2\big)$$

Quindi abbiamo al massimo n^2 classi di equivalenza. Ma il numero delle coppie (a, b) é maggiore di n^2, allora vi sono almeno 2 coppie distinte (a_1, b_1) e (a_2, b_2) che stanno nella stessa classe di equivalenza.
Pongo $x_1 = a_1 + b_1\sqrt{D}$ e $x_2 = a_2 + b_2\sqrt{D}$ e consideriamo $u = \frac{x_1}{x_2}$.
Ora poiché le due coppie (a_1, b_1) e (a_2, b_2) sono tali che $a^2 - Db^2 = n$ allora:

$$N(x_1) = N(x_2) = n$$

perció

$$N(u) = \frac{N(x_1)}{N(x_2)} = \frac{n}{n} = 1$$

e $u \neq \pm 1$ perché $x_1 \neq x_2$ e $x_1 \neq -x_2$ (quest'ultima perché $a_1 > 0$ e $a_2 > 0$).
Ma

$$u = \frac{x_1}{x_2} = 1 + \frac{x_1}{x_2} - 1 = 1 + \frac{x_1 - x_2}{x_2} = 1 + \frac{(x_1 - x_2)x_2'}{x_2 x_2'}$$

ove x_2' é il coniugato di x_2
Continuando:

$$1 + \frac{(x_1 - x_2)x_2'}{x_2 x_2'} = 1 + \frac{(x_1 - x_2)x_2'}{N(x_2)} = 1 + \left(\frac{a_1 - a_2}{n} + \frac{b_1 - b_2}{n}\sqrt{D} \right)(a_2 - b_2\sqrt{D})$$

e notiamo che $\frac{a_1 - a_2}{n}$ e $\frac{b_1 - b_2}{n}$ sono interi (perché $a_1 \equiv_n a_2 \;\; e \;\; b_1 \equiv_n b_2$).
Sviluppando i calcoli si ottiene:

$$u = a + b\sqrt{D} \qquad \text{con } a, b \in \mathbb{Z} \; .$$

Quindi u é un unitá diversa da ± 1.

Esistono anche unitá u di $\mathbb{Q}(\sqrt{D})$ tali che $u > 1$, infatti se u_1 é unitá anche $-u_1, u_1^{-1}, -u_1^{-1}$ lo sono e la piú grande di queste é maggiore di 1.
Cerchiamo di mostrare che di queste unitá $u > 1$, ne esiste una piú piccole di tutte.
Per farlo basta mostrare che per ogni numero reale $c > 1$, esiste solo un numero finito di unitá u tali che $1 < u < c$.
Se u é unitá $N(u) = uu' = \pm 1$ da cui:

$$u' = \frac{uu'}{u} = \frac{N(u)}{u} = \pm\frac{1}{u}$$

ma

$$1 < u < c \quad \Longleftrightarrow \quad \left(\frac{1}{c} < u' < 1 \right) \;\text{ o }\; \left(-1 < u' < -\frac{1}{c} \right)$$

comunque in ogni caso $|u'| < c$.
Ma per il teorema 14 esistono solo un numero finito di interi algebrici x di $\mathbb{Q}(\sqrt{D})$ tali che $|x^i| \leq c$ per tutti i coniugati x^i di x.
Allora l'insieme di queste unitá é finito.

Sia u_1 la piú piccola unitá tale che $u_1 > 1$. Mostriamo che ogni unitá u maggiore di zero é una potenza di u_1.
Infatti, esistono interi m tali che:

$$u_1^m \leq u \leq u_1^{m+1}$$

allora dividendo per u_1^m:

$$1 \leq \frac{u}{u_1^m} < u_1$$

quindi $\frac{u}{u_1^m}$ é ancora unitá tale che $1 \leq \frac{u}{u_1^m} < u_1$.
Ma u_1 era la piú piccola unitá maggiore di 1, allora:

$$\frac{u}{u_1^m} = 1 \quad \Longleftrightarrow \quad u = u_1^m$$

Analogamente per tutte le unitá negative, esse sono della forma:

$$-u_1^m \quad \text{con } m \in \mathbb{Z}$$

Sia infine C il gruppo moltiplicativo generato da u_1.
La funzione cosí definita:

$$\begin{array}{ccc} U & \longrightarrow & \{-1,1\} \times C \\ \\ u_1^m & \mapsto & (1, u_1^m) \\ -u_1^m & \mapsto & (1, -u_1^m) \end{array}$$

é chiaramente un isomorfismo. □

La piú piccola unitá $u_1 > 1$ é detta unitá fondamentale di $\mathbb{Q}(\sqrt{D})$.

Per provare i teoremi 6 e 7 sarebbe bastato dimostrare che é essenzialmente ciclico il gruppo degli invertibili di $\mathbb{Z}[\sqrt{D}]$, indipendentemente dal fatto che sia l'anello degli interi algebrici di $\mathbb{Q}(\sqrt{D})$ o un suo sottoanello proprio (per l'equazione (24) $x^2 - Dy^2 = 1$ lo abbiamo visto direttamente al paragrafo 8.2).
É evidente che il gruppo degli invertibil di $\mathbb{Z}[\sqrt{D}]$, essendo un sottogruppo di $\{-1,1\} \times C$, ha ancora la stessa struttura.

10 Misura di irrazionalitá

Per ogni irrazionale γ si puó dimostrare che é infinito il numero di frazioni $\frac{p_n}{q_n}$ tali che

$$\left|\gamma - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2} \tag{36}$$

La costruzione di queste frazioni $\frac{p_n}{q_n}$ é strettamente legato allo sviluppo in frazioni continue di γ. Infatti i convergenti nello sviluppo in frazioni continue di γ soddisfano la (36) che é immediata conseguenza della (10) del capitolo 4.

I numeri irrazionali $\gamma = \{a_0; a_1, a_2, \dots\}$ per i quali la successione dei termini a_n é superiormente limitata (cioé tali che $a_n < H \quad$ con $n = 1, 2, 3, \dots$ per un'opportuna costante $H > 0$) sono tutti e soli quelli per cui la disuguaglianza (36) é, a meno di costanti moltiplicative, la migliore possibile, cioé quella per cui:

$$\left|\gamma - \frac{p}{q}\right| > \frac{1}{Kq^2} \tag{37}$$

per ogni razionale $\frac{p}{q}$ e per un'opportuna costante $K > 0$.
In particolare quest'ultima disuguaglianza vale per ogni irrazionale quadratico γ in virtú del teorema di Lagrange.

Dato un irrazionale γ é naturale chiedersi per quali esponenti λ la disuguaglianza

$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{q^\lambda} \tag{38}$$

abbia infinite soluzioni razionali $\frac{p}{q}$.
La risposta a questa domanda non é univoca, ma dipende dall'irrazionale γ che si considera, suggerendo cosí una classificazione degli irrazionali. Precisamente si dá la seguente definizione:

Definizione 7 *Dato un irrazionale γ, si dice che μ é una misura di irrazionalitá di γ se per ogni $\epsilon > 0$ esiste una costante $C = C(\gamma, \epsilon) > 0$ tale che*

$$\left|\gamma - \frac{p}{q}\right| > \frac{1}{Cq^{\mu+\epsilon}} \tag{39}$$

per ogni p, q interi e $q > 0$.

Il minimo esponente μ per cui vale la condizione (39) si indica con $\mu(\gamma)$. Si noti che $\mu(\gamma)$ é l'estremo inferiore degli esponenti λ tali che la diseguaglianza (38) valga al piú per un numero finito di razionali $\frac{p}{q}$, e quindi é anche

l'estremo superiore degli esponenti λ tali che la (38) valga per infiniti $\frac{p}{q}$.

Per la (36) si ha che $\mu(\gamma) \geq 2$ per ogni irrazionale γ.
Si possono avere irrazionali γ tali che

$$\left|\gamma - \frac{p_n}{q_n}\right| < \frac{1}{f(q_n)}$$

(ove $f(q)$ é una funzione che tende a $+\infty$ per $q \to +\infty$ e $\frac{p_n}{q_n}$ é la successione dei convergenti a γ).
Se $f(q)$ tende a $+\infty$ piú rapidamente di q^λ per ogni λ (per esempio sia $f(q) = e^q$) allora la (38) vale per infiniti $\frac{p}{q}$, perció qualunque sia l'esponente λ allora $\mu(\gamma) = +\infty$ (si parla in questo caso di numeri di Liouville).

Ricordiamo che esistono infiniti irrazionali γ tali che $\mu(\gamma)$ sia uguale ad un reale prefissato nell'intervallo $[2, +\infty[$.

Cerchiamo di capire quale sia il valore piú probabile per $\mu(\gamma)$, se prendiamo un irrazionale γ a caso.
La risposta é data dalla seguente proposizione:

Proposizione 4 *Quasi tutti gli irrazionali γ sono tali che $\mu(\gamma) = 2$; piú precisamente l'insieme degli irrazionali γ per i quali $\mu(\gamma) > 2$ ha misura nulla.*

Questo risultato é un corollario del teorema seguente:

Teorema 18 *Sia $\varphi(q) > 0$ una funzione definita per $q = 1, 2, 3, \ldots$.*
Se la serie

$$\sum_{q=1}^{+\infty} \frac{1}{\varphi(q)}$$

converge, allora l'insieme E_φ degli irrazionali γ tali che la disuguaglianza

$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{q\varphi(q)}$$

abbia infinite soluzioni razionali $\frac{p}{q}$, ha misura nulla.

Dimostrazione l'insieme E_φ é invariante per una traslazione intera, e poiché l'unione numerabile di insiemi di misura nulla ha misura nulla, sará sufficiente

mostrare che $E_\varphi \cap [0,1]$ ha misura nulla.
Dato un $\epsilon > 0$, piccolo a piacere, fissiamo un intero N tale che

$$\sum_{q=N}^{+\infty} \frac{1}{\varphi(q)} < \frac{\epsilon}{2} \ .$$

Ora consideriamo la funzione

$$\begin{array}{rccc} \psi: & E_\varphi \cap [0,1] & \longrightarrow & \mathbb{Q} \\ & \gamma & \mapsto & \dfrac{p}{q} \end{array}$$

che ad ogni $\gamma \in E_\varphi \cap [0,1]$ associa un razionale $\frac{p}{q}$ con le seguenti proprietá:

i)
$$q \geq N \ ;$$

ii)
$$q\varphi(q) > \frac{1}{\|\gamma\|} \qquad \text{ove} \ \ \|\gamma\| = min\ _{n\in\mathbb{Z}} \left|\gamma - n\right| \ ;$$

iii)
$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{q\varphi(q)} \ ;$$

cosa evidentemente possibile perché per ipotesi quest'ultima disuguaglianza ha infinite soluzioni razionali.
Se $\frac{p}{q}$ soddisfa queste 3 condizioni allora ho che

$$\left|\gamma - \frac{p}{q}\right| < \|\gamma\|$$

e cioé

$$0 < \frac{p}{q} < 1 \qquad (\text{ anche } 0 < \gamma < 1 \text{ perché } \gamma \in E_\varphi \cap [0,1])$$

Sia ora $\psi(\gamma) = \frac{p}{q}$. Dato un qualunque intero $q \geq N$, considero tutte le coppie (p, γ) tali che $\psi(\gamma) = \frac{p}{q}$.
Poiché $0 < \frac{p}{q} < 1$ allora i valori di p non superano q.
Inoltre per ogni p le controimmagini di $\frac{p}{q}$ (cioé $\psi^{-1}\left(\frac{p}{q}\right)$) stanno nell'intervallo

$$\left[\frac{p}{q} - \frac{1}{q\varphi(q)} \ \ , \ \ \frac{p}{q} + \frac{1}{q\varphi(q)}\right]$$

che ha lunghezza $\frac{2}{q\varphi(q)}$.
Perció per ogni $q \geq N$ tutti i γ tali che $\psi(\gamma) = \frac{p}{q}$ per qualche p sono contenuti in un'unione di intervalli di misura complessiva $\leq q\frac{2}{q\varphi(q)} = \frac{2}{\varphi(q)}$. Ne segue che $E_\varphi \cap [0,1]$ é contenuto in un insieme di misura $\leq \sum_{q=N}^{+\infty} \frac{2}{\varphi(q)} < 2\frac{\epsilon}{2} = \epsilon$ e perció ha misura nulla. □

Per dimostrare la proposizione si procede cosí:

per ogni $\delta > 0$, indichiamo con F_δ l'insieme degli irrazionali γ tali che la disuguaglianza

$$\left|\gamma - \frac{p}{q}\right| < \frac{1}{q^{2+\delta}}$$

abbia infinite soluzioni razionali $\frac{p}{q}$.
Poiché la serie

$$\sum_{q=1}^{+\infty} \frac{1}{q^{1+\delta}}$$

converge, allora per il teorema precedente F_δ ha misura nulla.
Se $\delta_1, \delta_2, \delta_3, \ldots$ é una qualunque successione di positivi che tende a zero, allora l'insieme degli irrazionali γ tali che $\mu(\gamma) > 2$ é contenuta nell'unione numerabile:

$$\bigcup_{n=1}^{+\infty} F_\delta$$

e quindi ha misura nulla.

Come giá anticipata nel capitolo precedente sono pochi gli irrazionali, oltre ai quadratici, dei quali si conosca qualche aspetto di regolaritá, cioé per i quali sia possibile determinare per ogni n il termine a_n in modo ricorsivo, senza dover calcolare $a_0, a_1, a_2, \ldots, a_{n-1}$.
Fra questi irrazionali vi é il numero e e tutte le sue radici (di tutti gli ordini):

$$e = \{2; 1, 2, 1, 1, 4, 1, 1, 6, 1, \ldots, 1, 2n, 1, \ldots\}$$

$$e^{\frac{1}{s}}\{1; s-1, 1, 1, 3s-1, 1, 1, 5s-1, \ldots, 1, (2n+1)s-1, 1, \ldots\} .$$

Si noti che $\mu(e) = \mu(\sqrt{e}) = \ldots = \mu(\sqrt[n]{e}) = \ldots = 2$.
Invece per l'irrazionale π non si sono trovati aspetti di regolaritá. Si congettura che $\mu(\pi) = \mu(\pi^2) = 2$, ma con gli strumenti noti finora si é solo maostrato che:

$$\mu(\pi^2) < 5,44124\ldots$$
$$\mu(\pi) < 8,01604\ldots .$$

11 Aspetti probabilistici

In questo paragrafo accenneremo, senza dimostrazioni, 2 teoremi riguardanti la probabilitá che un intero a_i compaia nello sviluppo in frazioni continue di un numero reale e altri problemi probabilistici.

Sia x un numero reale scelto casualmente. Noi sappiamo che x ha uno sviluppo in frazioni continue:

$$x = \{a_0; a_1, a_2, \dots, a_n, \dots\}$$

con gli $a_i \in \mathbb{N}$ per $i > 0$. Indichiamo con x_n il quoziente completo $x_n = a_n + \frac{1}{x_{n+1}}$ ove $\frac{1}{x_{n+1}}$ é la parte frazionaria di x_n.
Gauss in una lettera indirizzata a Laplace diceva di aver scoperto che per le tipiche espansioni in frazioni continue la probabilitá che la parte frazionaria di x_n sia minore di x tende a $log_2(1+x)$, cioé:

$$P\left(\frac{1}{x_{n+1}} < x\right) = P\big(\{0; a_{n+1}, a_{n+2}, \dots\} < x\big) \to log_2(1+x)$$

cioé

$$\lim_{n\to\infty} P\big(\{0; a_{n+1}, a_{n+2}, \dots\} < x\big) = log_2(1+x)$$

Una dimostrazione di ció fu data da Kuzmin e da Lévy.
Piú precisamente, se si considerano le espansioni in frazioni continue di "quasi tutti"[5] i numeri reali la probabilitá che il termine $a_n = k$ si avvicina a:

$$P(a_n = k) = P(k) = \frac{log_2\left(1 + \frac{1}{k(k+2)}\right)}{log_2 2} = log_2\left(1 + \frac{1}{k(k+2)}\right) = -log_2\left(1 - \frac{1}{(k+1)^2}\right)$$

É opportuno ricordare che poiché si tratta di una distribuzione di probabilitá:

1. $\sum_{k=1}^{+\infty} P(k) = 1$;
2. i valori di k elevati sono rari si ha infatti che circa il 41% dei termini é 1; mentre circa il 17% dei termini é 2;
3. si noti che e non appartiene alla categoria di quasi tutti reali, mentre π sembra farne parte.

[5]Con ció intendiamo che l'insieme dei reali per i quali non vale la suddetta proprietá ha misura nulla.

Ora se $k \to +\infty \qquad P(k) \to \frac{1}{k^2}$.
Pertanto se noi vogliamo calcolare il valore medio di k, nello sviluppo in frazioni continue di quasi tutti i reali si ha che tale media é infinita. Infatti la media é data da:

$$\sum_{k=1}^{+\infty} kP(k)$$

(e poiché $\sum_{n=1}^{+\infty} \frac{1}{n^a}$ diverge se $a \leq 1$ allora mi trovo nella situazione:

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

che diverge.

La figura 3 mostra la distribuzione dei primi 500 termini nello sviluppo in frazioni continue di π, $sin\ 1$, della costante di Eulero-Mascheroni (γ) e della costante di Copeland-Erdos (C).

[Apriamo un piccola parentesi per introdurre quest'ultime due costanti: la costante di Eulero-Mascheroni e la costante di Copeland-Erdos. La prima é data da:

$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} \ - \ ln(n+1) \right) = 0,57721566490153286\ldots$$

si dimostra che essa é anche uguale a:

$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} \ - \ ln(n) \right)$$

Essa ha importanza in vari rami della matematica ed in particolare nella teoria della funzione gamma di Euler (Γ), della funzione digamma (ψ_0), o della costante di Catalan (G), cioé:

$$\begin{aligned} \gamma &= -\Gamma'(1)\ ; \\ \gamma &= -\psi_0(1)\ ; \\ G &= \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^2} = 1 - \frac{1}{3^2} + \frac{1}{5^2} - \frac{1}{7^2} + \ldots = 0,91596\ldots \end{aligned}$$

Per la costante di Eulero-Mascheroni e per quella di Catalan si congettura che siano trascendenti ma fino ad oggi non si sa neppure dimostrarne l'irrazionalitá.

La costante di Copeland-Erdos consiste nel seguente numero decimale:

$$0,23571113171923\ldots$$

ottenuto giustapponendo i primi 2, 3, 5, 7, 11, 13, ...
Copeland e Erdos mostrarono che esso é un numero normale in base 10 (ovvero in esso ogni cifra decimale compare con probabilitá di 1/10.)]

11.1 Costante di Lévy

Consideriamo un numero reale e il suo sviluppo in frazioni continue. Sia $\frac{p_n}{q_n}$ una sua convergente.
Si dimostra che per quasi ogni reale, q_n non puó aumentare esponenzialmente all'aumentare di n.
Cioé $q_n < e^{\alpha n}$ per $n \to +\infty$ ove $\alpha > 0$.
Lévy verificó che per i denominatori delle convergenti nello sviluppo in frazioni continue di quasi tutti i reali (escluso un insieme di misura nulla) si ha:

$$\lim_{n\to\infty} q_n^{\frac{1}{n}} = \lim_{n\to\infty} \left(\frac{p_n}{x}\right)^{\frac{1}{n}} = L$$

ove x é il reale di cui $\frac{p_n}{q_n}$ é convergente, e L é detta costante di Lévy. In particolare

$$L = e^{\frac{\pi^2}{12ln\ 2}} = 3,2758229187\ldots$$

A volte viene indicata come costante di Lévy solo l'esponente

$$\frac{\pi^2}{12ln\ 2} = 1,1865691101\ldots$$

Nella figura 4 mostriamo l'andamento di $q_n^{\frac{1}{n}}$ per i primi 500 termini nello sviluppo in frazioni continue di π, $sin\ 1$, γ, C, e come le curve si avvicinano alla costante di Lévy per $n \to +\infty$.

11.2 Costante di Khinchin

Il matematico russo Khinchin ha elaborato il terzo importante risultato sui termini delle espansioni in frazioni continue di quasi ogni reale (escluso un insieme di misura nulla).
Mentre la media aritmetica degli a_i non ha valore finito, la media geometrica é finita. Inoltre tale valore é uguale per quasi tutti i reali.
Khinchin ha mostrato che:

$$\lim_{n\to\infty}(a_0 a_1 \dots a_n)^{\frac{1}{n}} = K$$

ove gli a_i sono i valori che possono assumere i termini della frazione continua e K é la costante di Khinchin.
Tale costante é data da:

$$K = \prod_{n=1}^{+\infty}\left(1+\frac{1}{n(n+2)}\right)^{\frac{ln\ n}{ln\ 2}} = 2,68545\dots$$

Questo valore basso corrisponde al predominio dei valori piccoli, come si é giá visto nella distribuzione di probabilitá di Gauss.

Se sviluppo in frazioni continue la stessa costante di Khinchin, risulta che i suoi termini hanno una media geometrica che si avvicina a K stesso. Si é a conscenza che K é trascendente peró non si sa ancora se K é irrazionale.
Notiamo che e é un numero reale che non appartiene alla classe di "quasi tutti" i reali nel senso di Gauss, ma per il quale la media geometrica dei termini si avvicina a K.

La figura 5 mostra come per $n \to +\infty$ la media geometrica dei termini tenda a K per i numeri: π, $sin\ 1$, γ e C.
Il secondo grafico (figura 6) mostra che vi sono alcuni reali tipo e, $\sqrt{2}$, $\sqrt{3}$, la sezione aurea , per i quali:

$$\lim_{n\to\infty}(a_0 a_1 \dots a_n)^{\frac{1}{n}} \neq K$$

Riferimenti bibliografici

[1] H. Davenport, *Aritmetica superiore*, Zanichelli Editore S.p.A. , Bologna (sesta edizione 1994).

[2] C.D. Olds, *Continued fractions*, Random House and The L. W. Singer Company , (second Printing 1963).

[3] G.H. Hardy and E.M. Wright, *An Intoduction to the Theory of Numbers*, Oxford at the Clerendon Press , (fifth edition 1979)

[4] H. Pollard, *The Theory of Algebraic Numbers*, The Methematical Association of America , (1950).

[5] P. Ribenboim, *Algebraic Numbers*, John Wiley & Sons, Inc. , (1972).

[6] E. Weiss, *Algebraic Number Theory*, McGraw-Hill Book Company, Inc. , (1963).

[7] C. Brezinski, *History of Continued Fractions and Padé Approximants*, Springer-Verlag Berlin Heidelberg (1991).

[8] C. Viola, *Bollettino U.M.I. (Approsimazione Diofantea, frazioni continue e misura d'irrazionalitá)*, Serie VIII, Vol. VII-A, Agosto 2004, 291-320.

[9] J.D. Borrow, *Chaos in Numberland: The secret life of continued fractions*, Millennium Mathematics Project, University of Cambridge (June 2000).

[10] W.A. Beyer and M.S. Waterman, *Ergodic Computation with Continued Fractions and Jacobi's Algorithm*, Numer. Math. 19, 195-205 by Springer-Verlag (1972).

[11] L.J. Mordell, *Diophantine Equations*, Academic Press Inc. (London) Ltd., (1969)