Bollettino
Unione Matematica Italiana

Sezione A – La Matematica nella Società e nella Cultura

Carlo Viola

Approssimazione diofantea, frazioni continue e misure d'irrazionalità

Bollettino dell'Unione Matematica Italiana, Serie 8, Vol. **7-A**—*La Matematica nella Società e nella Cultura* (2004), n.2, p. 291–320.

Unione Mastematica Italiana

<http://www.bdim.eu/item?id=BUMI_2004_8_7A_2_291_0>

Bollettino dell'Unione Matematica Italiana, Unione Mastematica Italiana, 2004.

Bollettino U. M. I.
La Matematica nella Società e nella Cultura

Approssimazione diofantea, frazioni continue e misure d'irrazionalità (*).

Carlo Viola

1. Si dice *equazione diofantea*, dal nome del matematico greco Diofanto di Alessandria (III secolo d.C.), un'equazione algebrica a coefficienti interi, generalmente in più incognite, di cui si cercano soluzioni intere o razionali. Per esempio, la celebre equazione di Fermat $x^n + y^n = z^n$, dove l'esponente n è un intero positivo assegnato e dove le incognite x, y, z sono interi non nulli, è un'equazione diofantea, recentemente dimostrata irrisolubile per ogni esponente $n \geqslant 3$ (è questo il cosiddetto «ultimo teorema di Fermat», dimostrato da Wiles nel 1995). L'*approssimazione diofantea* è invece lo studio dell'approssimabilità di numeri irrazionali mediante i razionali (o, più in generale, dell'approssimabilità di numeri non appartenenti ad un corpo $\mathbb{K}$ mediante numeri appartenenti a $\mathbb{K}$), e l'uso dell'aggettivo «diofantea» per questo tipo di approssimazione è giustificato dalle applicazioni che si possono dare dell'approssimazione diofantea di numeri irrazionali *algebrici* alla risolubilità di opportune equazioni diofantee; ad una di queste applicazioni, riguardante l'e-

(*) *A causa di un increscioso errore tipografico il presente lavoro è stato pubblicato nel fascicolo Serie VIII, Vol. VII-A, Agosto 2004, 291-320, omettendo alcune righe a partire dalla riga 14 di pag. 295. Qui è pubblicato il testo corretto, emendato di tale errore.* (NdR) quazione di Thue, daremo un cenno nell'ultimo paragrafo ([1]). Conviene osservare che l'approssimazione diofantea degli irrazionali algebrici è una teoria molto studiata nel corso del XX secolo, soprattutto perché motivata dalle ricerche sulla risolubilità di equazioni diofantee, e nell'ambito della quale sono stati elaborati metodi di tipo algebrico e algebro-geometrico abbastanza generali, e sono stati ottenuti risultati che, per certi aspetti, possono considerarsi ottimali. Al contrario, l'approssimazione diofantea dei numeri trascendenti (o congetturalmente tali) è una teoria largamente frammentaria, per la quale non esistono a tutt'oggi metodi generali di indagine.

In questo articolo esporremo alcuni argomenti fondamentali in approssimazione diofantea «classica», cioè nell'approssimazione di numeri appartenenti a $\mathbb{R}\setminus\mathbb{Q}$ mediante numeri in $\mathbb{Q}$, per lo più limitandoci a trattare sommariamente aspetti introduttivi alla teoria, nell'ambito dei quali non è necessario distinguere se gli irrazionali che si vogliono approssimare siano algebrici o trascendenti. Daremo qualche dimostrazione di risultati semplici e significativi.

2. Introduciamo anzitutto alcune notazioni abituali in approssimazione diofantea. Per un $\alpha \in \mathbb{R}$ indichiamo con $[\alpha]$ la parte intera di α, cioè il massimo intero che non supera α, con $\{\alpha\}$ la sua parte frazionaria:

$$\{\alpha\} = \alpha - [\alpha],$$

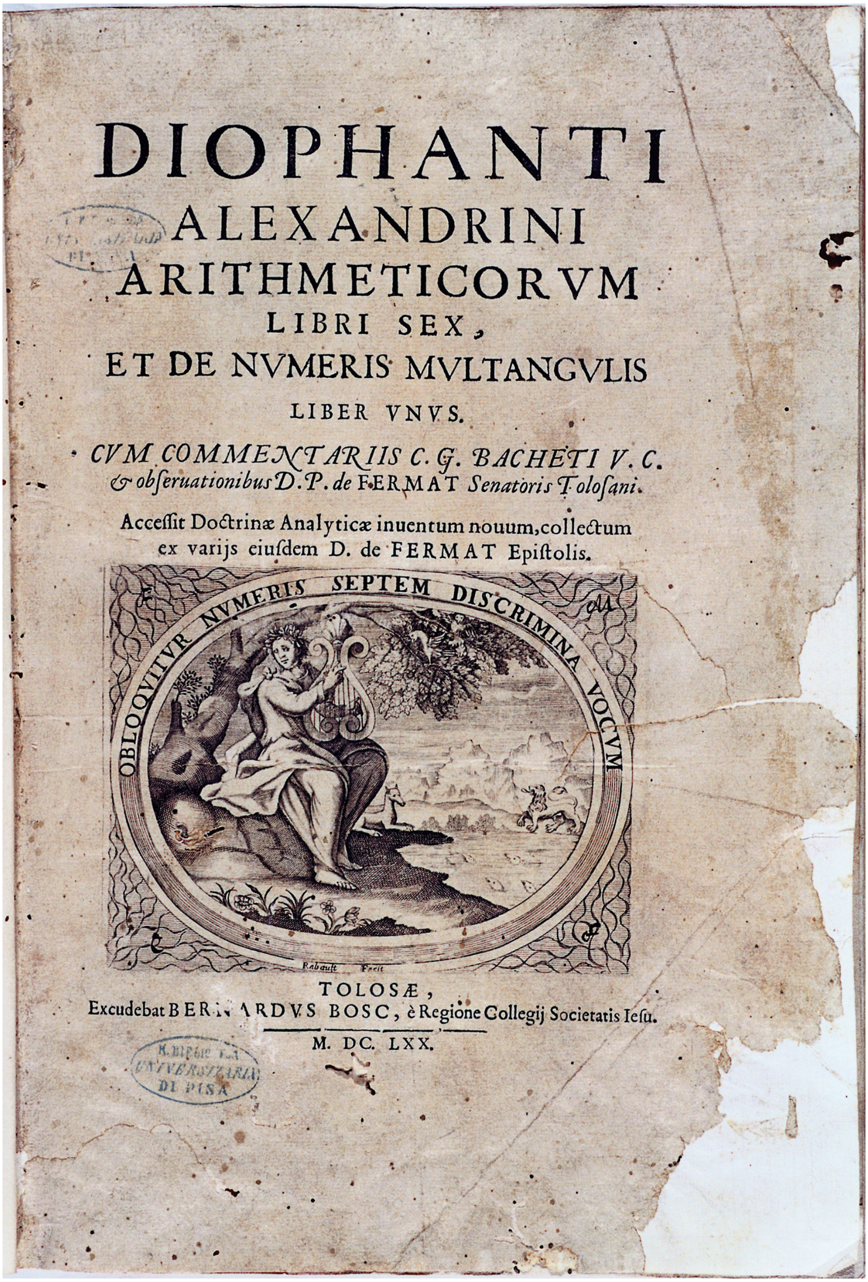
e con $\|\alpha\|$ la sua distanza dall'intero più vicino:

$$\|\alpha\| = \min\{\{\alpha\},\ 1 - \{\alpha\}\} = \min_{n \in \mathbb{Z}} |\alpha - n|\,.$$

Ad esempio, si ha

$$\begin{array}{lll} [1,7] = 1, & \{1,7\} = 0,7, & \|1,7\| = 0,3; \\ [-1,2] = -2, & \{-1,2\} = 0,8, & \|-1,2\| = 0,2. \end{array}$$

([1]) Ricordiamo che un numero reale o complesso α si dice algebrico se è radice di un polinomio $P(x)$ non identicamente nullo a coefficienti razionali (e quindi anche – moltiplicando l'equazione $P(\alpha) = 0$ per il minimo comune multiplo dei denominatori dei coefficienti di $P(x)$ – radice di un polinomio a coefficienti interi). Il grado di un numero algebrico α è il minimo grado dei polinomi $P(x)$ a coefficienti razionali tali che $P(\alpha) = 0$; in particolare, i numeri razionali sono i numeri algebrici di grado 1. I numeri che non sono algebrici si dicono trascendenti.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obseruationibus D. P. de FERMAT Senatoris Tolosani.
Accessit Doctrinæ Analyticæ inuentum nouum, collectum
ex varijs eiusdem D. de FERMAT Epistolis.

TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Iesu.
M. DC. LXX.

Tav. 1. – L'*Arithmetica* di Diofanto con le osservazioni di P. de Fermat (Tolosa, 1670). Su concessione del Ministero per i Beni e Attività Culturali, per cortesia della Biblioteca Universitaria di Pisa.

Dato un numero reale α, in approssimazione diofantea interessa la ricerca di numeri razionali r/s (con r e s interi primi fra loro, $s > 0$) che rendano piccola la distanza $|\alpha - r/s|$ pur avendo numeratore e denominatore non troppo grandi. In altre parole, r/s è una «buona» approssimazione ad α quando $|\alpha - r/s|$ è più piccolo di quanto *a priori* ci si aspetti dall'ordine di grandezza del denominatore s, e dunque quando il prodotto $s|\alpha - r/s| = |s\alpha - r|$ è relativamente piccolo. Chiaramente per ogni s assegnato la distanza $\left|\alpha - \frac{r}{s}\right| = \frac{1}{s}|s\alpha - r|$ è minima, al variare di r, quando r è l'intero più vicino a $s\alpha$. In tal caso

$$\left|\alpha - \frac{r}{s}\right| = \frac{1}{s}\|s\alpha\| \leqslant \frac{1}{2s}\,; \tag{1}$$

ma tale stima non si potrà migliorare in modo significativo, a meno che la distanza di $s\alpha$ dall'intero più vicino non sia eccezionalmente piccola. Se questo avviene, detto r l'intero più vicino a $s\alpha$, il numero razionale r/s è una «buona» approssimazione ad α.

Storicamente, il primo esempio di buona approssimazione nel senso indicato sopra è attribuito ad Archimede, che nella sua opera *Misura del cerchio* trovò che il rapporto fra la lunghezza di una circonferenza e quella del suo diametro è approssimativamente uguale a 22/7. Si ha infatti $\pi = 3{,}14159\ldots$ e $22/7 = 3{,}14285\ldots$, e quindi $\left|\pi - \frac{22}{7}\right| < 0{,}0013$, che è una quantità ben più piccola di $\frac{1}{2\times 7} = \frac{1}{14}$.

3. Possiamo precisare meglio l'idea sopra accennata osservando che per un numero irrazionale α interessa trovare *infiniti* razionali r/s che migliorino qualitativamente la diseguaglianza banale (1). Cioè interessano successioni (r_n/s_n) $(n = 1, 2, \ldots)$ di razionali che migliorino la stima asintotica ([2])

$$\left|\alpha - \frac{r_n}{s_n}\right| = O\left(\frac{1}{s_n}\right) \qquad (n \to \infty)$$

([2]) Ricordiamo la definizione dei simboli asintotici $O(\ldots)$ e $o(\ldots)$. Date due successioni (u_n) e (v_n) con $v_n > 0$, la notazione $u_n = O(v_n)$ indica che il quoziente u_n/v_n si mantiene limitato per $n \to \infty$, cioè che esiste una costante $c > 0$, indipendente da n, tale che $|u_n| \leqslant cv_n$ per ogni n. La notazione $u_n = o(v_n)$ indica che $u_n/v_n \to 0$ per $n \to \infty$.

ottenuta dalla (1) (intendendo ovviamente che r_n sia l'intero più vicino a $s_n\alpha$), ossia che verifichino almeno la stima

$$\left|\alpha - \frac{r_n}{s_n}\right| = o\left(\frac{1}{s_n}\right) \qquad (n \to \infty)\,. \tag{2}$$

La (2) è equivalente a

$$\lim_{n\to\infty} |s_n\alpha - r_n| = \lim_{n\to\infty} \|s_n\alpha\| = 0\,. \tag{3}$$

Per comprendere l'utilità di disporre di successioni (r_n/s_n) di questo tipo, osserviamo che la condizione (3) fornisce facilmente un criterio assai generale per decidere se un'assegnata costante $\alpha \in \mathbb{R}$, definita mediante un opportuno algoritmo (per es. come somma di una serie numerica, o come valore di un integrale definito, ecc.), sia razionale o irrazionale. Più precisamente, se, dato un $\alpha \in \mathbb{R}$, esistono due successioni di interi (r_n) e (s_n) tali che

$$0 \neq s_n\alpha - r_n \to 0 \qquad (n \to \infty)\,, \tag{4}$$

allora $\alpha \notin \mathbb{Q}$. Infatti se fosse $\alpha = M/N$ con $M, N \in \mathbb{Z}$, $N > 0$, per l'ipotesi $s_n\alpha - r_n \neq 0$ si avrebbe, per $n = 1, 2, \ldots$,

$$|s_n\alpha - r_n| = \frac{|s_nM - r_nN|}{N} > 0\,,$$

da cui $|s_nM - r_nN| \geqslant 1$ perché r_n, s_n, M, N sono interi, e quindi anche $s_nM - r_nN$ lo è. Dunque

$$|s_n\alpha - r_n| \geqslant \frac{1}{N}\,,$$

contro l'ipotesi $s_n\alpha - r_n \to 0$.

Diamo una semplice applicazione del precedente criterio dimostrando l'irrazionalità del numero $e = 2{,}71828\ldots$ (base dei logaritmi naturali), sfruttando la convergenza, sufficientemente rapida dal punto di vista diofanteo, della serie esponenziale. Essendo

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}\,, \tag{5}$$

definiamo, per $n = 1, 2, \ldots$,

$$\frac{r_n}{s_n} = \sum_{k=0}^{n-1} \frac{1}{k!}\,.$$

Poiché $(n-1)!$ è multiplo di $k!$ per ogni k tale che $0 \leqslant k \leqslant n-1$, abbiamo $s_n \leqslant (n-1)!$. Allora

$$e - \frac{r_n}{s_n} = \sum_{k=n}^{\infty} \frac{1}{k!} > 0\,,$$

e, moltiplicando per $s_n \leqslant (n-1)!$,

$$\begin{aligned} 0 < s_n e - r_n &\leqslant (n-1)!\left(\frac{1}{n!} + \frac{1}{(n+1)!} + \frac{1}{(n+2)!} + \dots\right) \\ &= \frac{1}{n}\left(1 + \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \dots\right) \\ &< \frac{1}{n}\left(1 + \frac{1}{n+1} + \frac{1}{(n+1)^2} + \dots\right) \\ &= \frac{1}{n} \cdot \frac{1}{1 - \frac{1}{n+1}} = \frac{n+1}{n^2} \to 0 \qquad (n \to \infty). \end{aligned}$$

Dunque la condizione (4) è soddisfatta, e quindi $e \notin \mathbb{Q}$.

Se avessimo utilizzato la formula

$$e = \lim_{n \to \infty}\left(1 + \frac{1}{n}\right)^n$$

anziché la serie (5), non avremmo potuto dimostrare altrettanto facilmente l'irrazionalità di e, poiché la successione $e - \dfrac{(n+1)^n}{n^n}$ tende a zero, ma non così rapidamente da compensare la crescita del denominatore n^n. È interessante osservare che vi sono costanti «classiche» α per le quali non si conosce un algoritmo di convergenza abbastanza rapido in senso diofanteo, cioè non si sa dimostrare l'esistenza di successioni (r_n) e (s_n) di interi soddisfacenti la (4); di tali costanti α, in effetti, non si sa dimostrare l'irrazionalità. È questo il caso, per esempio, della costante di Euler–Mascheroni (Tav. 3):

$$\gamma = \lim_{n \to \infty}\left(\sum_{k=1}^{n} \frac{1}{k} - \log n\right) = 0{,}57721\ldots,$$

che ha importanza in vari rami della matematica e in particolare nel-

ADNOTATIONES

AD

CALCULUM INTEGRALEM

EULERI

In quibus nonnulla Problemata ab EULERO *proposita resolvuntur*

AUCTORE

LAURENTIO MASCHERONIO

IN R. ARCHIGYMNASIO TICINENSI MATHEM. PROF.

ACAD. PATAVINAE AC R. MANTUANAE SOCIO.

TICINI.

EX TYPOGRAPHIA PETRI GALEATII

PRAESID. REI LITTER. PERMITT.

ANNO MDCCXC.

Tav. 2. – L. Mascheroni, *Adnotationes ad Calculum Integralem Euleri* (Pavia, 1790). (Collezione privata).

la teoria della funzione gamma di Euler, o della costante di Catalan:

$$G = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^2} = 1 - \frac{1}{3^2} + \frac{1}{5^2} - \frac{1}{7^2} + \ldots = 0{,}91596\ldots.$$

Si congettura che queste costanti siano trascendenti, ma, fino ad oggi, non se ne sa dimostrare neppure l'irrazionalità.

4. Per ogni α irrazionale si può dimostrare in modo del tutto elementare l'esistenza di successioni (p_n) e (q_n) di interi, con $0 < q_1 < q_2 < \ldots$, soddisfacenti una diseguaglianza fondamentale in approssimazione diofantea, e precisamente

$$(6) \qquad \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2} \qquad (n = 1, 2, \ldots);$$

la costruzione di tali successioni (p_n) e (q_n), come vedremo al paragrafo 5, è strettamente collegata allo sviluppo di α in frazione continua.

Il risultato (6) si può dimostrare in modo semplice ed elegante facendo ricorso al cosiddetto «principio dei cassetti» (in inglese: «box principle» o «pigeonhole principle»), che si può enunciare nel modo seguente: se si collocano, in un modo qualsiasi, $Q+1$ oggetti in Q cassetti, dovrà esserci almeno un cassetto contenente almeno due oggetti (infatti se ogni cassetto contenesse o nessuno o un solo oggetto, il numero totale degli oggetti sarebbe minore o uguale al numero dei cassetti). Questo semplice principio viene anche detto principio di Dirichlet, perché se ne attribuiscono a Dirichlet le prime applicazioni matematiche.

Come applicazione del principio dei cassetti, dimostriamo il seguente

LEMMA. – Siano $\alpha, Q \in \mathbb{R}$ con $Q > 1$. Esiste un intero q tale che $0 < q < Q$ e $\|q\alpha\| \leqslant 1/Q$.

DIMOSTRAZIONE. – Supponiamo anzitutto Q intero, e suddividia-

$$\int \frac{e^x\,dx}{x} = A - 1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{4} - \ldots - \frac{1}{n} + l - x.$$

Sed ex demonſtratione Euleri in Calc. Differ. Part. Poſt. C. VI. eſt

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots + \frac{1}{n} = ln + \frac{1}{2n} - \frac{\mathfrak{A}}{2n^2} + \frac{\mathfrak{B}}{4n^4} - \frac{\mathfrak{C}}{6n^6} + \frac{\mathfrak{D}}{8n^8} - \ldots$$
$$+ \frac{1}{2} + \frac{\mathfrak{A}}{2} - \frac{\mathfrak{B}}{4} + \frac{\mathfrak{C}}{6} - \frac{\mathfrak{D}}{8} + \ldots$$

ubi $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, $\mathfrak{D}$, &c. ſunt numeri Bernoulliani. In caſu autem $n = \infty$ eſt

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots + \frac{1}{n} = ln + \frac{1}{2} + \frac{\mathfrak{A}}{2} - \frac{\mathfrak{B}}{4} + \frac{\mathfrak{C}}{6} - \frac{\mathfrak{D}}{8} + \ldots$$

Erit ergo

$$\int \frac{e^x\,dx}{x} = A - ln - \frac{1}{n} - \frac{\mathfrak{A}}{2} + \frac{\mathfrak{B}}{4} - \frac{\mathfrak{C}}{6} + \frac{\mathfrak{D}}{8} - \ldots + l - x$$

ſeu ob $ln = l - x$; $\int \frac{e^x\,dx}{x} = A - \frac{1}{2} - \frac{\mathfrak{A}}{2} + \frac{\mathfrak{B}}{4} - \frac{\mathfrak{C}}{6} + \frac{\mathfrak{D}}{8} - \&c.$

Quod integrale cum in caſu ipſo $x = -n = -\infty$ debeat annihilari; erit tandem $A = \frac{1}{2} + \frac{\mathfrak{A}}{2} - \frac{\mathfrak{B}}{4} + \frac{\mathfrak{C}}{6} - \frac{\mathfrak{D}}{8} + \&c. \ldots =$ 0, 577215 664901 5235, ut Eulerus invenit loco citato. Eadem Euleri methodo actu collectis centum terminis ſeriei $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5}$ &c. invenimus eſſe

A = 0, 577215 664901 532860 618112 090082 39.

Cum vero ſit $M = e(A-L) + 1$ erit $M = 1 - 1.2 + 1.2.3 - \&c.$ = 0, 403652 637676 805925 7....

Cum valor $l - lz$ ſit realis a valore $z = 0$ uſque ad valorem $z = 1 - \omega$, ubi ω eſt quantitas infiniteſima; erit etiam intra hos limites

$$\int \frac{dz}{lz} = A + l - lz + lz + \frac{(lz)^2}{2.2} + \frac{(lz)^3}{2.3.3} + \frac{(lz)^4}{2.3.4.4} + \&c. \ldots$$

ubi nihil intercedet imaginarium.

B 2 Hinc

Tav. 3. – Costante di Euler-Mascheroni (L. Mascheroni, *Adnotationes ad Calculum...*, 1790, p. 11). Il calcolo della costante effettuato da Mascheroni è esatto fino alla 19ma cifra decimale dopo la virgola: 0, 577215 664901 532860 6 .... Le cifre successive indicate da Mascheroni sono errate. (Collezione privata).

mo l'intervallo chiuso $[0, 1]$ nell'unione disgiunta dei Q sottointervalli:

$$[0,1]=\left[0,\frac{1}{Q}\right)\cup\left[\frac{1}{Q},\frac{2}{Q}\right)\cup\ldots\cup\left[\frac{Q-2}{Q},\frac{Q-1}{Q}\right)\cup\left[\frac{Q-1}{Q},1\right],$$

che prendiamo, tutti tranne l'ultimo, chiusi a sinistra e aperti a destra. I $Q+1$ numeri

$$0,\{\alpha\},\{2\alpha\},\ldots,\{(Q-1)\alpha\},1$$

appartengono all'intervallo $[0, 1]$; dunque, per il principio dei cassetti, almeno due di essi devono appartenere ad uno stesso dei Q sottointervalli, e quindi devono avere distanza fra loro non superiore a $1/Q$. Ne segue che esistono interi p', p'', q', q'' tali che $0 \leqslant q'' < q' < Q$ e

$$|(q'\alpha - p') - (q''\alpha - p'')| \leqslant \frac{1}{Q},$$

dove $p' = [q'\alpha]$, $p'' = [q''\alpha]$ se $q'' > 0$, e $p'' = 0$ oppure $p'' = -1$ se $q'' = 0$. Ponendo $q = q' - q''$ e $p = p' - p''$, si ha $0 < q < Q$ e

$$\|q\alpha\| \leqslant |q\alpha - p| = |(q'\alpha - p') - (q''\alpha - p'')| \leqslant \frac{1}{Q}.$$

Se invece Q non è intero, sia $Q^* = [Q] + 1$. Per la dimostrazione precedente esiste un intero q tale che $0 < q < Q^*$, da cui $q < Q$, e inoltre

$$\|q\alpha\| \leqslant \frac{1}{Q^*} < \frac{1}{Q},$$

e ciò completa la dimostrazione del lemma.

Applichiamo ora il lemma precedente per dimostrare che, per ogni α irrazionale, esistono successioni di interi (p_n) e (q_n), con $0 < q_1 < q_2 < \ldots$, soddisfacenti la (6). Poniamo $q_1 = 1$. Si ha $\|\alpha\| > 0$ perché α non è intero; scegliamo un numero $Q > \|\alpha\|^{-1}$. Per il lemma, esiste un intero $q > 0$ tale che $\|q\alpha\| \leqslant Q^{-1} < \|\alpha\|$, da cui, in particolare, $q > 1$; sia q_2 *il più piccolo* intero > 1 tale che $\|q_2\alpha\| < \|\alpha\|$. Ne segue $1 = q_1 < q_2$, $\|\alpha\| = \|q_1\alpha\| > \|q_2\alpha\|$, $\|q\alpha\| \geqslant \|\alpha\|$ per ogni q tale che

$0 < q < q_2$, e quindi

$$\|q\alpha\| \geqslant \|q_2\alpha\| \quad \text{per } 0 < q \leqslant q_2. \tag{7}$$

Si ha $\|q_2\alpha\| > 0$ perché α è irrazionale; scegliamo un nuovo numero $Q > \|q_2\alpha\|^{-1}$. Per il lemma, esiste un intero $q > 0$ tale che $\|q\alpha\| \leqslant Q^{-1} < \|q_2\alpha\|$, da cui $q > q_2$ per la (7); sia q_3 *il più piccolo* intero $> q_2$ tale che $\|q_3\alpha\| < \|q_2\alpha\|$. Così proseguendo, si costruisce una successione di interi

$$1 = q_1 < q_2 < q_3 < \dots$$

tali che

$$\|\alpha\| = \|q_1\alpha\| > \|q_2\alpha\| > \|q_3\alpha\| > \dots,$$

e tali che i numeri $\|q_n\alpha\|$ $(n = 1, 2, 3, \dots)$ siano i minimi successivi fra tutti i valori $\|q\alpha\|$ al crescere di $q = 1, 2, 3, \dots$; in altre parole, per $n = 1, 2, 3, \dots$ si ha

$$\|q_{n+1}\alpha\| < \|q_n\alpha\| \leqslant \|q\alpha\| \quad \text{per ogni } q \text{ tale che } 0 < q < q_{n+1}. \tag{8}$$

Applicando il lemma con $Q = q_{n+1}$, sappiamo che esiste un intero q tale che $0 < q < q_{n+1}$ e $\|q\alpha\| \leqslant 1/q_{n+1}$. Dalla (8) si ha quindi

$$\|q_n\alpha\| \leqslant \frac{1}{q_{n+1}} < \frac{1}{q_n}. \tag{9}$$

Indicando con p_n l'intero più vicino a $q_n\alpha$, dalla (9) si ottiene, dividendo per q_n,

$$\left|\alpha - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2},$$

e quindi la (6).

Notiamo, per inciso, che dalla (6) si ottiene $|q_n\alpha - p_n| < 1/q_n \to 0$ per $n \to \infty$, con $q_n\alpha - p_n \neq 0$ $(n = 1, 2, \dots)$ perché α è irrazionale per ipotesi. Dunque, in particolare, la (6) implica la validità della (4) con $r_n = p_n$ e $s_n = q_n$, e quindi la condizione (4) non è solo sufficiente per l'irrazionalità di α, come abbiamo dimostrato nel paragrafo precedente, ma è anche necessaria.

5. Dati un numero reale α (non necessariamente irrazionale) e un numero razionale p/q ($p, q \in \mathbb{Z}$, $q > 0$), si dice che p/q è un'*approssimazione ottimale* ad α quando $\|q\alpha\| = |q\alpha - p|$ (con $p = [q\alpha]$ se $\|q\alpha\| = 1/2$) e inoltre $\|q\alpha\| < \|q'\alpha\|$ per ogni intero q' tale che $0 < q' < q$. Se α è irrazionale, le approssimazioni ottimali ad α, per la (8), sono esattamente gli infiniti razionali p_n/q_n ($n = 1, 2, 3, \ldots$) costruiti nel paragrafo precedente, cioè quelli per i quali le quantità $\|q_n\alpha\|$ ($n = 1, 2, 3, \ldots$) sono i minimi successivi fra i valori $\|q\alpha\|$ ($q = 1, 2, 3, \ldots$), e, per ogni n, p_n è l'intero più vicino a $q_n\alpha$. Se α è razionale, la costruzione dei razionali p_n/q_n di cui al paragrafo precedente è ancora possibile, ma dà luogo ad una successione finita il cui ultimo termine è α stesso. In altre parole, un $\alpha \notin \mathbb{Q}$ ha infinite approssimazioni ottimali, mentre un $\alpha \in \mathbb{Q}$ ne ha solo un numero finito.

Come abbiamo accennato, il concetto di approssimazione ottimale ad α è intimamente connesso con lo sviluppo di α in frazione continua. Definendo successivamente

$$
\begin{aligned}
a_0 &= [\alpha], & \alpha_1 &= \frac{1}{\alpha - a_0}; \\
a_1 &= [\alpha_1], & \alpha_2 &= \frac{1}{\alpha_1 - a_1}; \\
a_2 &= [\alpha_2], & \alpha_3 &= \frac{1}{\alpha_2 - a_2}; \\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}
$$

si ottiene $\alpha = a_0 + \dfrac{1}{\alpha_1}$, $\alpha_1 = a_1 + \dfrac{1}{\alpha_2}$, $\alpha_2 = a_2 + \dfrac{1}{\alpha_3}$, $\ldots$, e quindi lo sviluppo di α in *frazione continua semplice*:

$$
\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} \tag{10}
$$

dove i *quozienti parziali* $a_0, a_1, a_2, a_3, \ldots$ sono interi, con $a_1, a_2, a_3, \ldots > 0$ (l'aggettivo «semplice», che generalmente si sottintende, sta a significare che i numeratori in (10) sono tutti 1, e che i quozienti parziali a_n sono interi, con $a_n > 0$ per $n \geqslant 1$). Lo sviluppo in frazione continua (10), per semplicità di scrittura, si suole indicare

$$\alpha = [a_0;\, a_1,\, a_2,\, a_3,\, \ldots]\,. \tag{11}$$

Tale sviluppo contiene infiniti quozienti parziali se e solo se α è irrazionale.

Si dimostra che le frazioni continue ridotte nello sviluppo (11):

$$[a_0;\, a_1,\, a_2,\, \ldots,\, a_{n-1}] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1}}}} \tag{12}$$

($n = 1, 2, 3 \ldots$), dette anche i *convergenti* ad α, sono (ad eccezione del solo a_0 nel caso in cui si abbia $\{\alpha\} > 1/2$, cioè $a_1 = 1$) *tutte e sole* le approssimazioni ottimali ad α. L'importanza dell'algoritmo delle frazioni continue in approssimazione diofantea consiste nella coincidenza delle approssimazioni ottimali ad α con i convergenti (12).

Osserviamo incidentalmente che i primi quozienti parziali nello sviluppo di π in frazione continua sono i seguenti:

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

Dunque i primi convergenti a π (che coincidono *senza eccezioni* con le approssimazioni ottimali a π, poiché $\{\pi\} = 0,14\ldots < 1/2$, e infatti $a_1 = 7 > 1$) sono:

$$3,\ \frac{22}{7},\ \frac{333}{106},\ \frac{355}{113},\ \frac{103993}{33102},\ \frac{104348}{33215},\ \frac{208341}{66317},\ \ldots,$$

e il convergente p_2/q_2 è l'approssimazione 22/7 data da Archimede.

Non possiamo trattare esaurientemente qui la teoria aritmetica delle frazioni continue e le sue applicazioni in approssimazione diofantea; il lettore interessato ad approfondire questi argomenti può consultare i capitoli I e II di [2] e i capitoli X e XI di [5]. Qui osserviamo che il fondatore della teoria aritmetica delle frazioni continue è Lagrange, che in alcune memorie pubblicate fra il 1768 e il 1773 espone sistematicamente i principi fondamentali di questa teoria con varie applicazioni; in particolare, la dimostrazione – indipendente dal principio dei cassetti e ben anteriore a quella di Dirichlet – della diseguaglianza (6) per i convergenti ad un numero α (1769), il suo celebre teorema sulla periodicità dello sviluppo in frazione continua degli irrazionali quadratici (1770), e le applicazioni della teoria delle frazioni continue alla risoluzione delle equazioni diofantee di secondo grado in due incognite (1770) (per maggiori dettagli sull'opera di Lagrange in teoria dei numeri si veda [4]).

Enunciamo, senza dimostrazione, alcuni fra i principali risultati nella teoria elementare delle frazioni continue.

- Lo sviluppo in frazione continua (11) è periodico, cioè tale che esistano due interi $m \geqslant 0$ e $k \geqslant 1$ per i quali si abbia

$$a_n = a_{n+k} \quad \text{per ogni } n \geqslant m\,,$$

se e solo se α è un irrazionale quadratico (cioè algebrico di grado 2), ovvero radice di un'equazione $A\alpha^2 + B\alpha + C = 0$ con A, B, C interi, e $B^2 - 4AC > 0$ e non quadrato (Lagrange, 1770).

- Per ogni coppia $\dfrac{p_n}{q_n}, \dfrac{p_{n+1}}{q_{n+1}}$ di convergenti consecutivi ad α, uno almeno soddisfa la diseguaglianza

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}\,. \tag{13}$$

Inversamente, se un numero razionale p/q soddisfa la (13), allora p/q è un convergente ad α.

- Per ogni terna $\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}$ di convergenti consecutivi ad α, uno almeno soddisfa la diseguaglianza

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}\,; \tag{14}$$

in particolare, per ogni α irrazionale esistono infiniti razionali p/q soddisfacenti la (14). Inoltre questo risultato non è migliorabile, poiché esistono opportuni irrazionali β tali che per ogni costante $c > \sqrt{5}$ la diseguaglianza $|\beta - p/q| < 1/(cq^2)$ abbia al più un numero finito di soluzioni razionali p/q. I numeri β di questo tipo sono tutti e soli quegli irrazionali quadratici nel cui sviluppo in frazione continua $\beta = [a_0; a_1, a_2, \ldots]$ si ha $a_n = 1$ per ogni n abbastanza grande (Hurwitz, 1891).

- I numeri irrazionali $\alpha = [a_0;\, a_1,\, a_2,\, \ldots]$ per i quali la successione dei quozienti parziali è superiormente limitata, cioè tale che $a_n < H$ per ogni n e per un'opportuna costante $H > 0$ dipendente da α, sono tutti e soli quelli per cui la diseguaglianza (6) è, a meno di costanti moltiplicative, la migliore possibile, cioè quelli per cui

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{Kq^2} \tag{15}$$

per ogni razionale p/q e per un'opportuna costante $K > 0$ dipendente da α. In particolare, la (15) vale per ogni irrazionale quadratico α, in virtù del teorema di Lagrange citato sopra.

6. Dato un irrazionale α, è naturale domandarsi – tenuto conto delle diseguaglianze (6) e (15) – per quali esponenti λ la diseguaglianza

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^\lambda} \tag{16}$$

abbia infinite soluzioni razionali p/q. La risposta a questa domanda non è univoca ma dipende dall'irrazionale α che si considera, e suggerisce una possibile classificazione dei numeri irrazionali. Precisamente si dà la seguente

DEFINIZIONE. – Dato un irrazionale α, si dice che μ è una *misura d'irrazionalità* di α se per ogni $\varepsilon > 0$ esiste una costante $C = C(\alpha,\, \varepsilon) > 0$ tale che

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{Cq^{\mu+\varepsilon}}$$

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

La più piccola misura d'irrazionalità di α, cioè il minimo esponente μ per cui vale la condizione precedente, si indica con $\mu(\alpha)$.

In altre parole, $\mu(\alpha)$ è l'estremo inferiore degli esponenti λ tali che la diseguaglianza (16) valga al più per un numero finito di razionali p/q, e quindi è anche l'estremo superiore degli esponenti λ tali che la (16) valga per infiniti p/q.

Per la (6) si ha $\mu(\alpha) \geqslant 2$ per ogni α irrazionale, e la (15) implica che esistono irrazionali α tali che $\mu(\alpha) = 2$. Inoltre, data una funzione $f(q)$ tendente a $+\infty$ (per $q \to +\infty$) con crescita arbitrariamente rapida, è facile fornire esempi di irrazionali α, definiti mediante opportune frazioni continue, tali che $|\alpha - p_n/q_n| < 1/f(q_n)$ ($n = 1, 2, \ldots$), dove (p_n/q_n) è la successione dei convergenti ad α. In particolare, se $f(q)$ tende a $+\infty$ più rapidamente di q^{λ} per ogni λ (per esempio, se $f(q) = e^{q}$), la (16) vale per infiniti p/q qualunque sia l'esponente λ, e quindi $\mu(\alpha) = +\infty$ (un irrazionale α tale che $\mu(\alpha) = +\infty$ si dice un *numero di Liouville*). Utilizzando l'algoritmo delle frazioni continue, dato un qualunque numero reale $\mu \geqslant 2$ si possono anche costruire facilmente esempi di irrazionali α tali che $\mu(\alpha) = \mu$.

Esistono dunque (infiniti) irrazionali α tali che $\mu(\alpha)$ sia uguale ad un qualunque numero reale prefissato nell'intervallo $[2, +\infty]$. È naturale porsi la seguente domanda: se si assegna un irrazionale α «a caso», cioè senza imporre nella definizione stessa del numero α proprietà diofantee particolari, qual è il valore più probabile per $\mu(\alpha)$? La risposta a questa domanda è data dalla seguente

PROPOSIZIONE. – Quasi tutti gli irrazionali α sono tali che $\mu(\alpha) = 2$. In altre parole, l'insieme degli irrazionali α per i quali $\mu(\alpha) > 2$ ha misura nulla.

Questo risultato è un facile corollario del seguente

TEOREMA. – Sia $\varphi(q) > 0$ una funzione definita per $q = 1, 2, 3, \ldots$. Se la serie $\sum_{q=1}^{\infty} 1/\varphi(q)$ converge, l'insieme E_φ degli irrazionali α, tali che la diseguaglianza $|\alpha - p/q| < (q\varphi(q))^{-1}$ abbia infinite soluzioni razionali p/q, ha misura nulla.

DIMOSTRAZIONE. – Poiché l'insieme E_φ è chiaramente invariante per una traslazione intera, e poiché un'unione numerabile di insiemi di misura nulla ha misura nulla, è sufficiente dimostrare che $E_\varphi \cap [0, 1]$ ha misura nulla. Dato un $\varepsilon > 0$ piccolo a piacere, fissiamo un intero N tale che $\sum_{q=N}^{\infty} 1/\varphi(q) < \varepsilon/2$. Ad ogni $\alpha \in E_\varphi \cap [0, 1]$ associamo un numero razionale p/q tale che $q \geqslant N$, $q\varphi(q) > \|\alpha\|^{-1}$ e $|\alpha - p/q| < (q\varphi(q))^{-1}$, cosa evidentemente possibile poiché quest'ultima diseguaglianza ha infinite soluzioni razionali; queste condizioni implicano $|\alpha - p/q| < \|\alpha\|$, e quindi $0 < p/q < 1$. Indichiamo con $\psi : E_\varphi \cap [0, 1] \to \mathbb{Q}$ l'applicazione così ottenuta, cioè poniamo $\psi(\alpha) = p/q$. Dato un qualunque intero $q \geqslant N$, possiamo allora considerare tutte le coppie (p, α) tali che $\psi(\alpha) = p/q$; poiché $0 < p/q < 1$, i valori possibili di p non superano q, e per ogni p tutte le controimmagini α di p/q stanno nell'intervallo di estremi $\dfrac{p}{q} - \dfrac{1}{q\varphi(q)}$, $\dfrac{p}{q} + \dfrac{1}{q\varphi(q)}$, che ha lunghezza $\dfrac{2}{q\varphi(q)}$. Dunque per ogni $q \geqslant N$ tutti gli α tali che $\psi(\alpha) = p/q$ per qualche p sono contenuti in un'unione di intervalli di misura complessiva $\leqslant q \cdot \dfrac{2}{q\varphi(q)} = \dfrac{2}{\varphi(q)}$. Ne segue che $E_\varphi \cap [0, 1]$ è contenuto in un insieme di misura $\leqslant \sum_{q=N}^{\infty} 2/\varphi(q) < \varepsilon$, e perciò ha misura nulla.

Per dimostrare la Proposizione, per ogni $\delta > 0$ indichiamo con F_δ l'insieme degli irrazionali α tali che la diseguaglianza $|\alpha - p/q| < 1/q^{2+\delta}$ abbia infinite soluzioni razionali p/q. Poiché la serie $\sum_{q=1}^{\infty} 1/q^{1+\delta}$ converge, per il teorema precedente F_δ ha misura nulla. Se $\delta_1, \delta_2, \ldots$ è una qualunque successione di numeri positivi tendente a zero, l'insieme degli irrazionali α tali che $\mu(\alpha) > 2$ è evidentemente contenuto nell'unione numerabile $\bigcup_{n=1}^{\infty} F_{\delta_n}$, e quindi ha misura nulla.

7. Sono molto pochi i numeri irrazionali non quadratici, definibili con algoritmi diversi dalle frazioni continue, dei quali si conosca esplicitamente lo sviluppo in frazione continua: intendendo con ciò la conoscenza della successione dei quozienti parziali nella sua totalità, ovvero la possibilità di determinare per ogni n il quoziente parziale a_n in modo non ricorsivo, cioè senza dover precedentemente calcolare $a_0, a_1, \ldots, a_{n-1}$.

Fra questi pochi irrazionali vi è il numero e, che è trascendente (Hermite, 1873) e di cui abbiamo dimostrato l'irrazionalità nel paragrafo 3, e anche le sue radici di tutti gli ordini: $\sqrt{e}, \sqrt[3]{e}, \ldots$, nonché alcune altre costanti collegate a valori della funzione esponenziale in opportuni punti razionali. In particolare valgono gli sviluppi in frazione continua (Euler, 1737):

$$e = [2;\, 1,\, 2,\, 1,\, 1,\, 4,\, 1,\, 1,\, 6,\, 1,\, \dots,\, 1,\, 2n,\, 1,\, \dots],$$

e, per ogni intero $s \geqslant 2$,

$$e^{1/s} = [1; s-1, 1, 1, 3s-1, 1, 1, 5s-1, 1, \dots, 1, (2n+1)\,s-1, 1, \dots]$$

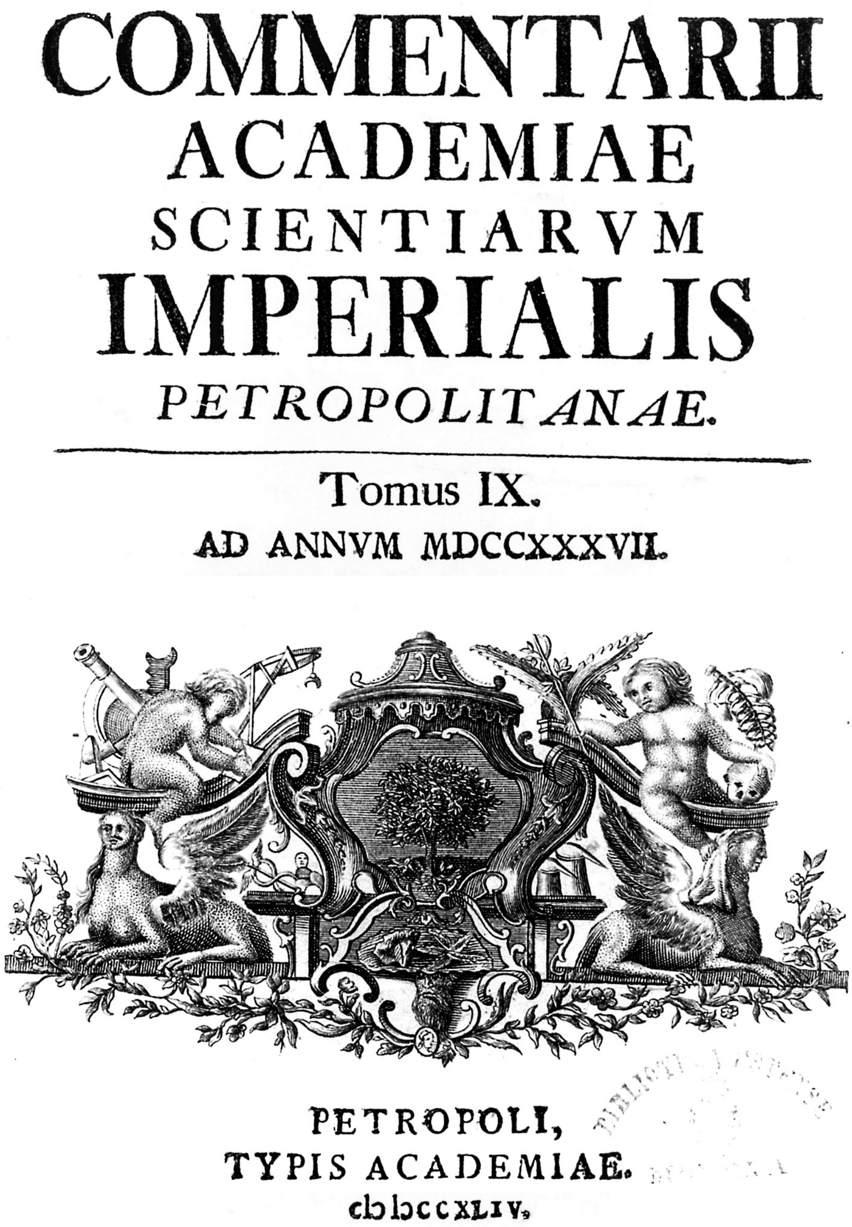
([3], pp. 120 e 132; 203 e 211. Vedi Tavv. 5 e 6). Da questi sviluppi in frazione continua si può facilmente dedurre che $\mu(e) = \mu(\sqrt{e}) = \mu(\sqrt[3]{e}) = \dots = 2$.

Tuttavia il caso dei numeri $e^{1/s}$ $(s = 1, 2, \dots)$ è eccezionale. Ad esempio, sono stati calcolati numericamente i primi 17 milioni di quozienti parziali nello sviluppo di π in frazione continua (vedi [1], p. 626) senza trovare alcun tipo di regolarità, così che la distribuzione dei quozienti parziali di π appare di tipo casuale, con una percentuale di quozienti parziali uguali ad 1 corrispondente a ciò che ci si aspetta statisticamente nello sviluppo in frazione continua di un irrazionale α generico, soddisfacente $\mu(\alpha) = 2$. In una situazione di questo tipo, che è la regola piuttosto che l'eccezione per costanti definite da algoritmi diversi dalle frazioni continue, la teoria delle frazioni continue non ha alcuna utilità per dimostrare l'irrazionalità delle costanti considerate o per calcolarne misure d'irrazionalità.

È noto che π è un numero trascendente (Lindemann, 1882). Volendo limitarsi a dimostrarne l'irrazionalità, risulta (sorprendentemente) più semplice dimostrare l'irrazionalità di π^2 (il che ovviamente implica l'irrazionalità di π), piuttosto che, direttamente, l'irrazionalità di π stesso. Questo risultato si ottiene applicando il criterio (4), cioè determinando una successione di razionali (r_n/s_n) convergente a π^2 abbastanza rapidamente in senso diofanteo.

Per quanto riguarda le misure d'irrazionalità di π^2 e di π, tenendo conto della Proposizione del paragrafo 6 e dei dati sperimentali sopra accennati riguardanti lo sviluppo in frazione continua di π, si congettura che $\mu(\pi^2) = \mu(\pi) = 2$, ma questi risultati sembrano fuori dalla portata dei metodi noti finora. I migliori risultati dimostrati fino ad oggi sono

$$\mu(\pi^2) < 5,44124\dots$$



COMMENTARII
ACADEMIAE
SCIENTIARVM
IMPERIALIS
PETROPOLITANAE.

Tomus IX.
AD ANNVM MDCCXXXVII.

PETROPOLI,
TYPIS ACADEMIAE.
CIϽ IϽCCXLIV.

Tav. 4. – Il volume IX dei *Commentarii* dell'Accademia delle Scienze di Pietroburgo. Su concessione del Ministero per i Beni e Attività Culturali, per cortesia della Biblioteca Estense Universitaria di Modena.

([7]), e

$$\mu(\pi) < 8,01604\ldots$$

([6]). Queste misure d'irrazionalità si ottengono con metodi assai sofisticati sui quali non possiamo qui dilungarci. Con tali metodi si costruisce un'opportuna successione di razionali (r_n/s_n) convergente abbastanza rapidamente in senso diofanteo alla costante α che si considera (nel caso specifico, a π^2 oppure a π), e per determinare una buona misura d'irrazionalità di α si applica una versione quantitativa del criterio (4) rappresentata ad esempio dal seguente teorema, o da sue opportune varianti ([3]).

TEOREMA. – Sia $\alpha \in \mathbb{R}$, e sia (S_n) una successione di numeri reali positivi tale che

$$\lim_{n \to \infty} S_n = +\infty \tag{17}$$

e, per ogni $\varepsilon > 0$,

$$S_{n+1} \ll_\varepsilon S_n^{1+\varepsilon}. \tag{18}$$

Inoltre, siano (r_n) e (s_n) due successioni di interi tali che $0 < s_n \leqslant S_n$ e

$$S_n^{-\varrho-\varepsilon} \ll_\varepsilon |s_n \alpha - r_n| \ll_\varepsilon S_n^{-\varrho+\varepsilon}, \tag{19}$$

per un'opportuna costante $\varrho = \varrho(\alpha) > 0$ e per ogni $\varepsilon > 0$. Allora $\alpha \notin \mathbb{Q}$, e si ha

$$\mu(\alpha) \leqslant 1 + \frac{1}{\varrho}. \tag{20}$$

DIMOSTRAZIONE. – La doppia diseguaglianza (19) con $0 < \varepsilon < \varrho$, insieme alla (17), implica ovviamente la (4), e quindi $\alpha \notin \mathbb{Q}$. Per ottenere la stima (20) dobbiamo dimostrare che, data una qualunque co-

([3]) Le notazioni $\ll$ e $\gg$ che usiamo nel teorema, abituali in teoria dei numeri, indicano diseguaglianze fra successioni di numeri positivi contenenti costanti moltiplicative imprecisate. Ad esempio, $u_n \ll v_n$ significa che esiste una costante $c > 0$, indipendente da n, tale che $u_n \leqslant c v_n$ per ogni n, e quindi che $u_n = O(v_n)$. La notazione $\ll_\varepsilon$ indica che la costante c può dipendere da un parametro ε.

vnde ſequitur

$$(bc+1)v^2+(bcd+b+d-c-2abc-2a)x-abcd+a^2bc-ab$$
$$-ad+aa-cd+ac-1=0.$$

Atque hoc modo omnes huiusmodi fractiones continuas, quarum denominatores vel omnes vel alterni vel terni vel quaterni etc. ſunt inter ſe aequales, ſummare licet. Semper autem ſumma ſeu valor x eſt radix ex aequatione quadrata.

§. 21. Antequam ad alias fractiones continuas, in quibus denominatores progreſſiones arithmeticas conſtituunt, ſummandas progrediamur; quantitates quasdam tranſcendentes euoluamus, quae in fractiones continuas conuerſae dent denominatores in progreſſione arithmetica progredientes, quo ex his via euadat planior eiusmodi fractiones continuas ſummandi. Hoc igitur logarithmis aliisque expreſſionibus transcendentibus tentans deprehendi in eiusmodi fractiones continuas deduci, ſi numerus cuius logarithmus hyperbolicus eſt vnitas, eiusque poteſtates quaeque conſiderentur. Poſito igitur hoc numero $=e$, erit $e=$ 2, 718281828459O4, qua expreſſione in fractionem continuam conuerſa erit

$$e=2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1\text{ etc.}}}}}}}}}}$$

cuius

Tav. 5. – Sviluppo in frazione continua di e (L. Euler, *De fractionibus continuis dissertatio*, Pietroburgo, 1737 (1744), p. 120). Su concessione del Ministero per i Beni e Attività Culturali, per cortesia della Biblioteca Estense Universitaria di Modena.

stante $\sigma > 1/\varrho$, la diseguaglianza

$$|q\alpha - p| < q^{-\sigma} \tag{21}$$

è soddisfatta al più da un numero finito di razionali p/q. Supponiamo che ciò sia falso. Allora esiste una successione *infinita* $\mathcal{Q}$ di interi positivi tali che per ogni $q \in \mathcal{Q}$ valga la (21), essendo p l'intero più vicino a $q\alpha$. Per la (19), siano $c_1(\varepsilon)$, $c_2(\varepsilon) > 0$ tali che

$$c_1(\varepsilon)\, S_n^{-\varrho-\varepsilon} \leqslant |s_n\alpha - r_n| \leqslant c_2(\varepsilon)\, S_n^{-\varrho+\varepsilon}, \tag{22}$$

e, in virtù della (17), per ogni $q \in \mathcal{Q}$ sia $n = n(q)$ *il più piccolo* indice soddisfacente

$$2c_2(\varepsilon)q < S_n^{\varrho-\varepsilon} \tag{23}$$

con un opportuno ε tale che $0 < \varepsilon < \varrho$, dipendente solo da ϱ e da σ, che sarà scelto in seguito. Si ha allora, per le (21), (22) e (23),

$$\begin{gathered}|s_n p - r_n q| = |q(s_n\alpha - r_n) - s_n(q\alpha - p)| \leqslant \\ q|s_n\alpha - r_n| + s_n|q\alpha - p| \leqslant qc_2(\varepsilon)\, S_n^{-\varrho+\varepsilon} + S_n q^{-\sigma} < \frac{1}{2} + S_n q^{-\sigma}.\end{gathered} \tag{24}$$

Inoltre abbiamo, per la (18) e perché n è il più piccolo indice tale che valga la (23),

$$q \geqslant \frac{S_{n-1}^{\varrho-\varepsilon}}{2c_2(\varepsilon)} \gg_\varepsilon S_n^{\frac{\varrho-\varepsilon}{1+\varepsilon}}, \tag{25}$$

da cui

$$S_n q^{-\sigma} \ll_\varepsilon S_n^{1-\frac{\varrho-\varepsilon}{1+\varepsilon}\sigma}. \tag{26}$$

Scegliamo $\varepsilon > 0$ così piccolo che $1 - \dfrac{\varrho-\varepsilon}{1+\varepsilon}\sigma < 0$, il che è possibile per continuità, poiché abbiamo scelto σ in modo che

$$\varrho\sigma > 1\,. \tag{27}$$

Per la (26) abbiamo allora $S_n q^{-\sigma} < 1/2$ per $q \in \mathcal{Q}$ abbastanza grande, e dalla (24) otteniamo $|s_n p - r_n q| < 1$. D'altra parte, per le (21),

132 *DE FRACTIONIBVS CONTINVIS.*

Atque ex priore inuenta aequatione erit

$$\frac{e^{\frac{1}{s}}+1}{e^{\frac{1}{s}}-1} = 2s+\cfrac{1}{6s+\cfrac{1}{10s+\cfrac{1}{14s+\cfrac{1}{18s+\text{etc.}}}}}$$

Si denominatores huius interpolentur binis vnitatibus habebitur

$$\frac{e^{\frac{1}{s}}+1}{e^{\frac{1}{s}}-1} = 2s-1+\cfrac{2}{1+\cfrac{1}{1+\cfrac{1}{3s-1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{5s-1+\cfrac{1}{1\ \text{etc.}}}}}}}}$$

Ex qua oritur ſequens fractio continua

$$e^{\frac{1}{s}} = 1+\cfrac{1}{s-1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{3s-1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{5s-1+\cfrac{1}{1\ \text{etc.}}}}}}}}}$$

Tav. 6. – Sviluppi in frazione continua di $e^{1/s}$ e di $(e^{1/s}+1)/(e^{1/s}-1)$ (L. Euler, *De fractionibus continuis*..., 1737 (1744), p. 132). Su concessione del Ministero per i Beni e Attività Culturali, per cortesia della Biblioteca Estense Universitaria di Modena.

(22), (25) e (26) si ha

$$(28)\qquad |s_n p - r_n q| = |q(s_n\alpha - r_n) - s_n(q\alpha - p)| \geqslant$$

$$q|s_n\alpha - r_n| - s_n|q\alpha - p| \geqslant qc_1(\varepsilon)S_n^{-\varrho-\varepsilon} - S_n q^{-\sigma} \gg_\varepsilon$$

$$S_n^{\frac{\varrho-\varepsilon}{1+\varepsilon}-\varrho-\varepsilon} - c_3(\varepsilon)\, S_n^{1-\frac{\varrho-\varepsilon}{1+\varepsilon}\sigma}$$

per ogni $q \in \mathcal{Q}$, per $n = n(q)$ come sopra, e per un'opportuna costante $c_3(\varepsilon) > 0$. Scegliamo $\varepsilon > 0$ così piccolo che $1 - \dfrac{\varrho-\varepsilon}{1+\varepsilon}\sigma < \dfrac{\varrho-\varepsilon}{1+\varepsilon} - \varrho - \varepsilon$, il che è possibile per continuità, in virtù della (27). Otteniamo allora, per la (17), $S_n^{\frac{\varrho-\varepsilon}{1+\varepsilon}-\varrho-\varepsilon} > c_3(\varepsilon)\, S_n^{1-\frac{\varrho-\varepsilon}{1+\varepsilon}\sigma}$ per $q \in \mathcal{Q}$ abbastanza grande, e quindi $|s_n p - r_n q| > 0$ per la (28).

Si conclude che $0 < |s_n p - r_n q| < 1$ per ogni $q \in \mathcal{Q}$ abbastanza grande e per $n = n(q)$, e questo è assurdo perché $|s_n p - r_n q|$ è intero.

Il teorema precedente, e la relativa dimostrazione, meritano qualche commento. Si noti anzitutto che la (19) (insieme alle altre ipotesi del teorema) non può valere per una costante $\varrho > 1$, poiché in tal caso dalla (20) si otterrebbe la conclusione falsa $\mu(\alpha) < 2$. La situazione ideale si avrebbe se la (19) valesse per $\varrho = 1$, poiché allora la (20) darebbe $\mu(\alpha) = 2$, secondo quanto si congettura per qualunque costante α assegnata «a caso» (nel senso specificato al paragrafo 6). Nei casi particolari che si sanno trattare, si riesce a determinare successioni (r_n), (s_n) e (S_n) soddisfacenti le ipotesi del teorema per opportune costanti ϱ, con $0 < \varrho < 1$, più piccole di quanto si vorrebbe (più vicine a 0 che a 1).

Osserviamo inoltre che, supposto di aver già dimostrato che $\alpha \notin \mathbb{Q}$, per arrivare alla conclusione $\mu(\alpha) = 2$ che si congettura nei casi concreti si sarebbe tentati di scegliere $r_n = p_n$ e $s_n = S_n = q_n$ dove (p_n/q_n) è la successione dei convergenti ad α, poiché la (6) garantisce la validità della *maggiorazione* (19) con $\varrho = 1$. Di fatto però questa scelta è impraticabile, poiché generalmente non si dispone di informazioni sui convergenti ad α che garantiscano che la successione (q_n) abbia una crescita controllata come richiesto dalla (18), cioè tale che $q_{n+1} \ll_\varepsilon q_n^{1+\varepsilon}$, o che valga la *minorazione* $|q_n\alpha - p_n| \gg_\varepsilon q_n^{-1-\varepsilon}$ espressa dalla (19) per $\varrho = 1$.

La maggiorazione (19), insieme alla diseguaglianza $s_n \leqslant S_n$, fornisce in particolare $|\alpha - r_n/s_n| \ll_\varepsilon 1/s_n^{1+\varrho-\varepsilon}$. Dunque la successione (r_n/s_n) data dalle ipotesi del teorema, pur approssimando α meno bene in senso diofanteo della successione dei convergenti ad α (perché $1+\varrho-\varepsilon < 2$), soddisfa un'opportuna versione quantitativa della stima asintotica (2), e cioè una condizione del tipo (16) con un qualunque esponente $\lambda < 1+\varrho$. Il teorema precedente fornisce quindi una specie di «principio di specularità» per gli esponenti: se si riesce a determinare, in modo assai esplicito e cioè con le condizioni restrittive indicate dalle ipotesi del teorema, una successione (r_n/s_n) di approssimazioni razionali ad α «abbastanza» buona (cioè soddisfacente la (16) con un qualunque esponente $< 1+\varrho$), allora, per la (20), non può esistere una successione (p_n/q_n) di approssimazioni razionali ad α «straordinariamente» buona (cioè soddisfacente la (16) con un esponente $> 1 + 1/\varrho$).

Osserviamo infine che la struttura della dimostrazione del teorema precedente, in particolare nel confronto fra la (24) e la (28), fornisce un esempio interessante dell'incompatibilità fra due entità qualitativamente dello stesso tipo ma con caratteristiche quantitative differenti (le successioni (r_n/s_n) e (p_n/q_n) accennate qui sopra), secondo un principio generale che trova varie applicazioni in approssimazione diofantea.

8. Concludiamo questo articolo con qualche cenno sull'approssimazione diofantea degli irrazionali algebrici. Il primo risultato ottenuto per numeri algebrici di grado qualsiasi è il seguente

TEOREMA (Liouville, 1851). – Per ogni numero algebrico α di grado $n \geqslant 2$ esiste una costante $K = K(\alpha) > 0$, dipendente da α ed esplicitamente calcolabile, tale che

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{Kq^n}$$

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

DIMOSTRAZIONE. – Se $\alpha \notin \mathbb{R}$ il teorema è banale perché, indicando con $\operatorname{Im}\alpha$ la parte immaginaria di α, si ha $|\alpha - p/q| \geqslant |\operatorname{Im}\alpha| \geqslant |\operatorname{Im}\alpha|/q^n$. Se $\alpha \in \mathbb{R}$, sia $P(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ il *polinomio minimo* di α, cioè il polinomio di grado minimo n a coefficienti interi primi fra loro, con $a_0 > 0$, tale che $P(\alpha) = 0$. Per il teorema del valor medio si ha, per ogni razionale p/q tale che $|\alpha - p/q| < 1$,

$$\left| P\left(\frac{p}{q}\right) \right| = \left| P(\alpha) - P\left(\frac{p}{q}\right) \right| = \left| \alpha - \frac{p}{q} \right| |P'(\xi)|, \tag{29}$$

per un opportuno ξ compreso fra α e p/q, e quindi soddisfacente $\alpha - 1 < \xi < \alpha + 1$. Posto $M = \max\limits_{\alpha - 1 \leqslant x \leqslant \alpha + 1} |P'(x)|$, dalla (29) si ha $|P(p/q)| \leqslant M|\alpha - p/q|$, con $M > 0$ perché $P(x)$ non è costante. Dunque

$$\left| \alpha - \frac{p}{q} \right| \geqslant \frac{1}{M} \left| P\left(\frac{p}{q}\right) \right|. \tag{30}$$

Ma $P(p/q) \neq 0$, perché altrimenti il polinomio $P(x)$ sarebbe divisibile per $qx - p$ e quindi α, essendo radice del polinomio $P(x)/(qx - p)$, sarebbe un numero algebrico di grado $\leqslant n - 1$ (in altre parole, $P(x)$ non sarebbe il polinomio minimo di α). Ne segue

$$\left| P\left(\frac{p}{q}\right) \right| = \frac{1}{q^n} |a_0 p^n + a_1 p^{n-1} q + \ldots + a_{n-1} p q^{n-1} + a_n q^n| \geqslant \frac{1}{q^n},$$

perché $a_0 p^n + a_1 p^{n-1} q + \ldots + a_n q^n$ è un intero non nullo e quindi ha valore assoluto $\geqslant 1$. Dalla (30) si ottiene allora $|\alpha - p/q| \geqslant 1/(Mq^n)$.

Se invece p/q è tale che $|\alpha - p/q| \geqslant 1$, si ha a più forte ragione $|\alpha - p/q| \geqslant 1/q^n$. Il teorema segue scegliendo $K > \max\{M, 1\}$.

Si noti che nel caso $n = 2$ il teorema di Liouville fornisce una dimostrazione della diseguaglianza (15) per ogni irrazionale quadratico α, indipendente dalla teoria delle frazioni continue. Inoltre è interessante osservare che nella dimostrazione del teorema di Liouville, così come per il teorema del paragrafo 7 e per la sua versione qualitativa (4), si utilizza in modo essenziale il principio che un intero > 0 è necessariamente $\geqslant 1$, ovvero che l'insieme $\mathbb{Z}$, a differenza di $\mathbb{Q}$, è «ben spaziato» in $\mathbb{R}$.

Il teorema di Liouville, in particolare, implica che se α è un numero algebrico di grado $n \geqslant 2$, allora $\mu(\alpha) \leqslant n$. Come immediata conseguenza, Liouville dimostrò per primo l'esistenza di numeri trascendenti, dando esempi di numeri α tali che $\mu(\alpha) = +\infty$, cioè di numeri di Liouville (cfr.paragrafo 6). La dimostrazione moderna dell'esistenza di numeri trascendenti si basa sul fatto che l'insieme dei numeri algebrici è numerabile, poiché ad ogni polinomio $a_0 x^n + \ldots + a_n$ a coefficienti interi di grado n si può far corrispondere il punto $(a_0, \ldots, a_n)$ in $\mathbb{Z}^{n+1}$, che è evidentemente un insieme numerabile; e l'unione numerabile $\mathbb{Z}^2 \cup \mathbb{Z}^3 \cup \ldots$ è a sua volta un insieme numerabile. Poiché $\mathbb{R}$ (o $\mathbb{C}$) non è numerabile, quasi tutti i numeri reali (o complessi) sono trascendenti. Tuttavia argomenti di questo tipo basati sulla cardinalità degli insiemi (Cantor, 1873) non erano noti all'epoca di Liouville, e perciò fino alla metà del XIX secolo l'esistenza di numeri trascendenti non era dimostrata. Inoltre il metodo di Liouville ha il vantaggio di essere costruttivo poiché, utilizzando algoritmi come ad esempio le frazioni continue, fornisce esplicitamente esempi di numeri α con $\mu(\alpha) = +\infty$ e quindi trascendenti, anche se di tipo eccezionale ([4]).

DEFINIZIONE. – Si dice *equazione di Thue* l'equazione diofantea

$$a_0 x^n + a_1 x^{n-1} y + \ldots + a_{n-1} x y^{n-1} + a_n y^n = m \tag{31}$$

con $n \geqslant 3$ e con coefficienti $a_0, a_1, \ldots, a_{n-1}, a_n, m$ interi $(m \neq 0)$, dove le incognite x, y sono interi, e dove il polinomio

$$P(t) = a_0 t^n + a_1 t^{n-1} + \ldots + a_{n-1} t + a_n \qquad (a_0 \neq 0) \tag{32}$$

è irriducibile in $\mathbb{Q}[t]$ ([5]).

Nel 1909 Thue fece la seguente osservazione riguardo alle conseguenze che un eventuale miglioramento del teorema di Liouville

([4]) I numeri di Liouville sono numeri trascendenti «eccezionali» perché formano un insieme di misura nulla, in virtù della Proposizione al paragrafo 6.

([5]) Ricordiamo che se $P(t)$ è un polinomio di grado n a coefficienti razionali irriducibile in $\mathbb{Q}[t]$, cioè non esprimibile come prodotto di due polinomi a coefficienti razionali di gradi $< n$, le sue n radici in $\mathbb{C}$ sono distinte e sono numeri algebrici di grado esattamente n. Infatti se α è una radice di $P(t)$ di grado k $(0 < k \leqslant n)$ avente polinomio minimo $S(t)$, dividendo $P(t)$ per $S(t)$ si ottiene $P(t) = S(t)Q(t) + R(t)$ con $\deg R < \deg S = k$ e $R(\alpha) = P(\alpha) - S(\alpha)Q(\alpha) = 0$. Se il resto $R(t)$ non fosse identicamente nullo, α sarebbe un numero algebrico di grado $\leqslant \deg R < k$. Dunque $R(t)$ è nullo, e poiché $P(t) = S(t)Q(t)$ è irriducibile si ha $n - k = \deg Q = 0$, $k = n$. Inoltre, il fatto che le radici di $P(t)$ abbiano grado esattamente n implica che sono distinte, perché se α fosse una radice almeno doppia di $P(t)$ sarebbe radice anche di $P'(t)$ e quindi avrebbe grado $\leqslant n - 1$.

comporta sulla risolubilità dell'equazione (31). Supponiamo che, per $n \geqslant 3$, si possa determinare un esponente $\nu = \nu(n) < n$ con la seguente proprietà: per ogni numero algebrico α di grado n esiste una costante $C = C(\alpha) > 0$ tale che

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{Cq^{\nu}} \tag{33}$$

per ogni p e q interi con $q > 0$. Allora l'equazione (31) ha al più un numero finito di soluzioni $(x, y) \in \mathbb{Z}^2$; inoltre, se la costante $C = C(\alpha)$ è esplicitamente calcolabile, anche le soluzioni $(x, y) \in \mathbb{Z}^2$ della (31) lo sono ([6]). Infatti, dette $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ le radici del polinomio (32), l'equazione (31) fornisce

$$|a_0| \left| \alpha_1 - \frac{x}{y} \right| \ldots \left| \alpha_n - \frac{x}{y} \right| = \left| \frac{m}{y^n} \right|, \tag{34}$$

con $\alpha_h \neq \alpha_k$ per $h \neq k$ perché $P(t)$ è irriducibile in $\mathbb{Q}[t]$. Posto $\gamma = \frac{1}{2} \min_{h \neq k} |\alpha_h - \alpha_k|$, si ha $\gamma > 0$; sia $\Delta_i \subset \mathbb{C}$ $(i = 1, \ldots, n)$ il disco aperto di centro α_i e raggio γ. Chiaramente $\Delta_1, \ldots, \Delta_n$ sono disgiunti. Le soluzioni (x, y) della (34) tali che $x/y \notin \Delta_1 \cup \ldots \cup \Delta_n$ soddisfano $|m/y^n| > |a_0| \gamma^n$, da cui $|y| < \gamma^{-1} |m/a_0|^{1/n}$. Quelle tali che $x/y \in \Delta_1$ soddisfano $|\alpha_i - x/y| > \gamma$ $(i = 2, \ldots, n)$ e quindi, per la (34), $|\alpha_1 - x/y| < L/|y|^n$, dove $L = |m|/(|a_0| \gamma^{n-1})$. Ma per la (33) si ha $|\alpha_1 - x/y| > 1/(C(\alpha_1) |y|^{\nu})$; dunque $1/(C(\alpha_1)|y|^{\nu}) < L/|y|^n$, da cui $|y| < (C(\alpha_1) L)^{1/(n-\nu)}$. Analogamente se $x/y \in \Delta_2, \ldots, x/y \in \Delta_n$. Si conclude che ogni soluzione $(x, y) \in \mathbb{Z}^2$ della (31) soddisfa

$$|y| < \max\left\{\gamma^{-1} |m/a_0|^{1/n}, (C(\alpha_1)L)^{1/(n-\nu)}, \ldots, (C(\alpha_n)L)^{1/(n-\nu)}\right\}, \tag{35}$$

e quindi le possibilità per y, e analogamente per x, sono in numero finito. Inoltre, se $C(\alpha_1), \ldots, C(\alpha_n)$ sono calcolabili esplicitamente, anche il confine superiore per $|y|$ dato dalla (35) lo è, e

([6]) Osserviamo per inciso che l'esistenza di al più un numero finito di soluzioni dell'equazione (31) dipende in modo essenziale dall'ipotesi $n \geqslant 3$, poiché, ad esempio, l'*equazione di Pell* $x^2 - ay^2 = 1$, dove a è un intero positivo non quadrato, ha infinite soluzioni $(x, y) \in \mathbb{Z}^2$ (Lagrange, 1768).

quindi la determinazione di tutte le soluzioni $(x, y) \in \mathbb{Z}^2$ della (31) è ricondotta ad un numero finito di verifiche entro confini espliciti per $|x|$ e $|y|$.

Thue dimostrò la (33) per ogni numero algebrico α di grado $n \geqslant 2$ e per ogni esponente reale $\nu > \frac{n}{2} + 1$ (si noti che $\frac{n}{2} + 1 < n$ se e solo se $n > 2$), ma con una costante $C = C(\alpha, \nu)$ non calcolabile (nel senso che il metodo di Thue è esistenziale ma non costruttivo; cioè dimostra l'esistenza della costante C, ma non fornisce un procedimento che permetta di calcolarla). Dopo successivi miglioramenti all'esponente di Thue, dovuti a Siegel, a Dyson e a Gel'fond, nel 1955 Roth dimostrò la (33) per ogni esponente reale $\nu > 2$. Precisamente, il teorema di Roth afferma che per ogni irrazionale algebrico α di grado qualsiasi e per ogni $\varepsilon > 0$ esiste una costante $C = C(\alpha, \varepsilon) > 0$ tale che

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{Cq^{2+\varepsilon}} \tag{36}$$

per ogni p e q interi con $q > 0$ (per una dimostrazione del teorema di Roth si veda il capitolo VI di [2]). Anche la costante $C = C(\alpha, \varepsilon)$ che compare nella (36) non è calcolabile.

Per un numero algebrico α di grado 2 i teoremi di Thue e di Roth sono più deboli del teorema di Liouville. Osserviamo inoltre che per nessun numero algebrico α di grado $\geqslant 3$ è noto se l'enunciato del teorema di Roth valga con $\varepsilon = 0$, e cioè se la successione dei quozienti parziali nello sviluppo di α in frazione continua sia superiormente limitata (cfr. la diseguaglianza (15)).

Dal teorema di Roth e dalla (6) segue che per ogni irrazionale algebrico α, senza eccezioni, si ha $\mu(\alpha) = 2$. Dunque dal punto di vista del calcolo delle misure d'irrazionalità il teorema di Roth è ottimale. Il principale difetto dei teoremi di Thue e di Roth è l'*ineffettività*, cioè la non calcolabilità della costante C. Negli ultimi decenni sono stati ottenuti alcuni miglioramenti effettivi al teorema di Liouville nel caso $n \geqslant 3$, ma tali risultati sono assai frammentari e quantitativamente insoddisfacenti; una versione effettiva del teorema di Roth, cioè una dimostrazione della (36) con una costante $C = C(\alpha, \varepsilon)$ calcolabile esplicitamente, sembra irraggiungibile con i metodi finora conosciuti, e rappresenta uno dei problemi più difficili dell'approssimazione diofantea attuale.

Bibliografia

[1] L. Berggren - J. Borwein - P. Borwein, *Pi: a source book*, Springer-Verlag, 1997.

[2] J. W. S. Cassels, *An introduction to diophantine approximation*, Cambridge Tracts in Mathematics no. 45, Cambridge University Press, 1957.

[3] L. Euler, *De fractionibus continuis dissertatio*, Commentarii Acad. Sci. Imper. Petropol. vol. **IX, 1737** (1744), 98-137; *Opera omnia*, ser. I, vol. **XIV**, Teubner, Lipsia e Berlino, 1925, 187-215.

[4] L. Giacardi - C. S. Roero - C. Viola, *Sui contributi di Lagrange alla teoria dei numeri*, Rend. Sem. Mat. Univ. Pol. Torino, **53** (1995), 151-181.

[5] G. H. Hardy - E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1960.

[6] M. Hata, *Rational approximations to π and some other numbers*, Acta Arith., **63** (1993), 335-349.

[7] G. Rhin - C. Viola, *On a permutation group related to $\zeta(2)$*, Acta Arith., **77** (1996), 23-56.

Carlo Viola, Dipartimento di Matematica, Università di Pisa
via Buonarroti 2, 56127 Pisa