Frazioni contine periodiche in teoria elementare dei numeri

Michele Elia - Politecnico of Torino

2^{nd} **Number Theory Meeting**

Torino, 26-27 Ottobre 2017

Premessa

Utilizzando una proprietà di simmetria delle frazioni continue periodiche, Legendre mostrò che è possibile ottenere direttamente (*sans aucun tatônnement*) la rappresentazione dei numeri primi, congruenti a 1 mod 4, come somma di due quadrati

$$p = X^2 + Y^2 \quad ,$$

Osservò inoltre che il metodo fornisce più in generale la rappresentazione, come somma di due quadrati, dei numeri la cui radice quadrata ha uno sviluppo in frazione continua con periodo dispari.

Vi sono diverse dimostrazioni oltre all'originale di Legendre.

Obiettivo

Questo breve intervento intende presentarne una molto simile a quella di Legendre, ma con alcune variazioni che permettono di estendere l'idea base di Legendre ai numeri la cui radice quadrata ha uno sviluppo in frazione continua con periodo pari.

Obiettivo

Questo breve intervento intende presentarne una molto simile a quella di Legendre, ma con alcune variazioni che permettono di estendere l'idea base di Legendre ai numeri la cui radice quadrata ha uno sviluppo in frazione continua con periodo pari.

In particolare, per i numeri prodotto di due primi congruenti a 3 mod 4, si ottiene esplicitamente il fattore minore.

Obiettivo

L'efficacia della procedura, estesa alla fattorizzazione di numeri compositi, pare interessante qualora si introducano opportune varianti al metodo infrastrutturale di **Shanks** assieme alla sua idea dei *giant-baby-steps*.

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

- **Euler - col metodo della discesa infinita di Fermat.**

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

- **Euler - col metodo della discesa infinita di Fermat.**
- **Legendre - usando la frazione continua per $\sqrt{p}$**

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

- **Euler - col metodo della discesa infinita di Fermat.**
- **Legendre - usando la frazione continua per $\sqrt{p}$**
- **Serret - usando la frazione continua finita per $\frac{p}{a}$ con $a^2 = -1 \bmod p$ e $0 < a < \frac{p}{2}$.**

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

- **Euler - col metodo della discesa infinita di Fermat.**
- **Legendre - usando la frazione continua per $\sqrt{p}$**
- **Serret - usando la frazione continua finita per $\frac{p}{a}$ con $a^2 = -1 \bmod p$ e $0 < a < \frac{p}{2}$.**
- **Gauss - con formule chiuse esplicite.**

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

- **Euler - col metodo della discesa infinita di Fermat.**
- **Legendre - usando la frazione continua per $\sqrt{p}$**
- **Serret - usando la frazione continua finita per $\frac{p}{a}$ con $a^2 = -1 \bmod p$ e $0 < a < \frac{p}{2}$.**
- **Gauss - con formule chiuse esplicite.**
- **Gauss - usando forme quadratiche e loro riduzione.**

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

- **Euler - col metodo della discesa infinita di Fermat.**
- **Legendre - usando la frazione continua per $\sqrt{p}$**
- **Serret - usando la frazione continua finita per $\frac{p}{a}$ con $a^2 = -1 \bmod p$ e $0 < a < \frac{p}{2}$.**
- **Gauss - con formule chiuse esplicite.**
- **Gauss - usando forme quadratiche e loro riduzione.**
- **Jacobsthal - con somme che ora portano il suo nome e stabiliscono una connessione con le curve ellittiche sopra i campi finiti.**

Origine: problema di Fermat

$$p = X^2 + Y^2 \quad , \quad p = 1 \bmod 4$$

X e Y si possono calcolare in modi diversi:

- **Euler - col metodo della discesa infinita di Fermat.**
- **Legendre - usando la frazione continua per $\sqrt{p}$**
- **Serret - usando la frazione continua finita per $\frac{p}{a}$ con $a^2 = -1 \bmod p$ e $0 < a < \frac{p}{2}$.**
- **Gauss - con formule chiuse esplicite.**
- **Gauss - usando forme quadratiche e loro riduzione.**
- **Jacobsthal - con somme che ora portano il suo nome e stabiliscono una connessione con le curve ellittiche sopra i campi finiti.**
- **Schoof - con un metodo di complessità polinomiale che utilizza la connessione con le curve ellittiche.**

Frazioni Continue

Frazioni continue regolari ($a_i > 0$, $i > 0$)

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}} \quad , \tag{1}$$

Frazioni continue periodiche sono scritte compattamente come

$$\alpha = \left[\underline{b_0, \ldots, b_k}, \overline{a_1, a_2, \ldots, a_{m-1}, a_m}\right] \quad , \tag{2}$$

dove il periodo è sopralineato, e l'anti-periodo è sottolineato. In particolare, se N è intero positivo si ha

$$\sqrt{N} = \left[a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}\right]$$

dove i primi $m-1$ termini del periodo sono un insieme ordinato palindromo.

Lagrange (1736-1813)

Teorema

Un numero $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ è un irrazionale quadratico se e solo se la sua espansione in frazione continua è periodica.

$$\sqrt{91} = [9, \overline{1, 1, 5, 1, 5, 1, 1, 18}] \quad \text{Periodo} = 8$$

Una frazione continua è detta **puramente periodica** se priva dell'anti-periodo.

$$\frac{9 + \sqrt{91}}{10} = [\overline{1, 1, 5, 1, 5, 1, 1, 18}] \quad \text{Periodo} = 8$$

$$\sqrt{89} = [9, \overline{2, 3, 3, 2, 18}] \quad \text{Periodo} = 5$$

$$\frac{9 + \sqrt{89}}{8} = [\overline{2, 3, 3, 2, 18}] \quad \text{Periodo} = 5$$

Lagrange (1736-1813)

Teorema

Un numero $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ è un irrazionale quadratico se e solo se la sua espansione in frazione continua è periodica.

$$\sqrt{91} = [9, \overline{1, 1, 5, 1, 5, 1, 1, 18}] \quad \text{Periodo} = 8$$

Una frazione continua è detta **puramente periodica** se priva dell'anti-periodo.

$$\frac{9+\sqrt{91}}{10} = [\overline{1, 1, 5, 1, 5, 1, 1, 18}] \quad \text{Periodo} = 8$$

$$\sqrt{89} = [9, \overline{2, 3, 3, 2, 18}] \quad \text{Periodo} = 5$$

$$\frac{9+\sqrt{89}}{8} = [\overline{2, 3, 3, 2, 18}] \quad \text{Periodo} = 5$$

$$\sqrt{941} = [30, \overline{1, 2, 11, 1, 14, 2, 2, 1, 1, 2, 2, 14, 1, 11, 2, 1, 60}] \qquad \tau = 17 \ .$$

Galois (1811-1832)

Un irrazionale quadratico α è detto **ridotto** se $\alpha > 1$ e se per il suo coniugato α' si ha $-1 < \alpha' < 0$. (Steuding p.75-78).

Teorema (Annals de Gergonne,1829)

Lo sviluppo in frazione continua di un numero irrazionale quadratico α è puramente periodico se e solo se α è ridotto. In questo caso, se α' denota il coniugato di α si ha

$$\alpha = \overline{[2a_m, a_1, a_2, \ldots, a_2, a_1]}$$

$$-\frac{1}{\alpha'} = \overline{[a_1, a_2, \ldots, a_2, a_1, 2a_m]} \qquad (3)$$

Legendre (1752-1833)

La soluzione di Legendre dell'equazione [2, p.120-124]

$$p = X^2 + Y^2 \quad \Leftrightarrow \quad p \equiv 1 \bmod 4 \tag{4}$$

$\sqrt{p} = \left[a_0, \overline{a_1, a_2, \ldots, a_m, a_m, \ldots, a_2, a_1, 2a_0}\right]$ Periodo dispari: $2m+1$

$$\alpha = \left[\overline{a_m, a_{m-1}, \ldots, a_1, 2a_0, a_1 \ldots, a_{m-1}, a_m}\right]$$

Teorema

Sia $\frac{P+\sqrt{p}}{Q}$ *il valore irrazionale quadratico di* α *in* $\mathbb{Q}(\sqrt{p})$. *allora*

$$p = P^2 + Q^2 \tag{5}$$

Legendre (cont.)

Proof.

La frazione continua per α è puramente periodica con periodo simmetrico, la conclusione segue dal teorema di Galois che implica $\alpha\alpha' = -1$, essendo

$$\alpha = \frac{Q + \sqrt{p}}{P} \quad .$$

□

Una seconda prova

Sia $\sqrt{p} = [a_0, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}]$, si dice m-convergent (o semplicemente convergente o ridotta) la frazione continua finita ottenuta troncando la frazione continua infinita al termine m-esimo.
Considerata la successione delle convergenti

$$\frac{p_0}{q_0} = \frac{a_0}{1}\ ,\ \frac{p_1}{q_1} = \frac{a_0 a_1 + 1}{a_1}\ ,\ \ldots\ ,\ \frac{p_j}{q_j} = \frac{a_j p_{j-1} + p_{j-2}}{a_j p_{j-1} + p_{j-2}}\ ,\ \ldots$$

si definiscono le successioni $\mathbf{\Delta} = \{\Delta_j\}_{j=1}^{\infty}$ e $\mathbf{\Omega} = \{\Omega_j\}_{j=1}^{\infty}$ come

$$\begin{cases} \Delta_j = p_j^2 - pq_j^2 \\ \Omega_j = p_j p_{j-1} - pq_j q_{j-1} \end{cases} \quad j = 1, 2, \ldots$$

Una seconda prova (cont.)

Teorema

Sia N un intero positivo e sia $\sqrt{N} = [a_0, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}]$.
La successione $\mathbf{\Delta} = \{\Delta_1, \Delta_2, \cdots, \Delta_{\tau-1}, \Delta_\tau, \cdots\}$ è periodica con periodo τ, o 2τ se τ è dispari. La parte costituita dai primi $\tau - 3$ termini ha la simmetria $\Delta_m = (-1)^\tau \Delta_{\tau-m-2}$.
La successione $\mathbf{\Omega} = \{\Omega_1, \Omega_2, \cdots, \Omega_{\tau-1}, \Omega_\tau, \cdots\}$ è periodica con periodo τ, o 2τ se τ è dispari. La parte costituita dai primi $\tau - 3$ termini ha la simmetria $\Omega_m = -(-1)^\tau \Omega_{\tau-1-m}$.
Le forme quadratiche $f_m = [\Delta_m, 2\Omega_{m+1}, \Delta_{m+1}]$ hanno discriminante $4N$.
In ciascun periodo la corrispondenza $m \leftrightarrow f_m$ è biunivoca.

Una seconda prova (cont.)

Sia $m = \frac{\tau-1}{2}$, da cui $\tau - m = \frac{\tau+1}{2}$ e la simmetria in ciascun periodo della successione $\mathbf{\Delta}$ implica $\Delta_{\frac{\tau+1}{2}} = -\Delta_{\frac{\tau-1}{2}}$, quindi il discriminante della forma quadratica $f_{\frac{\tau-1}{2}}$ permette di concludere (dopo aver diviso per 4)

$$p = \Delta^2_{\frac{\tau-1}{2}} + \Omega^2_{\frac{\tau-1}{2}} \tag{6}$$

Una seconda prova (cont.)

Sia $m = \frac{\tau-1}{2}$, da cui $\tau - m = \frac{\tau+1}{2}$ e la simmetria in ciascun periodo della successione $\mathbf{\Delta}$ implica $\Delta_{\frac{\tau+1}{2}} = -\Delta_{\frac{\tau-1}{2}}$, quindi il discriminante della forma quadratica $f_{\frac{\tau-1}{2}}$ permette di concludere (dopo aver diviso per 4)

$$p = \Delta^2_{\frac{\tau-1}{2}} + \Omega^2_{\frac{\tau-1}{2}} \tag{6}$$

Problema: Con quale complessità si possono calcolare $\Delta_{\frac{\tau-1}{2}}$ e $\Omega_{\frac{\tau-1}{2}}$?

Una seconda prova (cont.)

Sia $m = \frac{\tau-1}{2}$, da cui $\tau - m = \frac{\tau+1}{2}$ e la simmetria in ciascun periodo della successione $\mathbf{\Delta}$ implica $\Delta_{\frac{\tau+1}{2}} = -\Delta_{\frac{\tau-1}{2}}$, quindi il discriminante della forma quadratica $f_{\frac{\tau-1}{2}}$ permette di concludere (dopo aver diviso per 4)

$$p = \Delta^2_{\frac{\tau-1}{2}} + \Omega^2_{\frac{\tau-1}{2}} \tag{6}$$

Problema: Con quale complessità si possono calcolare $\Delta_{\frac{\tau-1}{2}}$ e $\Omega_{\frac{\tau-1}{2}}$?

Un bound superiore a questa complessità è fornito dal metodo infrastrutturale di Shanks.

Periodo pari

Teorema

Sia N composito e tale che il periodo τ della frazione continua per $\sqrt{N}$ sia pari, allora

1. *La unit fondamentale $\mathfrak{u}$ in $\mathbb{Q}(\sqrt{N})$ fattorizza $4N$,*
2. *Uno dei fattori di $4N$ si trova nelle posizioni $\frac{\tau-2}{2} + j\tau$, $j = 0, 1, \ldots$ della successione infinita $\mathbf{\Delta}$ prodotta dalla frazione continua di $\sqrt{N}$.*

Dimostrazione (outline)

Sia $\frac{A_j}{B_j}$ un termine della successione delle ridotte, e si definisca il vettore colonna $[A_j, B_j]^T$.
Considerata la matrice involutoria

$$M_{\tau-1} = \begin{bmatrix} -A_{\tau-1} & NB_{\tau-1} \\ -B_{\tau-1} & A_{\tau-1} \end{bmatrix}$$

il cui determinante è $A_{\tau-1}^2 - NB_{\tau-1}^2 = (-1)^\tau = 1$ e la cui traccia è zero. si può provare che vale la relazione

$$\begin{bmatrix} A_{\tau-j-2} \\ B_{\tau-j-2} \end{bmatrix} = (-1)^j M_{\tau-1} \begin{bmatrix} A_j \\ B_j \end{bmatrix} \quad . \tag{7}$$

Se $\tau - j - 2 = j$, i.e. $j = \frac{\tau-2}{2}$, si ha

$$A_{\tau-j-2} = A_j = A \quad \text{e} \quad B_{\tau-j-2} = B_j = B$$

Dimostrazione (cont.)

$[A, B]^T$ risulta essere autovettore della matrice $(-1)^{\frac{\tau-2}{2}} M_{\tau-1}$ di autovalore $(-1)^{\frac{\tau-2}{2}}$, ossia del tipo $\mu[A_{\tau-1} + (-1)^{\frac{\tau-2}{2}}, B_{\tau-1}]$.
Posto $\mu = \frac{1}{d}$, con $d = \gcd\{A_{\tau-1} + (-1)^{\frac{\tau-2}{2}}, B_{\tau-1}\}$ si ha

$$A = \frac{A_{\tau-1} + (-1)^{\frac{\tau-2}{2}}}{d} \quad , \quad B = \frac{B_{\tau-1}}{d}$$

poiché A e B sono relativamente primi e, per questa stessa ragione, dalla catena di uguaglianze

$$\Delta_{\frac{\tau-2}{2}} = A^2 - NB^2 = 2\frac{A_{\tau-1} + (-1)^{\frac{\tau-2}{2}}}{d^2} = 2\frac{A}{d}$$

segue che $2\frac{A}{d}$ **divide** $4N$, ossia $\Delta_{\frac{\tau-2}{2}}$ è divisore di $4N$.

Teorema principale

Teorema

Se N è prodotto di due primi p, q congruenti 3 modulo 4, allora τ è pari e

$$\Delta_{\frac{\tau-2}{2}} = \left(\frac{p}{q}\right) p \quad with \quad p < q \quad .$$

Teorema principale

Teorema

Se N è prodotto di due primi p, q congruenti 3 modulo 4, allora τ è pari e

$$\Delta_{\frac{\tau-2}{2}} = \left(\frac{p}{q}\right) p \quad with \quad p < q \quad .$$

Problema: Con quale complessità si può trovare $\Delta_{\frac{\tau-2}{2}}$?

Forme quadratiche ridotte

Definizione

Una forma quadratica reale $[a, 2b, c]$ *di discriminante* $4N$ *è ridotta se, definito* $\kappa = \min\{|a|, |c|\}$, b *è l'intero (unico a meno del segno) tale che* $\sqrt{N} - |b| < \kappa < \sqrt{N}$.

Definizione (Gauss reduction)

Sia $[a, 2b, c]$ *una forma quadratica primitiva, con* $|a| > |c|$, *si definisce una funzione di riduzione* ρ *come*

$$\rho([a, 2b, c]) = [c, 2(b + c\alpha), a + 2b\alpha + c\alpha^2] \quad ,$$

dove α *è scelto in modo tale che* $a + 2b\alpha + c\alpha^2$ *sia, in valore assoluto minore di* $|c|$.

Shanks: Infrastruttura nelle classi

Sia $[a_0, \overline{a_1, a_2, \ldots, a_{\tau-1}, a_\tau}]$ la frazione continua per $\sqrt{N}$, con N square-free, e il cui periodo sia pari.
$\mathbb{K} = \mathbb{Q}(\sqrt{N})$ con ϵ_0 unit fondamentale (positiva).
Il logaritmo naturale $R_{\mathbb{K}} = \ln \epsilon_0$ di ϵ_0 è detto *regulator* di $\mathbb{K}$.
Si consideri la sequenza infinita $\boldsymbol{\Upsilon}$ di forme quadratiche

$$\mathbf{f}_m(x, y) = \Delta_m X^2 + 2\Omega_m XY + \Delta_{m+1} Y^2 = [\Delta_m, 2\Omega_m, \Delta_{m+1}],\ m = 1, 2, \ldots,$$

con $\Omega_0 = -\Omega_{\tau-1}$ e $\Delta_0 = \frac{\Omega_0^2 - N}{\Delta_1}$.

Tutte le forme quadratiche di $\boldsymbol{\Upsilon}$ sono ridotte e hanno discriminante $4N$.

Infrastruttura

Teorema

La corrispondenza $m \leftrightarrow \mathbf{\Gamma}_m^T$ *con* $1 \leq m \leq \tau$ *è uno-a-uno, ossia tutte le forme quadratiche* $\mathbf{f}_m(x, y)$ *in un periodo sono distinte.*

Tra coppie di elementi di $\mathbf{\Upsilon}$ è possibile definire una operazione, indicata con "$\bullet$", per la quale $\mathbf{\Upsilon}$ è chiuso:

Definizione

Siano $f_m, f_n \in \mathbf{\Upsilon}$*, l'operazione* $f_m \bullet f_n$ *è definita come la composizione di Gauss delle due forme, seguita dalla riduzione alla forma più vicina in* $\mathbf{\Upsilon}$*.*

Infrastruttura

Definizione (Gauss composition)

La composizione di due forme $[a_1, 2b_1, c_1]$ *e* $[a_2, 2b_2, c_2]$ *aventi lo stesso discriminante, scritta*
$[a_3, 2b_3, c_3] = [a_1, 2b_1, c_1] \circ [a_2, 2b_2, c_2]$, *è definita come segue*

$$[d_0 \frac{a_1 a_2}{d^2}, b_2 + \frac{2a_2}{d}(vn - wc_2), \frac{b_3^2 - N}{a_3}] \quad ,$$

dove $n = b_1 - b2$, $d = \gcd\{a_1, a_2, b_1 + b_2\}$, $d_0 = \gcd\{d, c_1, c_2, n\}$, *e* v *e* w, *ottenuti con l'algoritmo di Euclide esteso soddisfano la condizione* $d = ua_1 + va_2 + w(b_1 + b_2)$.

Infrastruttura

Nella successione $\boldsymbol{\Upsilon}$ si introduce una metrica, compatibile con la composizione $\bullet$, definendo la distanza fra due forme quadratiche contigue

$$d(f_m, f_{m+1}) = \frac{1}{2} \left| \ln \frac{\sqrt{N} + \Omega_m}{\sqrt{N} - \Omega_m} \right| \quad .$$

Assumendo $n > m$, la nozione è estesa alla distanza tra due forme f_m e f_n come

$$d(f_m, f_n) = \sum_{j=m}^{n-1} d(f_j, f_{j+1}) \quad .$$

Infrastruttura (cont.)

Definendo $f_{-1} = f_\tau$, si può dimostrare che

$$d(f_{-1}, f_{\tau-1}) = \ln \epsilon_0$$

Shanks osservò che per la composizione $\bullet$ di forme quadratiche si ha con ottima approssimazione

$$d(f_{-1}, f_m \bullet f_n) \approx d(f_{-1}, f_m) + d(f_{-1}, f_n)$$

L'approssimazione è molto buona, l'errore essendo polinomiale $O((\ln N)^\kappa)$.

Fattorizzazione

Siano ϵ_0 la unit fondamentale positiva del campo quadratico $\mathbb{K} = \mathbb{Q}(\sqrt{N})$, $h_{\mathbb{K}}$ il class number, e $R_{\mathbb{K}} = \ln \epsilon_0$ il regulator.

Teorema

Sia $N = pq$ prodotto di due primi congruenti a 3 modulo 4. La complessità computazionale per fattorizzare N è non maggiore della complessità per calcolare il prodotto $h_{\mathbb{K}} R_{\mathbb{K}}$.

Dirichlet

Una celebre formula di Dirichlet stabilisce l'uguaglianza

$$h_{\mathbb{K}} R_{\mathbb{K}} = \frac{\sqrt{N}}{2} L(1, \chi_N)$$

ove

- χ è un carattere di Kronecker che, in questo caso, è dato dal simbolo di Jacobi $\left(\frac{N}{\cdot}\right)$.
- $L(1, \chi_N)$ è una L-function di Dirichlet definita dalla serie

$$\sum_{n=1}^{\infty} \left(\frac{N}{n}\right) \frac{1}{n}$$

Teorema condizionale

Il risultato di Dirichlet permette di formulare un teorema condizionale

Teorema

La complessità per fattorizzare $N = pq$ è non maggiore della complessità di calcolare la serie

$$\sqrt{N}\sum_{n=1}^{\infty}\left(\frac{N}{n}\right)\frac{1}{n}$$

con un'approssimazione $O((\ln N)^a)$, $a > 0$.

Dirichlet (cont.)

Il calcolo diretto di $L(1, \chi_N)$ non è pratico quando N è grande. Usando le equazioni funzionali si può ottenere la formula

$$L(1, \chi_N) = \sum_{x \geq 1} \left(\frac{N}{x} \right) \left(\frac{1}{x} \mathrm{erfc}(x\sqrt{\frac{\pi}{N}}) + \frac{1}{\sqrt{N}} E_1(\frac{\pi x^2}{N}) \right) \quad ,$$

dove $\mathrm{erfc}(x)$ è la funzione complementare d'errore, calcolabile come (vedi [Abramowitz, p.297-299])

$$\mathrm{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^\infty e^{t^2} dt = 1 - \mathrm{erf}(z) = 1 - \frac{2}{\sqrt{\pi}} \sum_{n=0}^{\infty} \frac{(-1)^n z^{2n+1}}{n!(2n+1)}$$

e $E_1(x)$ è la funzione esponenziale integrale, calcolabile come

$$E_1(z) = \int_1^\infty \frac{e^{-tz}}{t} dt = -\gamma - ln(z) - \sum_{n=1}^{\infty} \frac{(-1)^n z^n}{n \cdot n!}$$

Conclusioni

1. Se si conosce il prodotto $h_{\mathbb{K}}R_{\mathbb{K}}$ con una buona approsimazione, i.e. $O((\ln N)^{\kappa})$, allora si può fattorizzare con la stessa complessità.
2. La complesità di fattorizzazione di un intero N è limitata superiormente dalla precisione di calcolo di speciali funzioni integrali.
3. Queste proprietà hanno effetti significativi o trovano applicazione in numerosi campi, quali
   - **Number theory**
   - **Integer Factoring**
   - **Cryptography**

Referenze

1. Buell D.A., *Binary Quadratic Forms*, Springer, New York, 1989.
2. Davenport H., *The Higher Arithmetic*, Dover, New York, 1960.
3. Legendre A-M., *Essai sur la Théorie des Nombres*, Chez Courcier, Paris, 1808, reissued by Cambridge University Press, 2009.
4. Perron O., *Die Lehre von den Kettenbrüchen*, Band I, Springer, Wiesbaden, 1977.
5. Scharlau W., Opolka H., *From Fermat to Minkowski*, Springer, New York, 1985.
6. Sierpinski W., *Elementary Theory of Numbers*, North Holland, New York, 1988.