Frazioni continue

Abbiamo visto un metodo per determinare l'ordine t di un elemento $x \bmod N$ (OF)

Si è usata la stima della fase per ottenere un'approssimazione $\varphi \simeq \frac{s}{r}$

Dato che conosciamo solo $2L+1$ bits di φ (ma sappiamo che $\in \mathbb{Q}$) vogliamo calcolare la frazione più vicina a φ per ottenere r.

Usiamo l'espansione in frazioni

continua (CFE).

Una frazione continua è

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}} \qquad a_i \in \mathbb{Z}$$

a volte si denota con

$$[a_0; a_1, a_2, \dots]$$

Si definisce n-esimo convergente alla frac. cont

$$[a_0; a_1, \dots, a_n] = \frac{p_n}{q_n} \quad (p_n, q_n) = 1$$
$$p_n, q_n \in \mathbb{Z}$$

Se $x \in \mathbb{Q}$, $x \geq 1$, allora la sua rappresentazione come f.c è FINITA (e solo se).

Se x è irrazionale l'espansione è infinita ma la successione dei convergenti converge rapidamente a x.

Es. $x = \pi = 3,14\ldots$

$$\pi = 3 + 0.14\ldots \Rightarrow \frac{p_0}{q_0} = 3$$

$$\pi = 3 + \cfrac{1}{\cfrac{1}{0.14}} \ldots$$

$$= 3 + \cfrac{1}{7 + 0.06\ldots} \Rightarrow \frac{p_1}{q_1} = 3 + \frac{1}{7} = \frac{22}{7}$$

$$\frac{22}{7} = 3.14\ldots$$

Es. $\frac{415}{93} \simeq 4.4624$

$a_0 = 4$ prima approssimazione

$$\frac{415}{93} = 4 + \frac{43}{93} = 4 + \frac{1}{\frac{93}{43}} = 4 + \frac{1}{2 + \frac{7}{43}}$$

$$= 4 + \frac{1}{2 + \frac{1}{\frac{43}{7}}} = 4 + \frac{1}{2 + \frac{1}{6 + \frac{1}{7}}} =$$

$$= 4 + \frac{1}{2 + \frac{1}{6 + \frac{1}{7}}}$$

$\frac{415}{93} = [4; 2, 6, 7]$ e

$$\frac{p_0}{q_0} = 4 \quad , \quad \frac{p_1}{q_1} = 4 + \frac{1}{2} = \frac{9}{2} = 4.5$$

$$\frac{p_2}{q_2} = 4 + \frac{1}{2 + \frac{1}{6}} = \frac{58}{13} \cong 4.461$$

$$\frac{p_3}{q_3} = 4 + \frac{1}{2 + \frac{1}{6 + \frac{1}{7}}} = \frac{415}{93}.$$

Proposizione 1. Se $a_0, \dots, a_N$ sono interi allora

$$[a_0, \dots, a_n] = \frac{p_n}{q_n} \quad \text{dove}$$

$$p_0 = a_0 \qquad p_1 = 1 + a_0 a_1$$

$$q_0 = 1 \qquad q_1 = a_1$$

e per $2 \le n \le N$

$$p_n = a_n p_{n-1} + p_{n-2}$$

$$q_n = a_n q_{n-1} + q_{n-2}$$

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

e quindi $(p_n, q_n) = 1 \quad \forall n$

(Esercizio)

Quanti valori dobbiamo calcolare per trovare un'espansione in frazioni continue per $x = \frac{p}{q} > 1$, con $(p,q) = 1$?

Per definizione $p_n \uparrow$, $q_n \uparrow$

quindi $p_n = a_n p_{n-1} + p_{n-2} \geq 2 p_{n-2}$

e $q_n \geq 2 q_{n-2} \Rightarrow p_n, q_n \geq 2^{\lfloor \frac{n}{2} \rfloor - 1}$

Allora $2^{\lfloor N/2 \rfloor - 1} \leq q \leq p$ e $N = O(\log p)$

Da ciò segue che se

$x = p/q \in \mathbb{Q}$ e p, q sono interi con L bits $\Rightarrow$ l'espansione in

frazioni continua può essere calcolata con $O(L^3)$ operazioni ($O(L)$ passi di spostamento e inversione ognuno con $O(L^2)$ conti per entrambe)

<u>Teorema</u> Sia $x \in \mathbb{Q}$ e supponiamo che $\frac{p}{q}$ sia tale che

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}$$

Allora $\frac{p}{q}$ è un convergente della frazione continua di x.

Dim. Sia $\frac{P}{q} = [a_0, \dots, a_n]$ e definiamo p_1, q_1 come prima, così $\frac{p_n}{q_n} = \frac{P}{q}$. Definiamo δ t.c.

$$\alpha = \frac{p_n}{q_n} + \frac{\delta}{2q_n^2} \qquad |\delta| < 1$$

e λ t.c

$$\lambda = 2\left(\frac{q_n p_{n-1} - p_n q_{n-1}}{\delta} \right) - \frac{q_{n-1}}{q_n}$$

cioè

$$x = \frac{\lambda p_n + p_{n-1}}{\lambda q_n + q_{n-1}} \qquad \text{M+1 convergenti}$$

e $x = [a_0, \dots, a_n, \lambda]$

Possiamo supporre n pari.

Abbiamo definito

$a_n = (a_n - 1) + \frac{1}{1}$ e con p_{n-1} per Es. 2

$$\lambda = \frac{2}{\delta} - \frac{q_{n-1}}{q_n} > 2 - 1 = 1$$

Da questo segue che $\lambda \in \mathbb{Q}$, $\lambda > 1$

e quindi $\lambda = [b_0, \dots, b_m]$

da cui $x = [a_0, \dots, a_n, b_0, \dots, b_m]$

è un sviluppo per x che ha

P/q come n-mo convergente.