SENIOR 2023
TdN 2 Advanced | Ben

Note Title 06/09/2023

CONVOLUZIONI, FUNZIONI MOLTIPLICATIVE, FORMULA DI INVERSIONE DI MÖBIUS

Def. Un semigruppo $(G, \cdot)$ è un insieme G munito di un'operazione binaria $\cdot : G \times G \to G$ tale che $\cdot$ sia ASSOCIATIVA. $((x \cdot y) \cdot z = x \cdot (y \cdot z))$

Esempi $(\mathbb{N}, \cdot)$ $(\mathbb{N}_{>0}, \cdot)$

le funzioni $S \to S$ con $\circ$ ← composizione

$f : G \to \mathbb{C}$
$g : G \to \mathbb{C}$

$(f+g)(x) := f(x) + g(x)$

Def. L'operazione $*$ di "convoluzione" tra funzioni $f, g : G \to \mathbb{C}$ è definita così:

$$(f * g)(x) = \sum_{yz = x} f(y)\, g(z)$$

→ BISOGNA DARE UN SENSO A QUESTA SOMMA (vedremo in seguito)

(su G o su f,g affinché $\forall x$: sia somma finita)

Se G ha la seguente proprietà: $\forall x \in G$ esistono finite coppie $y,z \in G$ tali che $yz = x$ ($\wp$)

Vale nei seguenti esempi

$(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, ~~$(\mathbb{Z}, +)$~~, $(\mathbb{N}, +)$

$\wp$. Se la proprietà $\wp$ non vale magari sono fortunato e riesco comunque a definire $f*g$

se ad esempio $\forall x$ $\exists$ finite coppie y,z per cui $yz = x$ e $f(y), g(z) \neq 0$

Proprietà di $*$:

- ASSOCIATIVA!

$$(f*g)*h\,(x) = \sum_{yz=x} (f*g)(y)\,h(z) = \sum_{yz=x} h(z) \sum_{lm=y} f(l)g(m)$$

$$= \sum_{\substack{l,m,z:\\ lmz=x}} h(z) f(l) g(m)$$

$$= f*(g*h)$$

· ——

- Se G è commutativo allora $f * g$ commutativo

↳ $f*g(x) = \sum_{yz=x} f(y)g(z) = \sum_{zy=x} f(y)g(z) = g*f$

Esempio: $(\mathbb{N}_{\geq 0}, \cdot)$ $\quad f*g(n) = \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right)$

CONVOLUZIONE DI DIRICHLET

$(\mathbb{N}, +)$ $\quad f*g$ è come fare il prodotto delle serie formali associate

$$f*g(n) = \sum_{y+z=n} f(y)g(z).$$

- DISTRIBUTIVA RISPETTO $+$ (somma di funzioni)

OSS. $\{f : G \to \mathbb{C}\}$ munito di $+$ e di $*$ è un anello

DOMANDA: chi è l'elemento neutro di $*$?

IN GENERALE NON È DETTO CHE ESISTA

Noi ci lavoriamo con $(\mathbb{N}_{\geq 0}, \cdot)$

$\varepsilon(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases}$ è elemento neutro di $*$

Def. $1(n) = 1 \quad \forall n \in \mathbb{N}_{>0}$ (da non confondere con elemento neutro!)

DOMANDA? Quali f ammettono inverso rispetto a $*$?

g tale che $g * f = \varepsilon$ (= $f * g$)

$g * f(1) = 1 \Rightarrow g(1) f(1) = 1 \Rightarrow f(1) \neq 0$

CONDIZIONE NECESSARIA

CLAIM: è anche sufficiente!

Ragioniamo ricorsivamente: Supponiamo di aver scelto $g(1), \dots, g(k)$ in modo che $g * f(i) = \begin{cases} 1 & \text{se } i = 1 \\ 0 & \text{se } 1 < i \leq k \end{cases}$

allora $g * f(k+1) = 0$

$\iff \sum_{d \mid k+1} g(d) f\left(\frac{k+1}{d}\right) = g(k+1) f(1) + \underbrace{\sum_{\substack{d \mid k+1 \\ d < k+1}} g(d) f\left(\frac{k+1}{d}\right)}$

$\iff g(k+1) = -\frac{1}{f(1)}$ ☒

Def. una $f: \mathbb{N}_{>0} \to \mathbb{C}$ è TOTALMENTE MOLTIPLICATIVA se

$$f(mn) = f(m) f(n) \quad \forall m, n \in \mathbb{N}_{>0}$$

f MOLTIPLICATIVA se $f(mn) = f(m) f(n)$

$\forall (m, n) = 1$

Esempi φ di Eulero è moltiplicativa.

τ (numero di divisori) moltiplicativa

σ (somma dei divisori) $\nwarrow$

$1_1 \in$ TOT. MOLT.

$f(n) = \varepsilon_2(n)$ è TOT. MOLT

$f(n) = n^\alpha$ con $\alpha \in \mathbb{R}$ è TOT. MOLT.

OSS.

Proposizione f moltiplicativa. $f(1) \neq 0$

allora $f * g$ moltiplicativa $\iff g$ moltiplicativa.

Dim. ($\Rightarrow$) Supponiamo per ass. g non molt.

Sia $x \in \mathbb{N}_{>0}$ il più piccolo intero

con cui $\exists (m,n) = 1$ con $mn = x$

e $g(mn) \neq g(m)\, g(n)$

$$f * g\,(mn) = \sum_{d \mid mn} f(d)\, g\left(\frac{mn}{d}\right) = \sum_{\substack{a \mid m \\ b \mid n}} f(ab)\, g\left(\frac{m}{a}\frac{n}{b}\right)$$

$$= f(1)\, g(mn) + \sum_{\substack{a \mid m \\ b \mid n}} f(a) f(b)\, g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right)$$

$$- f(1)\, g(m)\, g(n)$$

$$= g(mn) - g(m)\, g(n) + f * f(m) \cdot f * f(n)$$

$$\hookrightarrow g(mn) = g(m)\, g(n). \qquad \lightning$$

($\Leftarrow$) altri passaggi ...

FORMULA DI INVERSIONE DI MÖBIUS

Supponiamo di avere $f(n) = \sum_{d \mid n} g(d) \cdot 1\left(\frac{n}{d}\right)$

Vogliamo capire quanto vale $g(n)$ in termini di f

$g(n) =$ roba in f

$f = g * 1 \Rightarrow$ f si ottiene da g moltiplicando per l'inversa di 1

$f * \mu = (g * 1) * \mu$

$= g * (1 * \mu) = g * \varepsilon$

$= g$

$$g(n) = \sum_{d|n} f(d)\, \mu\left(\frac{n}{d}\right)$$

↓ vogliamo capire di più!

Oss μ è moltiplicativa! $(1 * \mu = \varepsilon)$ ← mult.

$$\mu\left(\prod_i p_i^{\alpha_i}\right) = \prod_i \mu\left(p_i^{\alpha_i}\right)$$

$1 * \mu(1) = 1 \Rightarrow$ $\boxed{\mu(1) = 1}$

$1(1) \cdot \mu(1)$

$1 * \mu(p) = 0$

$1(1) \cdot \mu(p) + 1(p)\,\mu(1) \Rightarrow \boxed{\mu(p) = -1}$

$1 * \mu(p^n) = 0 \iff \sum_{i=0}^{n} \mu(p^i) = 0 \Rightarrow \boxed{\mu(p^k) = 0 \ \forall k > 1}$

$$\mu(n) = \begin{cases} 0 & \text{se } n \text{ non è sq. privo di quadrati} \\ (-1)^{\#\{\text{primi distinti in } n\}} & \text{se } n \text{ è sq. privo di quadrati.} \end{cases}$$

$$g(n) = \sum_{d \mid n} f(d)\, \mu\left(\frac{n}{d}\right) \quad \blacksquare$$

FORMULA DI INVERSIONE DI MÖBIUS

Divertitevi a mostrare le seguenti: (suggr. USARE LA MOLTIPLIC.)

① $f(n) = n^\alpha$ ha inversa $g(n) = \mu(n)\, n^\alpha$

② $|\mu|$ ha inversa $d(n) := \#\{\text{fattori primi di } n \text{ con molteplicità}\} = \sum \alpha_i$

③ φ " " $g(n) = \sum_{d \mid n} \mu(d)\, \frac{n}{d}$

④ $\sigma_\alpha(n) = \sum d^\alpha$ " " $\sum_{d \mid n} d^\alpha \mu(d)\, \mu\left(\frac{n}{d}\right)$ $\quad q(d)$ $\quad h(n)$

⑤ $|\mu|(n) = \sum_{d^2 \mid n} \mu(d)$

Vediamone una (le altre sono nello stesso stile)

(4) Dim. moltiplicativa!

$h = a * \mu$ | σ_α molt.

a basta mostrare $h * \mu \sigma_\alpha(p^k) = \begin{cases} 1 & \text{se } k=0 \\ 0 & \text{se } k>0 \end{cases}$

$h * \sigma_\alpha(p^k) = a * \mu * \sigma_\alpha(p^k) = \sum_{\substack{d,b,c \\ d+b+c=k}} \square =$

$= a(1)\ \sigma_\alpha(p^k)$
$- a(1)\ \sigma_\alpha(p^{k-1})$
$+ a(p)\ \sigma_\alpha(p^{k-1})$
$- a(p)\ \sigma_\alpha(p^{k-2})$

i conti sono facili in dopo.

Esercizio calcolare $f(n) = \sum_{1 \le d \le n} \mu(d) \left[\frac{n}{d}\right]$

↓

è una convoluzione su $(\mathbb{Q}_{>0}, \cdot)$

$1(x) = \begin{cases} 1 & \text{se } x \in \mathbb{N}_{>0} \\ 0 & \text{se } x \notin \mathbb{N}_{>0} \end{cases}$ μ (la estendo a 0 sui razionali non interi)

$g(x) = \lfloor x \rfloor$

$\boxed{f = \mu * g}$

sono ben definiti!! a patto di ⊛

$1 * f = g$ $\qquad g(n) = [n]$

$$1*f\,(n) = \sum_{m=1}^{\infty} 1(m)\, f\left(\frac{n}{m}\right) = [n]$$

$$\Rightarrow = \sum_{m=1}^{[n]} f\left(\frac{n}{m}\right) = [n]$$

⊛ SCEGLIAMO DELIBERATAMENTE che $f(x) = 0$ se $x < 1$

TUTTO FUNZIONA SE $f(x) = 1 \ \forall x \geq 1$

$f(x) = 0 \ \forall x < 1$

Per scriverla bene faccio il giro nella f e vedo i passaggi

Esercizio [Shortlist IMO 1997] Abbiamo $(a_n)_{n \geq 1}$ $a_i \in \mathbb{Z}$

t.c. $\sum_{d|n} a_d = 2^n$

$\left(a * 1^{(n)} = \underbrace{2^n}_{b(n)} \right)$

Tesi: $\forall n \quad n \mid a_n$

—

Esercizio Dimostrare che $f * 1 = \left[\sum_{d|n} \underbrace{\tau(d)^3}_{f(d)} = \underbrace{\left(\sum_{d|n} \tau(d) \right)^2}_{(\tau * 1)^2} \right]$

(1) Main idea: USIAMO INVERSIONE DI MÖBIUS:

$$g = b * \mu$$

$$g\left(\prod_i p_i^{\alpha_i}\right) = \underbrace{\sum_{s_1 \in \{0,1\}} \sum_{s_i \in \{0,1\}} \cdots \sum_{s_k \in \{0,1\}} 2^{\sum_i s_i} \cdot (-1)^{\sum s_i}}_{(*)}$$

Facciamo vedere che $p_i^{\alpha_i} \mid (*)$ $\forall i$

ci basta mostrare che $\sum_{s_i \in \{0,1\}} 2^{\sum s_j} \cdot (-1)^{\sum s_j} \equiv 0 \pmod{p_i^{\alpha_i}}$

$$2^{p_i^{\alpha_i} M} - 2^{p_i^{\alpha_i - 1} M} \equiv 0 \pmod{p_i^{\alpha_i}}$$

la differenza degli esponenti è multipla di $\varphi(p_i^{\alpha_i}) = (p_i - 1) p^{\alpha_i - 1}$

(2) L'idea principale è osservare che sia LHS che RHS sono funzioni moltiplicative in n

poi conti con p^k ...

Esercizio (μ cosa)

$$\mu(n) = \sum_{\substack{1 \le k \le n \\ (k,n)=1}} \cos\left(2\pi \frac{k}{n}\right)$$

Problema (2008 Bulgarian Autumn contest)

Dato $n \in \mathbb{N}_{>0}$ trovare il numero di a n. free con $\left\lfloor \frac{n}{\sqrt{a}} \right\rfloor$ dispari.

$$\sum_{a=1}^{n^2} \overline{|\mu^2(a)|} \cdot \underline{1}_{\{x : \lfloor \frac{n}{\sqrt{x}} \rfloor \text{ dispari}\}}(a)$$

$$= \sum_{a=1}^{n^2} \left(\sum_{d^2 \mid a} \mu(d) \right) \cdot \underline{1} \dots (a)$$

EURISTICA dove cercare di esprimere in maniera furba il fatto che $x \in \mathbb{N}$ sia dispari

$$x \text{ è dispari} \iff \sum_{i=1}^{x} (-1)^{i+1} = 1$$

$$\sum_{a=1}^{m^2} \left(\sum_{d^2 \mid a} \mu(d) \right) \sum_{i \le \left[\frac{m}{\sqrt{a}}\right]} (-1)^{i+1} = \sum_{i=1}^{m} \sum_{a \le \frac{m^2}{i^2}} (-1)^{i+1} \sum_{d^2 \mid a} \mu(d)$$

$$= \underbrace{\sum_{1 \le i \le m} \sum_{a \le \frac{m^2}{i^2}} \sum_{d^2 \mid a} \mu(d)}_{A(m)} - 2 \sum_{1 \le t \le \frac{m}{2}} \sum_{a \le \frac{m^2}{4t^2}} \sum_{l^2 \mid a} \mu(l)$$

$$A\left(\frac{m}{2}\right)$$

$A(m)$ → è definita valendo anche per arg. razionali

Per concludere il problema mi basterebbe capire A quanto vale ($\forall x \in \mathbb{Q}_{>0}$)

$$A(m) = \sum_{1 \le i \le m} \left(\sum_{a \le \frac{m^2}{i^2}} \sum_{d^2 \mid a} \mu(d) \right) = \sum_{1 \le i \le m} \sum_{d=1}^{\frac{m}{i}} \mu(d) \left\lfloor \frac{m^2}{i^2 d^2} \right\rfloor$$

$$= \sum_{1 \le n \le m} \left(\sum_{d \mid n^2} \mu(d) \right) \left\lfloor \frac{m^2}{n^2} \right\rfloor$$

$$= \sum_{1 \le n \le m} \mu(n^2) \left\lfloor \frac{m^2}{n^2} \right\rfloor$$

$$= \left\lfloor m^2 \right\rfloor$$

La risposta è $\lfloor n^2 \rfloor - 2 \lfloor (\frac{n}{2})^2 \rfloor$

CAMPI FINITI

soddisfacente ✓

L'obiettivo di questa parte è dare una risposta al seguente problema: successioni $(a_n)_{n \geq 0}$ di elementi in $\mathbb{Z}/p\mathbb{Z}$ $(\mathbb{F}_p)$

$$\begin{cases} a_0 = c_0 \\ \vdots \\ a_{d-1} = c_{d-1} \\ a_n = r_1 a_{n-1} + r_2 a_{n-2} + \dots + r_{d-1} a_{n-d} \quad \forall n \geq d \end{cases}$$

Ci viene chiesto di trovare un k (non troppo grosso) tale che siamo sicuri che il periodo della succ. mod p divide k.

Voi sapete una formula esplicita per succ. ric. lin. omo. a valori in $\mathbb{C}$ però potrebbe coinvolgere delle radici.

Esempio per cui posso ragionare senza probl. mod p $\quad p = 5 \quad p(x) = (x-1)(x+3)$.

la formula generale sarà qualcosa

tipo $a_n = c_1 1 + c_2 \cdot (-3)^{n}$

che divide

ho periodo $\forall \varphi(p) = p-1$.

Def. CAMPO è $(L, \cdot, +)$ con L insieme,

$\cdot, +$ operazioni binarie $L \times L \to L$

- $+$ e $\cdot$ hanno elementi neutri 0 e 1
- commut.
- associative
- vale prop. distr. $\cdot$ risp. $+$
- $+$ ammette inversi
- $\cdot$ ammette inversi tranne che per l'elemento neutro di $+$ (0)

$\mathbb{Q}$, $\mathbb{F}_p$, $\mathbb{Q}(x)$, $\mathbb{R}$, $\mathbb{C}$

Def. Due campi L e M sono ISOMORFI se $\exists f: L \to M$ biiettiva

t.c. 1) $f(0) = 0$

$f(1) = 1$

$f(ab) = f(a) f(b)$

$f(a+b) = f(a) + f(b)$

Def. L campo, si dice ALGEBRICAMENTE CHIUSO se $\forall\, p(x) \in L[x]$ $\exists\, \alpha \in L$ con $p(\alpha) = 0$

Esempio $\mathbb{C}$ è alg. chiuso

TEOREMA DI FEDE:

Dato L un campo qualsiasi esiste $\overline{L} \supseteq L$ tale che

1) $\overline{L}$ è alg. chiuso

2) $\forall\, \alpha \in \overline{L}$ è radice di un polinomio $p(x) \in L[x]$

questa richiesta da sola significa che $\overline{L}$ è "ALGEBRICO" su L

Non solo, $\overline{L}$ è unico a meno di isomorfismo.

NO DIM.

$\overline{\mathbb{F}_p}$ è la chiusura algebrica di $\mathbb{F}_p$.

Consideriamo $\mathbb{F}_{p^n}$ l'insieme di tutte le radici di $q_n(x) = x^{p^n} - x$ all'interno di $\overline{\mathbb{F}_p}$

OSS. Se $n=1$ recupero $\mathbb{F}_p$ all'interno di $\overline{\mathbb{F}_p}$

OSS. Sono tutti distinti perché $q_n'(x) = -1$ coprimo con $q_n(x)$

Prop. $\mathbb{F}_{p^n} \subset \overline{\mathbb{F}_p}$ è chiuso rispetto a

$+$

$\cdot$

$-$ inverso additivo

$-$ inverso moltiplicativo

Dim $a, b \in \mathbb{F}_{p^n}$

$$\Rightarrow (a+b)^{p^n} - (a+b) \overset{?}{=} 0$$

$$a^{p^n} + b^{p^n} - a - b = 0 \quad \checkmark$$

$$(a \cdot b)^{p^n} = ab \Rightarrow ab \in \mathbb{F}_{p^n}$$

Sono CONTENTO perché adesso so che $\mathbb{F}_{p^n}$ è un campo finito con p^n elementi.

Prop. Se trovo L sottocampo di $\overline{\mathbb{F}_p}$ con p^n elementi allora $L = \mathbb{F}_{p^n}$

Dim. voglio dire che $\alpha \in L \setminus \{0\}$ sta anche in $\mathbb{F}_{p^n}$, cioè è radice di $q_n(x)$

$\{x_1, x_2, x_3, \dots, x_{p^n-1}\}$ gli elementi di $L^* := L \setminus \{0\}$

$\{\alpha x_1, \alpha x_2, \dots, \alpha x_{p^n-1}\} \Rightarrow \alpha^{p^n-1} = 1$

La cosa bella di $\overline{\mathbb{F}_p}$ è che adesso posso scomporre il polinomio caratteristico $(h(x))$ della mia successione (a patto di vederla a valori in $\overline{\mathbb{F}_p} \supset \mathbb{F}_p$)

Se solo riuscissi a capire in quali campi finiti si trovano le radici di $h(x)$ (contraddizione) potrei dire che la successione è periodica modulo $\operatorname{lcm}(p^{d_i}-1)$

$\mathbb{F}_{p^{d_i}}$ è il campo finito della radice i-esima

$x^d + \sum_{i=0}^{d-1} r_i x^i$

Def. $\alpha \in \overline{\mathbb{F}_p} \Rightarrow \exists\, \mu_\alpha(x)$ polinomio di grado minimo che si annulla in α $\left(\mu_\alpha(x) \mid r(x) \ \forall\, r : r(\alpha)=0\right)$

Prop. Sia d il grado di $\mu_\alpha(x)$, allora $\alpha \in \mathbb{F}_{p^d}$.

LEMMA chiamo S quest. insieme { gli elementi di $\mathbb{F}_p$ della forma $c_0\alpha^0 + c_1\alpha^1 + \dots + c_{d-1}\alpha^{d-1}$ $(c_i \in \mathbb{F}_p)$

sono un anello

(la cosa non ovvia è che sia chiuso rispetto a $\cdot$)

Dim. $a = \sum_{i=0}^{d-1} c_i \alpha^i$

$b = \sum_{i=0}^{d-1} e_i \alpha^i$

$ab = ?$

$\alpha^d = -\sum_{i=0}^{d-1} \pi_i \alpha^i$ ← $\mu_\alpha(\alpha) = 0$

ci fa dire che $\alpha^M \in S$

Se $M \le d-1$ ok

se no induzione

$\alpha^M = \alpha^{M-d}\,\alpha^d = \alpha^{M-d}\left(-\sum_{i=0}^{d-1} \pi_i \alpha^i\right) = -\sum_{i=0}^{d-1} \pi_i \alpha^{M+i-1}$

↓ per ipotesi ind. anche questo $\in S$

Per dire che S è campo (non solo anello) ci manca da dire che S è dotato di inverso moltiplicativo

OSS. $|S| = p^d$

Prendiamo $a \in S$

$$1, a, a^2, a^3, \ldots \in S$$

prima o poi capita $a^l = a^m \quad l < m$

$$a^{l-1} = a^{m-1}$$

$$\vdots$$

$$1 = a^{m-l}$$

$\Rightarrow$ a ha inverso $a^{m-l-1} \in S$

$\Rightarrow$ S è un campo in $\mathbb{F}_p$ con p^d elementi

$\Rightarrow$ $S = \mathbb{F}_{p^d}$ (IN REALTÀ $\mathbb{F}_{p^d}$ È PURE IL PIÙ PICCOLO SOTTOCAMPO DI $\mathbb{F}_p$ CHE CONTIENE α)

Esempio: $h(x) \in \mathbb{F}_p[x]$ irriducibile in $\mathbb{F}_p$

Prop. $h(x)$ è polinomio minimo di ciascuna delle sue radici!

Dim: Vi ricordo che $\mu_\alpha(x) \mid \pi(x) \quad \forall\, \pi(x) \in \mathbb{F}_p[x]$ t.c. $\pi(\alpha) = 0$

$\Rightarrow$ $\mu_\alpha(x) \mid h(x)$ ($\forall \alpha$ radice di h)

$\Rightarrow \quad \mu_\alpha(x) = h(x)$

sto usando che h è irriducibile

$\Rightarrow$ il periodo modulo p della successione divide $p^d - 1$

$$\mathrm{mcm}\left(p^{\alpha_i} - 1 \right) = ?$$

$$\mathrm{mcm}_i \left(p^{\alpha_i} - 1 \right)$$

In generale dovrò scomporre h in fattori irriducibili in $\mathbb{F}_p[x]$ (supponendo sempre che h non abbia zeri multipli)

però so che il periodo divide $\mathrm{lcm}_i(p^{\alpha_i}-1)$

$\alpha_1, \dots, \alpha_k$ sono i gradi della decomposizione di h.

$$c\alpha^n + d n \alpha^n + n^2 \alpha^n$$

Se ho radici multiple il periodo divide $p \cdot \mathrm{lcm}_i (p^{\alpha_i} - 1)$