N2 Advanced Tess

Note Title 9/5/2016

Estensioni di campi, in particolare campi finiti

→ successioni per ricorrenza lineari mod p

Def: $(K, +, \cdot)$ è un campo se
$+$ e $\cdot$ soddisfano: assoc., commut., distributiva
$\exists\, 0$, $\exists\, 1$, $\exists\, x^{-1}\ \forall x \neq 0$

Esempi: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\quad \mathbb{Z}/p = \mathbb{F}_p$

$\mathbb{R}(x) = \{$ frazioni di polinomi a coeff. in $\mathbb{R} \}$

Def: se K, L sono campi con $K \subseteq L$
L è estensione di K

Esempi: $\mathbb{Q} \subseteq \mathbb{R}$ $\quad \mathbb{R} \subseteq \mathbb{C}$ $\quad \mathbb{Q} \subseteq \mathbb{C}$
$K \subseteq K(x)$
non è vero che $\mathbb{F}_p \subseteq$ qualcuno di questi

infatti $\mathbb{F}_2 = \mathbb{Z}/2 \not\subseteq \mathbb{R}$
altrimenti $1+1 \neq 0$
però $\mathbb{F}_2 \subseteq \mathbb{F}_2(x)$

Definiamo la caratteristica di un campo:

Oss: $1 \in K$, $1;\ 1+1;\ 1+1+1;\ \ldots$

se ci sono 2 termini uguali, allora la diff è 0, cioè $\underbrace{1+1+\dots+1}_{\boxed{n} \text{ volte}} = 0$ ← posso prendere il + piccolo

altrimenti non succede mai (es: $\mathbb{Q}, \mathbb{R}$)

la caratteristica di K è $\boxed{n}$ (se esiste)
altrimenti è 0

Es: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ ecc. hanno char $= 0$
$\mathbb{F}_p$ ha char $= p$

Oss: non ci sono K t.c. char $= 1$ (altrimenti $1 = 0$)

non ci sono K t.c. char $= n$ non primo

altrimenti $n = ab = \underbrace{(1+\dots+1)}_{a \text{ volte}} \underbrace{(1+\dots+1)}_{b \text{ volte}} = 0$

divido per a e ottengo $b = 0$

Oss: ogni campo contiene $\mathbb{Q}$ oppure uno degli $\mathbb{F}_p$

in particolare: se char $K = p$
$\{0, 1, 1+1, \dots, p-1\} \subseteq K$
si comporta esattamente come $\mathbb{F}_p$

se char $K = 0$
allora $\mathbb{N} \subseteq K$, ma allora anche $\mathbb{Z} \subseteq K$, e anche $\mathbb{Q} \subseteq K$.

Def: se K è un campo, $\mathbb{Q}$ o $\mathbb{F}_p$ è il campo fondam. di K (a seconda della caratteristica)

Allora ogni campo è estensione di un campo fondamentale

Def: se $K \subseteq L$ è un'estensione
un elemento $\alpha \in L$ è algebrico se
$\exists\ p \in K[x]$ t.c. $p(\alpha) = 0$

$K \subseteq L$, se $\forall \alpha \in L$ è algebrico, allora
$K \subseteq L$ è estensione algebrica

Esempi: $\mathbb{R} \subseteq \mathbb{C}$ se $z \in \mathbb{C}$, z è zero di
$p(x) = (x - z)(x - \bar{z})$
$\rightarrow$ è est. algebrica

$\mathbb{Q} \subseteq \mathbb{R}$ ad es $\sqrt[7]{2}$ è algebrico $\left(p(x) = x^7 - 2\right)$
però ci sono elementi non algebrici
(ad es. π, e)

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = \{ a + b\sqrt{2} : a, b \in \mathbb{Q} \} \subseteq \mathbb{R}$
$\uparrow$
è algebrica infatti $a + b\sqrt{2}$ soddisfa
$p(x) = (x - a - b\sqrt{2})(x - a + b\sqrt{2})$

anche $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[7]{2})$ è algebrica ...

Piccola osservazione, se $K \subseteq L$ [es: in $\mathbb{R} \subseteq \mathbb{C}$, $\underset{\mathbb{R}}{r} \cdot \underset{\mathbb{C}}{z} \in \mathbb{C}$]

allora L è uno spazio vettoriale su K

quindi $\exists$ una base di L su K $\quad B = \{b_i\} \subseteq L$

chiamo grado dell'estensione $[L:K] = \# B$

Es: $[\mathbb{C}:\mathbb{R}] = \#\{1, i\} = 2$

$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$

$[\mathbb{Q}(\sqrt[7]{2}):\mathbb{Q}] = 7$

$1, \sqrt[7]{2}, \sqrt[7]{2}^2, \sqrt[7]{2}^3, \dots, \sqrt[7]{2}^6$

sono indip. perché altrimenti

$\lambda_0 + \lambda_1 \sqrt[7]{2} + \dots + \lambda_6 \sqrt[7]{2}^6 = 0$

$\Rightarrow \sqrt[7]{2}$ è radice di $p(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_6 x^6 \in \mathbb{Q}[x]$

ma anche $q(x) = x^7 - 2$ ha come radice $\sqrt[7]{2}$

ma q è irriducibile su $\mathbb{Q}$ (per Eisenstein)

quindi $(q, p) = 1$ ma allora non possono avere una radice in comune

Se ho un campo K e un polinomio $p \in K[x]$ allora esiste $K \subseteq L$ t.c. p ha tutte le radici in L

Se p è irriducibile, posso fare $K[x] / p(x)$ ← modulo

Esempio: x^2+1, $\mathbb{R}$

$$\mathbb{R}[x] / x^2+1 = \{ a+bx : a,b \in \mathbb{R} \}$$

ma $x^2 \equiv -1 \pmod{x^2+1}$

quindi la x è come la i

Sia $a+bx \in \mathbb{R}[x] / x^2+1$

$\boxed{\text{dato che } x^2+1 \text{ è irr}}$ allora $(x^2+1, a+bx) = 1$

allora $\exists\, p,q \in \mathbb{R}[x]$ t.c. $(x^2+1)p + (a+bx)q = 1$

↑ è l'inverso di $a+bx$

Serve che x^2+1 è irr.

Se x^2-1, $\mathbb{R}[x] / x^2-1$ $\quad x+1, x-1 \in \mathbb{R}[x] / x^2-1$

$(x+1)(x-1) \equiv 0$

ma $x+1, x-1 \neq 0$ e vorrei fossero invertibili, per avere un campo.

Con questa costruzione, dato ~~p(x)~~ riesco a trovare L

$p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ ← fatt. in K.

Posso ottenere $K \leq L_1$ aggiungendo una radice di $p_1(x)$

(se faccio $K[x]/p_1(x)$, qui x è una radice di $p_1(x)$)

allora $p(x) = q_1(x) \cdot \ldots \cdot q_m(x)$ ← fatt. in L_1

e $m > n$ perché $p_1(x)$ si spezza

$K \leq L_1 \leq L_2 \leq \ldots \leq L$

Campi finiti

Sia K un campo con finiti elementi

Oss: $\operatorname{char} K = p$

$\mathbb{F}_p \leq K \Rightarrow K$ è $\mathbb{F}_p$ sp. vett.

$\Rightarrow \exists\, B$ base (finita)

$\overset{!}{=} \{b_1, \ldots, b_n\}$

$\Rightarrow \forall \alpha \in K$, $\alpha = \lambda_1 b_1 + \dots + \lambda_n b_n$
(con $\lambda_i \in \mathbb{F}_p$)

$\Rightarrow \# K = p^n$

Sia $\alpha \in K \setminus \{0\}$ campo finito

$1, \alpha, \alpha^2, \dots$ $\quad \exists\, m$ t.c. $\alpha^m = 1$

Se $K = \mathbb{F}_p$ basta $m = p-1$ (LFT)

sicuramente $m \leq p^n - 1$, ma in realtà $\alpha^{p^n - 1} = 1$
$\forall \alpha$

Dim: $\{1, 2, \dots, \alpha, \alpha+1, \dots\} = K \setminus \{0\}$
Sia $\beta \in K \setminus \{0\}$

$$\{\beta, 2\beta, \dots, \beta\alpha, \beta(\alpha+1), \dots\} = K \setminus \{0\}$$

$x \mapsto \beta x$ è iniettiva infatti $\beta x = \beta y \Rightarrow x = y$
divido per β

$$P = \prod_{\alpha \in K \setminus \{0\}} \alpha = \prod_{\alpha \in K \setminus \{0\}} \beta\alpha = P \cdot \beta^{p^n - 1}$$

$P \neq 0 \Rightarrow \beta^{p^n-1} = 1$

Quindi $\forall \alpha \in K$, α è radice di $X^{p^n} - X$

Anche in questo caso $\exists$ g generatore di $K \setminus \{0\}$

Voglio dim. che $\exists$ $\alpha \in K^* := K \setminus \{0\}$ t.c.
$ord_{K^*}(\alpha) = p^n - 1$

$\forall \alpha \in K^*$, $\underset{m}{\underset{\shortparallel}{ord}}(\alpha) \mid p^n - 1$

quanti elementi esistono di ord $= m$? (al max)

Sicuramente $x^m - 1$ ha al max m radici

però se $ord(\alpha) = m$ α è radice di $x^m - 1$
e non di $x^k - 1$ per $k < m$

(volendo, per inversione di Moebius) otteniamo che

$\#\{\alpha : ord(\alpha) = m\} \boxed{\leq} \varphi(m)$

D-C su K^* $\quad p^n - 1 = \sum_{m \mid p^n - 1} \#\{\alpha : ord(\alpha) = m\}$

$$\boxed{\leq} \sum_{m \mid p^n - 1} \varphi(m) = p^n - 1$$

$\Rightarrow$ devono essere tutte $=$
$\Rightarrow$ $\exists$ $\varphi(p^n - 1)$ generatori.

$\mathbb{F}_2 = \{0, 1\}$ $\quad$ $\mathbb{F}_4$ si può costruire con x^2+x+1

$= \{0, 1, \alpha, \alpha+1\}$

(poi $\alpha^2 = \alpha+1$, $\alpha(\alpha+1) = 1$ ecc.)

$\mathbb{F}_8$ con x^3+x+1

$= \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$

$\mathbb{F}_{16}$ $\quad$ x^4+x+1 (non ha radici, e l'unico polinomio irr. di $\deg = 2$ è x^2+x+1, ma $(x^2+x+1)^2 = x^4+x^2+1$)

$= \{\boxed{0}, \boxed{1}, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \boxed{\alpha^2+\alpha}, \boxed{\alpha^2+\alpha+1},$
$\alpha^3, \alpha^3+1, \alpha^3+\alpha, \alpha^3+\alpha+1, \alpha^3+\alpha^2, \alpha^3+\alpha^2+1, \alpha^3+\alpha^2+\alpha, \alpha^3+\alpha^2+\alpha+1\}$

$$(\alpha^2+\alpha)^2 + (\alpha^2+\alpha) + 1 = \alpha^4 + \alpha + 1 = 0$$

$\Rightarrow$ $\alpha^2+\alpha$ è radice di x^2+x+1

Abbiamo trovato $\mathbb{F}_4 \subseteq \mathbb{F}_{16}$

Supponiamo $K \subseteq L$ (finiti)

$\Rightarrow \#L = (\#K)^m$ $\quad$ (perché $\exists$ Base e ogni $\alpha \in L$ si scrive come combinazione lineare a coeff. in K)

Se $\#L = (\#K)^m$. $\Rightarrow$ $K \subseteq L$

infatti: $\alpha \in L \Rightarrow \alpha^{p^{n\cdot m}-1} = 1$, $\beta \in K \Rightarrow \beta^{p^n-1} = 1$

$p^n - 1 \mid p^{n\cdot m} - 1$, $\exists\, \beta \in L$ t.c. $\beta^{p^n-1} = 1$

ma si ha anche che $x^{p^n} - x$ ha tutte le radici in L, infatti: $x^{p^n} - x \mid x^{p^{nm}} - x \leftarrow$ ha tutte le radici

e K è unico! (infatti tutti gli elementi di K devono soddisfare $x^{p^n} - x = 0$)

Thm: Se $\exists\, \mathbb{F}_{p^n}$ è unico e

$$\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m} \iff n \mid m$$

Osserviamo, infatti che se α, β sono radici di $x^{p^n} - x$, anche $\alpha+\beta$, $\alpha\beta$ sono radici di $x^{p^n} - x$ $(-\alpha, \alpha^{-1})$

se $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta \Rightarrow (\alpha\beta)^{p^n} = \alpha\beta$

e $(\alpha+\beta)^{p^n} \underset{\substack{\uparrow \\ \text{i coeff. binomiali} = 0}}{=} \alpha^{p^n} + \beta^{p^n} = \alpha + \beta$

Es: ci sono polinomi irriducibili su $\mathbb{Q}$ ($\circ\ \mathbb{Z}$) che sono riducibili mod p $\forall p$

$$x^4 + 1 \overset{!}{=} (x^2 + i)(x^2 - i) \quad \text{vale su } \mathbb{F}_{p^2}$$

$$\overset{!}{=} (x^2 + 1 + \sqrt{2}x)(x^2 + 1 - \sqrt{2}x) \quad \text{"}$$

$$\overset{!}{=} (x^2 - 1 + \sqrt{-2}x)(x^2 - 1 - \sqrt{-2}x)$$

infatti: $\not\!\, i \in \mathbb{F}_p \subseteq \mathbb{F}_{p^2}$

$\not\!\, i \in \mathbb{F}_{p^2}$

$\therefore$ Se $i \in \mathbb{F}_p$, o se $\sqrt{2} \in \mathbb{F}_p$ è già riducibile

altrimenti -2 è un quadrato e $\sqrt{-2}$ è in $\mathbb{F}_p$

Quando $\mathbb{F}_p \subseteq \mathbb{F}_{p^2}$ tutti i polinomi di secondo grado si spezzano cioè ho le radici

infatti: $(x^2-a)(x^2-b) = p(x)$

$\exists\, L \supseteq \mathbb{F}_p$ t.c. in L ci sono le radici di p

però $L \supseteq \mathbb{F}_p(\sqrt{a})$, ma $\mathbb{F}_p(\sqrt{a}) = \mathbb{F}_{p^2}$

$\supseteq \mathbb{F}_p(\sqrt{b})$ $\qquad \mathbb{F}_p(\sqrt{b}) = \mathbb{F}_{p^2}$

Sia $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$

$x \mapsto x^p$

$$\phi(xy) = \phi(x)\phi(y)$$

$$\phi(x+y) = \phi(x) + \phi(y)$$

$(x+y)^p = x^p + y^p$; i coeff. binomiali sono $=0$

Sia $q(x)$ un polinomio $\in \mathbb{F}_p[x]$

se $\alpha \in \mathbb{F}_{p^n}$ è radice, allora $q(\alpha) = 0$

$$0 = \phi(q(\alpha)) = q(\alpha^p)$$

$$\overset{!}{=} \phi\left(\sum_i c_i \alpha^i\right) = \sum_i \phi(c_i \alpha^i)$$

$$\overset{!}{=} \sum_i \phi(c_i)(\phi(\alpha))^i$$

$\phi(c_i) = c_i \in \mathbb{F}_p$

$c_i^p = c_i$

$$\overset{!}{=} \sum_i c_i (\alpha^p)^i$$

$$\overset{!}{=} q(\alpha^p)$$

$\Rightarrow \alpha^p$ è radice!

$\Rightarrow \alpha^{p^k}$ sono tutte radici di q

(È vero che, se q è irriducibile su $\mathbb{F}_p$, α^{p^k} sono tutte le radici di q)

Es: Sia $q(x) = x^3 - 3x - 1$, sia p un primo t.c.

$q(x)$ è irriducibile mod p, sia α una radice di $q(x)$

$$\alpha^{p^2+p+1} = 1$$

(perché $\alpha, \alpha^p, \alpha^{p^2}$ sono le radici di q e sono diverse, altrimenti $\alpha^p = \alpha \Rightarrow \alpha \in \mathbb{F}_p$, $\alpha^p = \alpha^{p^2}$ no e neanche $\alpha = \alpha^{p^2}$ no, perché sono in $\mathbb{F}_{p^3}$,

$\alpha^p \in \mathbb{F}_p$, $\alpha^{p \cdot n} = \alpha \in \mathbb{F}_p$

$(p, \operatorname{ord} \alpha) = 1$

Irriducibilità dei $\Phi_n(x)$ su $\mathbb{Z}$

Dim: Supponiamo che $f(x) \mid \Phi_n(x)$ sia irriducibile

allora $f(x) = (x-\xi_1)\cdot\ldots\cdot(x-\xi_m)$ $\quad \xi_1 = \xi$

dimostriamo che se $(p,n)=1 \Rightarrow \xi^p$ è radice di f

da qui ho vinto perché ogni ξ' radice di $\Phi_n(x)$

è t.c. $\xi' = \xi^k$ $\quad (k,n)=1$ con k opportuno.

$$g(x) = (x-\xi^p)\cdot(x-\xi_2^p)\cdot\ldots\cdot(x-\xi_m^p)$$

I coeff. di $g(x)$ sono funzioni polinomiali simmetriche in $\xi^p,\ldots,\xi_m^p$ quindi anche in $\xi,\ldots,\xi_n$

quindi sono interi perché polinomi a coefficienti interi valutati sui coeff. interi di f.

siano $g_1,\ldots,g_m$ e $f_1,\ldots,f_m$ i coeff. di grado $1,\ldots,m$ allora $g_i \equiv f_i \mod p$

$$f_i = \underset{\substack{\uparrow \\ \text{funzione simm. elem. i-esima}}}{e_i}(\xi,\ldots,\xi_m), \quad g_i = e_i(\xi^p,\ldots,\xi_m^p)$$

$$e_i(x_1,\ldots,x_m)^p \equiv e_i(x_1^p,\ldots,x_m^p) \mod p$$

$e_i(x_1^p, \dots, x_m^p) = e_i(x_1, \dots, x_m)^p + p\, f(x_1, \dots, x_m)$

simmetrico

valuto in $x_1, \dots, x_m = \xi_1, \dots, \xi_m$

e ottengo $g_i = f_i^p + p \cdot \text{intero}$

mod p $\quad g_i \equiv f_i^p \equiv f_i$

Se $f(x)$ ha ξ^p come radice sono contento

altrimenti $g(x) \neq f(x)$, quindi sono coprimi

perché f è irr. e $\deg g = \deg f$

inoltre g è irr., altrimenti $g = a \cdot b$

e come sono passato da f a g elevando alla p

così posso ottenere f da g elevando alla p^{-1} mod n

$a(\xi^p) = 0 \Rightarrow a'(x)$ con radici quelle di a elevate alla p^{-1} mod n

quindi c'è anche ξ

quindi $a' \in \mathbb{Z}[x]$ e $f \mid a'$

ma $\deg f = \deg g > \deg a = \deg a' \geq \deg f$

$f(x) \mid \Phi_n(x)$

$g(x) \mid \Phi_n(x)$

$\Rightarrow f(x) g(x) \mid \Phi_n(x) \mid x^n - 1$

assurdo mod p:

$\bar{f} \cdot \bar{g} = \bar{f}^2 \mid x^n - 1 \quad$ assurdo perché per il test derivata $x^n - 1$ ha radici doppie $\iff$ le condivide con la derivata $= n x^{n-1}$

$$\equiv x^{n-1}$$

Successioni per ricorrenza mod p

Come al solito, se scrivete il polinomio caratteristico della ricorrenza e avete le radici (per esempio, supponiamole distinte)

$$\Rightarrow a_n = \lambda_1 r_1^n + \lambda_2 r_2^n + \dots + \lambda_m r_m^n$$

con $r_1, \dots, r_m$ radici di $t^m - \dots = 0$ (il pol. caratt.)

$a_{n+2} = a_{n+1} + a_n \qquad t^2 - t - 1$

mod $p = 11$ si ha che $t^2 - t - 1 = (t-4)(t+3)$

quindi $a_n = \lambda_1 4^n + \lambda_2 (-3)^n$

quindi è periodica di periodo $| \; 10$

mod 3 non c'è la radice ma posso scrivere

$$t^2 - t - 1 = \left(t - \frac{1+\sqrt{5}}{2}\right)\left(t - \frac{1-\sqrt{5}}{2}\right) \quad \text{in } \mathbb{F}_9$$

$$\overset{!}{=} \left(t + (1+\sqrt{-1})\right)\left(t + (1-\sqrt{-1})\right)$$

$$\overset{!}{=} \left(t + (1+i)\right)\left(t + (1-i)\right)$$

$$a_n = \lambda_1 (-(1+i))^n + \lambda_2 (-1+i)^n$$

qui il periodo $| \; p^2 - 1 = 8$

perché così è per $-1-i$ e $-1+i$

In generale, se ho 2 radici distinte il periodo $| \; p^2 - 1$

Invece, solo per $p=5$ $\quad t^2 - t - 1 = (t-3)^2$

in tal caso $a_n = \lambda_1 \boxed{3^n} + \lambda_2 \boxed{n} \boxed{3^n}$

$\Rightarrow$ il periodo $| \; \boxed{p} \cdot \boxed{(p-1)}$

Es: trovare termini iniziali per Fibonacci per avere periodo 4 mod 5

Lo stesso discorso funziona per qualsiasi ricorrenza lineare

$$a_{n+m} = c_{m-1} a_{n+m-1} + \dots + c_0 a_0$$

allora il periodo $\mid p^h - 1$ per h opportuno (che dipende dalla fattorizzazione mod p) se le radici sono distinte

se ci sono 2+ radici coincidenti, periodo $\mid p \cdot (p^h - 1)$

Es: se $m = 3$ se radici distinte ci sono 3 possibilità

$p(x)$ sia irr. $\rightarrow$ per $\mid p^3 - 1$

$p(x) = (x - r_1)\, q(x)$

$\uparrow$ irr deg = 2 $\rightarrow$ $\mid p^2 - 1$

$p(x) = (x - r_1) \cdot \ldots \cdot (x - r_k)$ $\rightarrow$ $\mid p - 1$

Oss: con polinomi più grossi basta lavorare in $\mathbb{F}_{p^h}$

con $h = \mathrm{mcm}(\deg_i)$

$\uparrow$ quelli che compaiono nella fattorizzazione

Es: $\begin{cases} a_0 = 2 \\ a_{n+1} = 2a_n^2 - 1 \end{cases}$

dimostrare che se $p \mid a_n \Rightarrow 2^{n+3} \mid p^2 - 1$

$b_n(x) = \dfrac{x^n + x^{-n}}{2}$ ($= \cosh(y)$ per y opportuno)

($\cosh(ix) = \cos(x)$ in $\mathbb{C}$)

$b_{2n}(x) = 2b_n^2(x) - 1$

Se trovassimo un opportuno c, si avrebbe

$a_n = \dfrac{c^{2^n} + c^{-2^n}}{2}$ vorrei poterla scrivere mod p

c si ottiene guardado $n=0$ $\quad 2 = \dfrac{c + c^{-1}}{2}$

$\rightsquigarrow$ sarebbe $c = 2 + \sqrt{3}$

In $\mathbb{F}_{p^2}$ si ha $a_n = \dfrac{(2+\sqrt{3})^{2^n} + (2+\sqrt{3})^{-2^n}}{2}$

se $p \mid a_n$ $\quad a_n = 0$ in $\mathbb{F}_{p^2}$

$\Rightarrow \underbrace{(2+\sqrt{3})}_{c}^{2^{n+1}} = -1$

ord $c = 2^{n+2} \mid p^2 - 1$

Se si avesse che $c = D^2$ in $\mathbb{F}_{p^2}$ avremmo finito

$2(2+\sqrt{3}) = (1+\sqrt{3})^2$

mi basterebbe che 2 fosse un $\square$, ma ce l'ho perché sono in $\mathbb{F}_{p^2}$.

Sistemi di ricorrenze e ricorrenze su una sola successione

$$\begin{cases} a_{n+1} = \lambda_1 a_n + \lambda_2 b_n + \dots \\ b_{n+1} = \mu_1 a_n + \mu_2 b_n + \dots \\ \vdots \qquad \ddots \end{cases}$$

$$a_{n+m+1} = \nu_m a_{n+m} + \dots + \nu_0 a_n$$

dipende da $m+1$ termini precedenti

$$x_n = \begin{pmatrix} a_n \\ b_n \\ \vdots \end{pmatrix} \qquad M = \begin{pmatrix} \lambda_1 & \lambda_2 & \dots \\ \mu_1 & \mu_2 & \dots \\ \vdots & & \ddots \end{pmatrix}$$

Ho una ricorsione espressa come

$$x_{n+1} = M x_n$$

passaggio facile

$a_{n-1} = b_n \quad , \quad b_{n-1} = c_n \quad , \quad \ldots$

$$\begin{cases} a_{n+1} = v_m a_n + v_{m-1} b_n + \ldots + v_0 z_n \\ b_{n+1} = a_n \\ c_{n+1} = b_n \\ \vdots \end{cases}$$

$$M = \begin{pmatrix} v_m & v_{m-1} & \cdots & v_0 \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & & \\ 0 & \cdots & 1 & 0 \end{pmatrix}$$

$\longrightarrow$ più difficile

Sia $p_M(t)$ il polinomio caratteristico di M

allora $p_M(M) = M^n + c_{n-1} M^{n-1} + \ldots + c_1 M + c_0 \underset{\uparrow \text{ l'identità}}{I} = 0$

Es: $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = M$

$p_M(t) = t^2 - t - 1$

infatti $M^2 - M - I = 0$

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$p_M(M)\, x_n = 0 \cdot x_n = 0$$

$$\sum_i c_i M^i x_n = 0$$

$$= \sum_i c_i x_{n+i} = 0$$

$\Rightarrow$ $p_M(t)$ è la ricorrenza che soddisfano tutte le coordinate di x_n