SENIOR 2011 - A1 MEDIUM

Titolo nota 06/09/2011

① Polinomi
② Poli simmetrici in + variabili
③ Lemma di Gauss, irriduc in $\mathbb{Q}[x]$
④ Polinomi ciclotomici

Polinomio $\sum_{i=0}^{m} a_i x^i$. $a_i \in \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$K[x_1, \dots, x_m]$

Principio di identità → infinito

A anello. f, g polinomi di grado $\leq m$. Sono equivalenti:

① $f = g$ come poli (sono = i coeff)
② $f(x) = g(x)$ per $m+1$ valori di x
③ $f(x) = g(x)$ $\forall x \in A$.

Dim:

① ⇒ ②,③

② ⇒ ① $x_1, \dots, x_{m+1}$ radici

$x - x_1 \mid f(x) - g(x)$.

$f(x) - g(x) = (x - x_1)\, q_1(x)$

$= (x - x_1)(x - x_2) \cdots (x - x_{m+1})\, q_{m+1}(x)$

grado $\leq m$ — grado $\geq m+1$ a meno che è il poli $= 0$

Attenzione! ③ non è equivalente

$\mathbb{Z}/p\mathbb{Z}$ $x^p - x = 0$ è vero $\forall x \in \mathbb{F}_p$ (piccolo Fermat)

ma non sono uguali come poli!!

Con anello infinito, basta ③ ⇒ ②.

② ⇒ ① $f(x) = \sum_{i=0}^{m} a_i x^i$ t.c

$f(x_i) = g(x_i) \quad \forall i = 0, \dots m+1$

$$\begin{cases} a_0 + a_1 x_1 + \dots + a_m x_1^m = g(x_1) \\ \vdots \\ a_0 + a_1 x_{m+1} + \dots + a_m x_{m+1}^m = g(x_{m+1}) \end{cases}$$

sono $m+1$ condizioni lineari.

Fatto misto 1: un sist lineare (m eq in m incognite) ha esattam una sol ($\Leftrightarrow$) det della matrice dei coeff è $\neq 0$

$$\begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^m \\ \vdots & & & & \\ 1 & x_{m+1} & x_{m+1}^2 & \dots & x_{m+1}^m \end{pmatrix}$$ = matrice dei coeff

Fatto misto 2: le matrici di questa forma hanno sempre det $\neq 0$.

Prop: dati $m+1$ punti (x_i, y_i) esiste un unico poli di grado $\leq m$ t.c $p(x_i) = y_i \ \forall i$.

Dim:

1° caso: $y_0 = \dots y_m = 0 \qquad p(x) = 0$

$y_0 = 1 \quad y_2 = \dots y_m = 0. \qquad (x - x_2) \cdots (x - x_m) = q(x)$

$\frac{q(x)}{q(x_0)}$ realizza tutto $= \frac{(x - x_1) \cdots (x - x_m)}{(x_0 - x_1) \cdots (x_0 - x_m)} = L_0(x)$

Caso generale:

$P(x) = \sum y_i L_i(x)$ funziona, perché

$$L_i(x) = \begin{cases} 0 & \text{se } x \neq x_i \\ 1 & \text{se } x = x_i \end{cases}$$

$P(x_k) = y_k$.

Criterio delle derivate

$f(x) = \sum_{i=0}^{m} a_i x^i \Rightarrow Df(x) := \sum_{i=1}^{m} a_i\, i\, x^{i-1}$. $a_i \in K$ campo

Proprietà:

$D(f+g) = Df + Dg$

$D(\lambda f) = \lambda Df$ se $\lambda \in K$

$D(fg) = Df \cdot g + Dg \cdot f$ [Ex: verificare]

Ex: ① $x^4 + 3x + 1 \longrightarrow 4x^3 + 3$

② in $\mathbb{F}_p$ $x^p - 1 \longrightarrow \underbrace{p}_{=0} x^{p-1} = 0$

Criterio: K campo, $f \in K[x]$.

f ha radici multiple (in $\overline{K}$) $\iff$

$MCD(f, Df) \neq 1$.

Dim

$\Rightarrow$) $f(x) = (x-x_1)^m \cdot q(x)$ $m > 1$

$MCD\big((x-x_1)^m \cdot q(x),\ (x-x_1)^m Dq(x) + \underbrace{D((x-x_1)^m)}_{m(x-x_1)^{m-1}} q(x)\big)$

[Ex: per induz su m]

L'MCD è diviso da $(x-x_1)^{m-1} \neq 0$!

$\Leftarrow$) Dobbiamo dimostrare che, se f non ha radici multiple,

$x - x_1 \mid f(x) \overset{?}{\Rightarrow} x - x_1 \nmid Df(x)$.

$f(x) = (x-x_1)\, q(x)$ e $q(x_1) \neq 0$

$Df(x) = q(x) + (x-x_1)\, Dq(x)$

$Df(x_1) = \underbrace{q(x_1)}_{\neq 0} + 0$.

ok.

Polinomi in più indeterminate.

$p(a,b,c) = a^3+b^3+c^3-3abc$.

Ex: p simmetrico $\Rightarrow$ se posso scomporlo, i suoi fattori sono simmetrici.

Ex: p è omogeneo $\Rightarrow$ tutti i fattori sono omogenei.

Dim 2:

Idea: $p(x_1,\dots,x_m) = f(x_1,\dots,x_m)\cdot g(x_1,\dots,x_m)$

Consideriamo i monomi di grado più alto in f e g.

Come si fattorizzano?

1° modo: guardiamo c come la variabile principale, a,b fissi. $c=-a-b$ è radice

$$a^3+b^3+(-a-b)^3+3ab(a+b)=0$$

$$a^3+b^3+3a^2b+3ab^2 = (a+b)^3$$

$$a+b+c \mid a^3+b^3+c^3-3abc$$

$$a^3+b^3+c^3-3abc = (a+b+c)\cdot \text{cosa?}$$

Posso ottenere "cosa" facendo la divisione

$$\begin{array}{l} c^3 - 3abc + a^3+b^3 \\ -c^3 + ac^2+bc^2 \\ \hline / \ (a+b)c^2 - 3abc + a^3+b^3 \end{array} \quad \Big| \ \begin{array}{l} c+a+b \\ \hline c^2 \end{array} \quad \text{etc.}$$

Altro modo per det "cosa":

Teorema fondamentale dei poli simmetrici

$x_1,\dots,x_n$ indeterminate

$$\begin{cases} \sigma_1 = x_1+\dots+x_n \\ \sigma_2 = x_1x_2+x_1x_3+\dots+x_{n-1}x_n \\ \sigma_k = \prod_{i=1}^{n} x_i \end{cases}$$ sono funz simmetriche.

$F(x_1,\dots,x_n)$ poli simmetrico, allora $\exists\ \tilde{F}$ polinomio

t.c $F(x_1,\dots,x_n) = \tilde{F}(\sigma_1,\dots,\sigma_n)$.

Ex: $x_1^2 + \dots + x_n^2 = F(x_1,\dots,x_n)$

$\sum x_i^2$

$(\sum x_i)^2 - 2\sum_{i\neq j} x_i x_j$

$\tilde{F}(\sigma_1,\dots,\sigma_n) = \sigma_1^2 - 2\sigma_2$.

$$a^3+b^3+c^3-3abc = (a+b+c)\cdot f(a,b,c)$$

Sappiamo che $f(a,b,c)$ è simmetrico (ex di prima), è omogeneo di grado 2.

$$f(a,b,c) = A\,\frac{\sigma_1^2}{(a+b+c)^2} + B\,\frac{\sigma_2}{ab+bc+ca}$$

Devo determinare A e B.

Chi è il coeff di a^3?

In LHS è 1, in RHS è A

$$1 = A$$

Come det B? L'uguaglianza deve valere con $a=b=c=1$

$$0 = 3(3^2 + B\cdot 3)$$

$$B = -3$$

$$a^3+b^3+c^3-3abc = (a+b+c)\cdot\left((a+b+c)^2 - 3(ab+bc+ca)\right)$$

$$= (a+b+c)(a^2+b^2+c^2-ab-bc-ca).$$

Es: $\mathbb{Q}(i)$.

K campo $p(x) \in K[x]$.

$$\frac{K[x]}{(p(x))}$$

Ex: $p(x) = x^2 - 5 \qquad x^3 - 3x$ va diviso per $p(x)$ e poi si prende la classe di resto.

Fatto: $\frac{K[x]}{p(x)}$ è un campo se p è irriducibile.

Es: $\frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{C}$

$\frac{\mathbb{R}[x]}{(x^2+1)} \cong \mathbb{R}[i]$

$\{a+bx : a,b \in \mathbb{R}\}$

$a+bx \longrightarrow a+bi$.

Gli oggetti si sommano e moltiplicano allo stesso modo:

$(a+bx)+(a'+bx) = a+a'+(b+b')x$

$(a+bi)+(a'+b'i) = a+a'+(b+b')i$

Idem per la moltiplicaz

Dim del fatto:

Ogni elemento $\overline{f(x)}$ ha un inverso?

Teorema di Bezout per polinomi:

$f(x)$, $p(x)$ sono coprimi $\Rightarrow \exists\, a(x), b(x)$ t.c

$1 = a(x)\cdot f(x) + b(x)\cdot p(x)$.

L'inverso di $f(x)$ in $\frac{K[x]}{(p(x))}$ è $a(x)$, perché

$a(x)\cdot f(x) \equiv 1 \quad (p(x))$.

Ex: $\frac{\mathbb{F}_p[x]}{(x^2-5)} =$ → se $\exists\, a \in \mathbb{F}_p$ t.c $a^2 = 5$, poco interessante
→ altrimenti il denom è irriducibile, quindi quello è un campo.

$\{a+bx : a,b \in \mathbb{F}_5\}$

Quanti elementi? 25.

Ex: consideriamo i Fibonacci

$$\begin{cases} F_0 = 0 \\ F_1 = 1 \\ F_{n+1} = F_n + F_{n-1} \end{cases}$$

Guardiamo la succ mod p, p primo.

① La succ è periodica, chiamiamo $\pi(p)$ il periodo.

② Se $p \equiv \pm 1 \ (5)$ allora $\pi(p) \mid p-1$

③ Se $p \equiv \pm 2 \ (5)$ allora $\pi(p) \mid 2(p+1)$

Dim:

① $\{(F_i, F_{i+1}) : i = 1, \dots, p^2+1\}$

Una coppia si ripete. Da lì, si ripete tutta la stringa.

Perchè non ha antiperiodo?

Oss 1: $p \equiv \pm 1 \mod 5 \iff p$ è un quadrato mod 5
$\iff 5$ è un quadrato mod p

(dalla reciprocità quadratica,

$$\left(\frac{p}{5}\right)\cdot\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{5-1}{2}} = 1.$$

Oss 2: Possiamo pensare la succ in $\mathbb{F}_p$

Oss 3: $F_n = \dfrac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$.

Vale anche in $\mathbb{F}_p$, se $\exists\, x \in \mathbb{F}_p$ t.c $x^2 = 5$

Ex: ricavare la formula per i Fibonacci in $\mathbb{F}_p$.

Dim di ②. $\sqrt{5}$ è un elemento di $\mathbb{F}_p$.
mod 11 $\sqrt{5} = 4$

Basta far vedere che

$F_{p-1} = 0$ e $F_p = 1$.

$$F_{p-1} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{p-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{p-1}}{\sqrt{5}} \overset{\text{piccolo teo Fermat}}{=} \frac{1-1}{\sqrt{5}} = 0$$

$$F_p = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{p} - \left(\frac{1-\sqrt{5}}{2}\right)^{p}}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = 1 \text{ . ok.}$$

Dim di ③ In $\frac{\mathbb{F}_p[x]}{(x^2-5)} =: K$ c'è elemento x è una radice di 5.

$x^2 = 5$

$K = \mathbb{F}_p \ni a + 0 \cdot x$

le piccolo teo di Fermat non vale più!!! (No dim di prima).

Domanda: quanto fa $\left(\frac{1+\sqrt{5}}{2}\right)^p$ in K?

$(a+b)^p = ?$ se $a, b \in K$

$$= \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p$$

Quindi $\left(\frac{1+\sqrt{5}}{2}\right)^p = \frac{(1+\sqrt{5})^p}{2^p} \overset{\text{fatto sopra}}{=} \frac{1 + (\sqrt{5})^p}{2}$

Basta capire cosa fa $(\sqrt{5})^p$.

Osserviamo che $(\sqrt{5})^p$ risolve $x^2 - 5 = 0$:

$$(\sqrt{5}^p)^2 - 5 = \sqrt{5}^{2p} - 5 = 5^p - 5 = 0.$$

$x^2 - 5 = 0$ ha due sol: $\sqrt{5}$ e $-\sqrt{5}$

Può essere $(\sqrt{5})^p = \sqrt{5}$? No! Se lo fosse, $\sqrt{5}$ sarebbe una radice di $x^p - x = 0$.

Ma conosciamo tutte quelle radici: $0, 1, \dots p-1$.
Avevamo assunto che $\sqrt{5} \notin \mathbb{F}_p$.

Quindi $(\sqrt{5})^p = -\sqrt{5}$.

Allora $\left(\frac{1+\sqrt{5}}{2}\right)^p = \frac{1+(\sqrt{5})^p}{2} = \frac{1-\sqrt{5}}{2}$ (*)

Similmente $\left(\frac{1-\sqrt{5}}{2}\right)^p = \frac{1-(\sqrt{5})^p}{2} = \frac{1+\sqrt{5}}{2}$ (*)

Per dim la tesi, basta vedere

$F_{2p+2} = 0 \qquad F_{2p+3} = 1$

$$F_{2p+2} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{2p+2} - \left(\frac{1-\sqrt{5}}{2}\right)^{2p+2}}{\sqrt{5}} \overset{(*)}{=} \frac{\left(\frac{1-\sqrt{5}}{2}\right)^2\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1+\sqrt{5}}{2}\right)^2\left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}}$$

$$= 0$$

[$F_{2p+3} = $ ex.]

□.

Ex! (4) mostrare che $\pi(p^k) \leq p^{k-1}\pi(p)$
con $=$ se e solo se $\pi(p) \neq \pi(p^2)$.

Polinomi a coeff interi

Teorema: $f(x) = \sum a_i x^i$ $\quad a_i \in \mathbb{Z}$, $\quad p/q$ radice razionale $\quad (p,q)=1$

Allora

$p \mid a_0$

$q \mid a_m$.

Dimo

$$q^m \cdot 0 = \left(a_0 + a_1 \tfrac{p}{q} + \dots + a_m \tfrac{p^m}{q^m}\right) q^m$$

$$0 = a_0 q^m + a_1 p q^{m-1} + \_\_\_ + a_m p^m$$

p divide la somma e il 2°, $\_\_$ n° monomio

$\Rightarrow p \mid a_0 q^m \qquad (p,q)=1$

$\Rightarrow p \mid a_0$.

L'altra è uguale.

Esempio: x^3+x+1 è riducibile in $\mathbb{Q}[x]$?

No. Se fosse riducibile avrebbe un monomio di grado 1, quindi una radice razionale

Per il teo precedente, il numerat dovrebbe dividere 1 e anche il denom.

Ma 1 e -1 non sono radici

Lemma di Gauss

$p(x) \in \mathbb{Z}[x]$. Se $p(x)$ si spezza in $\mathbb{Q}[x]$ allora si spezza anche in $\mathbb{Z}[x]$.

$p(x) = a(x) \cdot b(x)$ $\quad a, b \in \mathbb{Q}[x] \Rightarrow \exists\, \tilde{a}$ e $\tilde{b} \in \mathbb{Z}[x]$ t.c

$$p(x) = \tilde{a}(x) \cdot \tilde{b}(x).$$

Esempio: $x^2 - 1 = \left(\frac{1}{2}x - \frac{1}{2}\right)(2x+2)$

$$= (x-1)(x+1)$$

Def: $p(x) \in \mathbb{Z}[x]$. $p(x) = \sum a_i x^i$. Il CONTENUTO DI p è

$$c(p) = MCD(a_0, \dots, a_m).$$

Lemma: il contenuto è moltiplicativo,

$$c(a(x)) \cdot c(b(x)) = c(a(x) \cdot b(x))$$

Oss: una divisibilità è ovvia.

Dim lemma:

① Basta farlo con $c(a) = c(b) = 1$.

$a(x) = c(a) \cdot \tilde{a}(x)$ $\qquad$ $b(x) = c(b) \cdot \tilde{b}(x)$

con $c(\tilde{a}) = c(\tilde{b}) = 1$

$a(x) \cdot b(x) = c(a) \cdot c(b) \cdot \tilde{a}(x) \cdot \tilde{b}(x)$

Supponiamo di aver dimostrato la tesi su $\tilde{a}$ e $\tilde{b}$

$c(a(x) \cdot b(x)) = c(a) \cdot c(b) \cdot c(\tilde{a} \cdot \tilde{b})$

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \| \; 1$

$c(a) = c(b) = 1$

② Dobb.amo dim che $\nexists\, p$ t.c.

p | tutti i coeff di $a(x) \cdot b(x)$.

Se esistesse un tale p,

$$\bar{a}(x) \cdot \bar{b}(x) = 0 \quad \text{in } \mathbb{F}_p[x],$$

assurdo (prendiamo $a_k x^k$ monomio di grado max in $\bar{a}(x)$, $b_q x^q$ monomio di grado max in $\bar{b}(x)$.
$\bar{a}(x)\cdot\bar{b}(x)$ contiene un solo monomio di grado x^{q+k}, che è $a_k \cdot b_q x^{k+q}$, che non si annulla).

[Fatto intermedio: se p divide tutti i coeff di $a(x)\cdot b(x)$, allora divide tutti i coeff di a oppure di b.].

Dim lemma di Gauss

① Supponiamo $c(p)=1$

② $p(x) = a(x)\cdot b(x)$ $\qquad a(x) = \frac{A(x)}{m} \in \mathbb{Z}[x]$ $\qquad b(x) = \frac{B(x)}{n} \in \mathbb{Q}$.
$m, n \in \mathbb{N}$

$mn\ p(x) = A(x)\cdot B(x)$

$c(mn\ p(x)) = mn\ \underbrace{c(p(x))}_{=1} = c(A(x)\cdot B(x))$

[Fatto: $c(m\cdot p(x)) = m\cdot c(p(x))$] $\qquad = c(A(x))\cdot c(B(x))$

Lemma $\qquad (*)$

$p(x) = a(x)\cdot b(x) = \frac{A(x)}{m}\cdot\frac{B(x)}{n} \overset{\text{uso } (*)}{=} \frac{A(x)}{c(A(x))}\cdot\frac{B(x)}{c(B(x))}$

$\in \mathbb{Z}[x]$?

Oss: se $n=6$ esistono due poli a prodotto nullo in $\mathbb{Z}/6\mathbb{Z}[x]$:

$(2x+2)\cdot 3x = 6x^2+6x = 0$ in $\mathbb{Z}/6\mathbb{Z}[x]$.

Irriducibilità

Come faccio a dire che $f(x)$ (monico) è irriducibile su $\mathbb{Z}[x]$?

(1) Trovare p primo t.c. $\overline{f}(x)$ è irriducibile.

Oss: esistono polinomi riducibili in $\mathbb{F}_p[x]$ $\forall p$ primo, ma irriducibili in $\mathbb{Z}[x]$. Es: x^4+1. [Ex] -

Se si riducesse $f(x) = a(x) \cdot b(x)$ in $\mathbb{Z}[x]$

La guardo mod p.

(2) Eisenstein (vedi N1)

(3) $f(x) \in \mathbb{Z}[x]$, con termine noto ap primo e $|a_d| > \sum |a_i|$.

Allora f è irriducibile in $\mathbb{Q}[x]$

Dim!

Se f si riducesse

$f(x) = a(x) \cdot b(x)$ $\quad a, b \in \mathbb{Z}[x]$ (per il lemma di Gauss)

↑ ↑

wlog il termine noto di $a(x)$ è ± 1 (e altrimenti è $\pm p$)

Allora $a(x)$ ha una radice (complessa) di mod ≤ 1, che chiamo z. (perché il prodotto delle radici è 1)

z è radice anche di f

$$0 = |f(z)| = \left|\sum a_i z^i\right| \geq |a_0| - \sum |a_i| \underbrace{|z|}_{\leq 1}^i$$

$$\geq |a_0| - \sum |a_i|$$

$$> 0$$

↑ per hp.

Assurdo.

Ex (IMO 2006 - 5)

$P(x)$ poli a coeff interi, $K \in \mathbb{N}$, $n = \deg P > 1$

Consideriamo il polinomio

$$P^{(k)}(x) = \underbrace{P(\dots P}_{k \text{ volte}}(x)) .$$

Dimostrare che esistono al più n interi t.c.

$$P^{(k)}(x) = x .$$

Dim:

[Fatto gen] $a, b \in \mathbb{Z}$ $\quad a-b \mid p(a)-p(b)$ (*)

Dim1: fisso b, muovo a. $a=b$ è radice

Dim2: $p(x) = \sum a_i x^i$

$$p(a) - p(b) = \sum a_i (a^i - b^i)$$

$\uparrow$ divisibile per $a-b$

Step 1: sia a t.c $P^{(k)}(a) = a$.

$a - P(a) \mid P(a) - P^{(2)}(a) \mid P^{(2)}(a) - P^{(3)}(a) \mid \dots \mid P^{(k)}(a) - P^{(k+1)}(a)$

$\uparrow$ (*) con $b = P(a)$

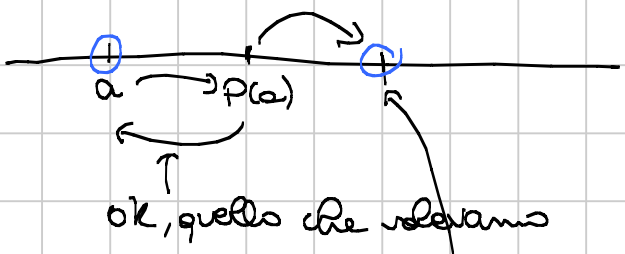
$= a - P(a)$

Sono tutte "quasi" uguaglianze:

$$a - P(a) = \pm (P(a) - P^{(2)}(a))$$

Vediamo che $a = P^{(2)}(a)$ per ogni a t.c $a = P^{(k)}(a)$

WLOG $a < P(a)$



Se $P(P(a)) \geq$, $P^{(k)}(a)$ non può mai essere a (perché si dovrebbe ripassare da $P(a)$...)

Ci siamo ridotti al caso $K=2$.

Vogliamo dim che

$p(p(x)) = p^{(2)}(x) = x$

ha al più n sol intere.

[Nota: $p^{(2)}(x) = x$ ha n^2 sol in $\mathbb{C}$ (perché n^2 è il grado]

Supponiamo per assurdo che ne abbia $n+1$, e siano $a_1, \dots, a_{n+1}$.

$$a-b \mid p(a)-p(b) \mid p(p(a)) - p(p(b)) \quad (*) \quad \forall a,b \in \mathbb{Z}.$$

Se $a=a_i$, $b=a_j$, otteniamo

$$a_i - a_j = \pm(p(a_i)-p(a_j)) \quad \circledast$$

(perché (*) dice

$a_i-a_j \mid p(a_i)-p(a_j) \mid a_i-a_j$)

ovvero

- $p(a_i)-a_i = p(a_j)-a_j$ (segno + in $\circledast$)
- $p(a_i)+a_i = p(a_j)+a_j$

per ogni $i,j \in \mathbb{N}$.

Chiamiamo $R(x) = p(x)-x$

$S(x) = p(x)+x$.

Allora $\forall i,j \in \mathbb{N}$

- $R(a_i) = R(a_j)$
- $S(a_i) = S(a_j)$

È possibile che $R(a_i) = R(a_j)$ $\forall j = 2, \dots, n+1$?

No, perché $R(x)-R(a_1)$ ha grado n e $n+1$ radici

Similmente, non è possibile che $S(a_1) = S(a_j)$ $\forall j = 1, \dots, n+1$

Quindi $\exists a_i, a_j$ t.c

(*) $R(a_i) \neq R(a_i) \Rightarrow S(a_i) = S(a_i)$

$S(a_i) \neq S(a_j) \Rightarrow R(a_i) = R(a_j)$ (*)

Prendiamo la coppia i, j.

$R(a_i) = R(a_j)$ o $S(a_i) = S(a_j)$

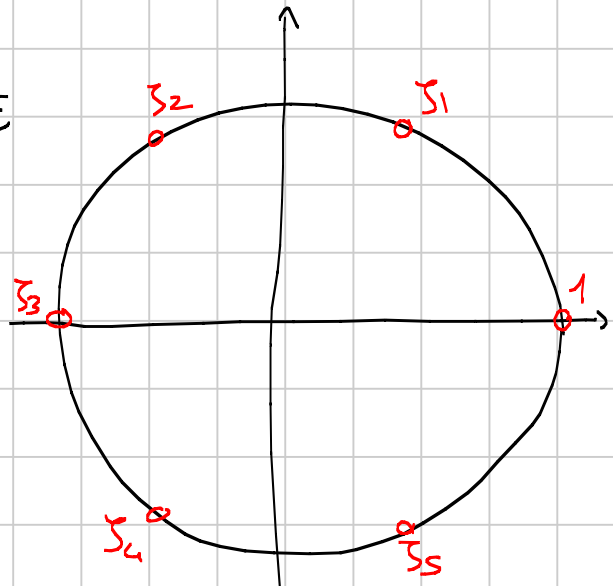
impossibile $R(a_i) = R(a_i)$ da (*), che contraddice (*)

Anche l'altra è assurda.

Radici dell'unità

Def: $\zeta \in \mathbb{C}$ si chiama RADICE n-ESIMA DI 1 se risolve

$$x^n - 1 = 0$$



Calcoliamo

ζ_1	$\zeta_1^2 = \zeta_2$	$\zeta_1^3 = \zeta_3$	ζ_4	ζ_5	1
ζ_2	ζ_4	1			
$\zeta_3 = -1$	1				
ζ_4	ζ_2	1			
ζ_5	ζ_4	ζ_3	ζ_2	ζ_1	1

ζ_1 ha periodo	6
ζ_2 " "	3
ζ_3 " "	2
ζ_4 " "	3
ζ_5 " "	6

Fattorizziamo

$$x^6 - 1 = (x^3 - 1)(x^3 + 1)$$
$$= (x-1)(x^2+x+1)(x+1)(x^2-x+1)$$

1 — periodo 1; $\zeta_2\ \zeta_4$ — 3 perché sono le radici terze di 1; -1 — 2; $\zeta_1\ \zeta_5$ — periodo 6

Oss: radici con lo stesso periodo stanno nello stesso fattore

Def: si chiama n-ESIMO POLINOMIO CICLOTOMICO

$$\Phi_n(x) = \prod_{(i,n)=1} (x - \zeta_i)$$

Oss: ζ_i ha ordine $n \iff (i,n) = 1$ [Ex].

Oss: ① $\deg \Phi_n(x) = \varphi(n)$

② $\Phi_p(x)$ con p primo? $\Phi_p(x) = 1 + x + \dots + x^{p-1} = \dfrac{x^p - 1}{x - 1}$

Fatto 1 $\Phi_n(x)$ ha coeff in $\mathbb{Z}[x]$ e è monico.

Dim

Per induzione su n. (estesa)

$$x^n - 1 = \prod (x - \zeta_i)$$

$$= \prod_{d \mid n} \Phi_d(x)$$

(Ex: pensarci bene)

$$= \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) \cdot \Phi_n(x)$$

↑

Per ehp induttiva $\Phi_d(x) \in \mathbb{Z}[x]$ $\forall d \mid n$ e monici

$\Rightarrow \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(x) \in \mathbb{Z}[x]$ ed è monico

Se divido poli a coeff interi per poli monico e coeff interi, ottengo poli a coeff interi.

(pensare a come si fa la divisione)

Quindi $\Phi_n(x)$ ha coeff interi ed è monico.

Ex: $z = \frac{3+4i}{5}$ può essere una radice di 1 per qualche n?

No!

Oss: $e^{i\theta}$ è radice di 1 se e solo se $\theta = p/q \cdot 2\pi$

(ex: scrivere perché)

Se fosse radice, $\{z^j\}_{j \in \mathbb{N}}$ sarebbe succ periodica.

Ma allora lo sarebbe in particolare $\mathrm{Re}(z^j) = \cos j\theta$

Allora $\{\cos j\theta\}_{j \in \mathbb{N}}$ sarebbe finito

$\cos\theta = \frac{3}{5}$, $\cos 2\theta = 2\cos^2\theta - 1 = 2 \cdot \frac{3^2}{5^2} - 1 = \frac{-7}{5^2}$

$\cos 4\theta = 2\cos^2 2\theta - 1 = 2\frac{7^2}{5^4} - 1 = \frac{2 \cdot 7^2 - 5^4}{5^4}$

Si vede che $\{\cos 2^j\theta\}$ ha potenze di 5 sempre + grandi

al denom.
Quindi la succ non assume un n° finito di valori.

D

Fatto: $\Phi_n(x)$ è irriducibile per ogni n

Dim:
[Ex: per n primo.
Idea: applicare Eisenstein a $\Phi_n(x+1)$]
↑ trucco

$n \in \mathbb{N}$.
Teorema: esistono infiniti primi $p \equiv 1 \ (n)$.

Dim:
Consideriamo $a \in \mathbb{N}$, p primo

$$p \mid \Phi_n(a)$$

$$p \nmid n$$

[Ex: vedere che a e p con queste proprietà esistono e sono ∞]

[Ruscitto: dato $f(x)$ polinomio non costante
$\{p : \exists x \in \mathbb{N} \ p \mid f(x)\}$ è infinito
Supponiamo sia finito. $\{p_1, \dots, p_m\}$.
Prendiamo $a_0 p_1 \cdots p_m \cdot 2$

$$f(a_0 p_1 \cdots p_m) = a_0 + a_1 a_0 p_1 \cdots p_m + \cdots + a_n a_0^n p_1^n \cdots p_m^n$$
$$= a_0 \left(1 + \underbrace{a_1 p_1 \cdots p_m + \cdots}_{\text{è divisibile per } p_1 \cdots p_m}\right)$$

$\Rightarrow$ è coprimo con $p_1 \cdots p_m$, quindi ha un altro fattore primo (se non è 1...)]

$n \in \mathbb{N}$.

Teorema: esistono infiniti primi $p \equiv 1 \ (n)$.

Dim:

Consideriamo $a \in \mathbb{N}$, p primo

$$p \mid \Phi_n(a)$$

$$p \nmid n .$$

$$a^n - 1 = \Phi_n(a) \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d(a) \equiv 0 \quad (p)$$

$$a^n \equiv 1 \ (p) \implies \operatorname{ord}_p a \mid n$$

Vediamo che $\boxed{\operatorname{ord}_p a = n}$. Potrebbe essere meno? ok

Chiamiamo $\operatorname{ord}_p a = k$. Sappiamo $k \mid n$.

$$a^k - 1 \equiv 0 \ (p).$$

$$p \mid \Phi_n(a) \mid \frac{a^n - 1}{a^{n/k} - 1} = 1 + a^k + a^{2k} + \dots + a^{(n/k - 1)k}$$

$$\equiv 1 + 1 + 1 \dots + 1$$

$$\equiv \frac{n}{k} \quad (p)$$

$$\not\equiv 0 \quad (\text{perché } p \nmid n)$$

Siccome $\operatorname{ord}_p a = n$, $n \mid p-1$, che è la tesi.

□