A1 MEDIUM

Titolo nota 04/09/2018

Anello = insieme su cui sono definiti +, −, *
Campo = " " " " , / (tranne che per 0)

ES: Anelli $\mathbb{Z}$, $\mathbb{Z}_n$, $A[x, y, \ldots]$
Campi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$

Se A anello posso considerare $A[x]$

- Funziona tutto bene, tranne se lavoro su $\mathbb{Z}_n$, con n non primo, perché ha divisori di zero:

es: $\mathbb{Z}_6$ $\quad 2 \cdot 3 = 0$

$$(2x+2)(3x-3) = 0$$

$$(2x^{17} + \ldots)(3x^{18} \ldots) = 0 \cdot x^{17+18}$$

$$\deg(fg) \neq \deg f + \deg g$$

$x^2 - 1$ in $\mathbb{Z}_{15}$ ha $-1, 1, 4, -4$ come radici

Su tutti gli altri anelli (e campi) visti, non ci sono divisori di zero, e si può sviluppare normalmente una teoria dei polinomi

Fattorizzazione unica: se $a(x) \mid f(x)\,g(x)$, allora:

- $a(x) \mid f(x)$
- $a(x) \mid g(x)$
- $a(x)$ si fattorizza in $a_1(x) \mid f(x)$ e $a_2(x) \mid g(x)$

Altro ⚠

$f(x) = g(x)$ come polinomi se $f_0 = g_0, \dots f_d = g_d$

$f(x) = g(x)$ come funzioni se $f(a) = g(a)$ $\forall a \in$ dominio

In $\mathbb{Z}_p[x]$, esistono f, g che sono diversi come polinomi ma uguali come funzioni:

$$x^p, \quad x$$

(Principio identità polinomi:

Teo: se due polinomi f, g di grado $\leq d$ sono tali che $f(x_i) = g(x_i)$ $x_1, x_2, \dots x_{d+1}$ punti distinti, allora $f(x) = g(x)$ come polinomi]

[ma non posso applicarlo perché in $\mathbb{Z}_p$ ho "solo" p punti distinti]

⚠ Principio di identità dei polinomi vale solo per polinomi in una variabile: esistono $f(x,y), g(x,y) \in \mathbb{R}[x,y]$

tali che esistono infinite coppie (x_i, y_i), $i = 0, 1, 2, \dots$

fatti che $f(x_i, y_i) = g(x_i, y_i)$ ma f, g diversi

ES: $f(x,y) = (y-x^2)(x^2+1)+1$

$g(x,y) = (y-x^2)(y^3-57x)+1$ $\circledast$

Tutte le coppie (n, n^2), $n \in \mathbb{N}$.

L'unica cosa che si riesce a dire è che

$$y-x^2 \mid f(x,y) - g(x,y)$$

Hint: guardali in $(\mathbb{R}[x])[y]$

$$g(x,y) = y^4 - x^2y^3 - 57xy + 1 + 57x^3$$

$g_4 = 1$, $g_3 = -x^2$, $g_2 = 0$, $g_1 = -57x$, $g_0 = 1+57x^3$

Vorremmo usare Ruffini: se dimostro che $p(a) = 0$, allora $(y-a) \mid p(y)$ $\quad a = x^2$

Devo dimostrare che $h(x, x^2) = 0$ in $\mathbb{R}[x]$ dove $h = f - g$.

$h(x, x^2)$ è un polinomio nella variabile x tale che valutandolo in $n \in \mathbb{N}$ fa zero $\Rightarrow$ è il polinomio $0 \in \mathbb{R}[x]$.

Quindi per Ruffini $(y-x^2) \mid f(x,y) - g(x,y)$

Lemma di Gauss: se $\underset{\in \mathbb{Z}[x]}{c(x)} = \underset{\in \mathbb{Q}[x]}{a(x)}\, \underset{\in \mathbb{Q}[x]}{b(x)}$, allora $\exists\, q \in \mathbb{Q}$ t.c. $q\,a(x), \; \frac{1}{q} b(x) \in \mathbb{Z}[x]$

ES: $x^2 - 4 = (3x+6)\left(\frac{1}{3}x - \frac{2}{3}\right)$

$= (x+2)\cdot(x-2)$

dim:

Lemma 2: se $\gamma(x) = \alpha(x)\beta(x)$, con $\alpha(x), \beta(x), \gamma(x) \in \mathbb{Z}[x]$,

e $p \mid \gamma_0, \gamma_1, \dots \gamma_{\deg \gamma}$, allora

$p \mid \alpha_0, \dots \alpha_{\deg \alpha}$ oppure $p \mid \beta_0, \beta_1, \dots \beta_{\deg \beta}$

dim: idea: considero $\overline{\gamma}(x)$ il polinomio "proiettato" su $\mathbb{Z}_p$, cioè $\overline{\gamma}_i$ è la classe di resto modulo p di γ_i

$$0 = \overline{\gamma}(x) = \overline{\alpha}(x)\,\overline{\beta}(x) \quad \text{in } \mathbb{Z}_p[x]$$

Su $\mathbb{Z}_p$ funziona annullamento del prodotto:
se $\overline{\alpha}(x)\overline{\beta}(x) = 0$, allora uno dei due dovrebbe essere 0

(per assurdo: $\overline{\alpha}(x) = \overline{\alpha}_n x^n + \dots \quad \overline{\beta}(x) = \overline{\beta}_m x^m + \dots$)

$$c(x) = a(x)\,b(x) = \frac{1}{A}\alpha(x)\;\frac{1}{B}\beta(x) \qquad \alpha, \beta \in \mathbb{Z}[x]$$

$\Updownarrow$

$$AB\,c(x) = \alpha(x)\beta(x)$$

$p \mid AB \Rightarrow p \mid$ tutti i coeff. di $\alpha(x)$ o di $\beta(x)$

$$\Rightarrow \frac{AB}{p} c(x) = \frac{\alpha}{p}(x)\beta(x)$$

... elimino un primo per volta... $c(x) = \underbrace{\frac{\alpha}{r}(x)}_{\in \mathbb{Z}[x]} \underbrace{\frac{\beta}{s}(x)}_{\in \mathbb{Z}[x]}$

Criterio di Eisenstein:

$a(x) \in \mathbb{Z}[x]$ di grado d tale che

$p \nmid a_d \quad p \mid a_{d-1}, \dots a_1, a_0 \quad p^2 \nmid a_0 \quad v_p(a_0) = 1$

Allora non esistono $b(x), c(x) \in \mathbb{Z}[x]$ (di grado $\neq 0$)

tali che $a(x) = b(x)c(x)$

e neppure in $\mathbb{Q}[x]$, per Gauss

Dim:

Proietto modulo p:

$$\overline{a}(x) = Kx^d \quad \text{con } K \neq 0 \text{ in } \mathbb{Z}_p$$

Se per assurdo $a(x) = b(x)c(x)$

$Kx^d = \overline{a}(x) = \overline{b}(x)\overline{c}(x)$ è una fatt. in $\mathbb{Z}_p[x]$

Per fatt. unica $\overline{b}(x) = K_1 x^{d_1}$, $\overline{c}(x) = K_2 x^{d_2}$

$d_1 + d_2 = d$

$d_1, d_2 \neq 0$

$$a(x) = (b_{d_1}x^{d_1} + \dots b_1 x + b_0)(c_{d_2}x^{d_2} + \dots + c_1 x + c_0)$$

$p \nmid b_0$ $\qquad$ $p \mid c_0$

$p^2 \mid a_0 = b_0 c_0$, assurdo.

Conseguenza di Eisenstein: $x^n - K$,
con $K \in \mathbb{Z}$ non quadrato perfetto, è irriducibile
in $\mathbb{Z}[x]$, $\mathbb{Q}[x]$

<u>OSS</u>: fattorizzare dà più informazioni che non
applicare $\quad b-a \mid p(b)-p(a)$ per $p \in \mathbb{Z}[x]$:

<u>es</u>: se $p \in \mathbb{Z}[x]$, $p(2)=p(4)=5$, quanto
può valere $p(0)$?

<u>Soluzione 1 (incompleta)</u>: $2-0 \mid p(2)-p(0) = 5-p(0)$

$\Rightarrow p(0)$ dispari

$4-0 \mid p(4)-p(0) = 5-p(0)$

$\Rightarrow p(0) \equiv 1 \ (4)$

<u>Soluzione 2</u>: $p(x)-5 = (x-4)(x-2)\,r(x)$ $\qquad r(x) \in \mathbb{Z}[x]$

$\Rightarrow p(0)-5 = -4 \cdot (-2) \cdot r(0)$

$\Rightarrow p(0) \equiv 5 \pmod 8$

(e si fanno tutti scegliendo r)

Congruenze modulo polinomi:

$$a(x) \equiv b(x) \pmod{m(x)} \iff m(x) \mid a(x) - b(x)$$

<u>Esempio</u>: voglio sapere il resto nella divisione

$$x^6 - x^3 + 1 = (x^2+1)\, q(x) + r(x)$$

Posso pensarlo così: lavoro mod x^2+1:

$-1 \equiv x^2$, quindi $\quad 1 \equiv x^4 \quad -1 \equiv x^6$

$$x^6 - x^3 + 1 \equiv -1 - x \cdot (-1) + 1 \equiv x.$$

<u>Altro esempio</u>:

Modulo $x+a$ $\qquad x \equiv -a$

$$x^{2n+1} \equiv -a^{2n+1} \Rightarrow x+a \mid x^{2n+1} + a^{2n+1}$$

(vero in $(\mathbb{R}[a])[x]$)

Altro esempio:

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

$$a+b+x \mid a^3+b^3+x^3-3abx$$

$x \equiv -a-b$, quindi $\qquad$ mod $a+b+x$

$$a^3+b^3+(-a-b)^3 - 3ab(-a-b) \equiv$$

$\equiv 0 \qquad \Rightarrow a+b+x \mid a^3+b^3+x^3-3abx.$

Altro trucco: "mettere l'altra radice"

$x^2-2 \qquad \pm\sqrt{2}$

ES: Quanto vale $\lfloor(\sqrt{2}+1)^{2018}\rfloor$ modulo 5?

Idea:

$$(\sqrt{2}+1)^{2018}+(-\sqrt{2}+1)^{2018} \quad \text{è razionale}$$

$$=\sum_{n=0}^{2018}\binom{2018}{n}(\sqrt{2})^n+\sum_{n=0}^{2018}\binom{2018}{n}(-\sqrt{2})^n=$$

$=$ (i termini con n dispari si semplificano) $=\sum_{n \text{ pari}} 2\binom{2018}{n}(\sqrt{2})^{2n}\in\mathbb{Q}$

Idea 2:

$a_n=(\sqrt{2}+1)^n+(-\sqrt{2}+1)^n$ soddisfa una certa relazione per ricorrenza:

pol. minimo $(x-1)^2=2$ $\qquad x^2-2x+1=2$

$x^2=2x+1$

Quindi la rel. per ricorrenza sarà $\underline{a_{n+1}=2a_n+a_{n-1}}$

$a_0=2$

$a_1=2$

Modulo 5, ho

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
2	2	1	-1	-1	2	3	3	-1

a_9	a_{10}	a_{11}	a_{12}	a_{13}
1	1	3	2	2

ciclica (si ripete ogni

$2018 \equiv 2 \pmod{12} \Rightarrow Q_{2018} \equiv Q_2 \equiv 1 \pmod 5$

$$(\sqrt{2}+1)^{2018} + (-\sqrt{2}+1)^{2018} \equiv 1 \pmod 5$$

$\overset{\shortparallel}{(-0.4142\ldots)^{2018}}$ positiva e molto piccola

$$(\sqrt{2}+1)^{2018} + \text{cosa positiva e molto piccola} \equiv 1 \pmod 5$$

$$\lfloor (\sqrt{2}+1)^{2018} \rfloor \equiv 0 \pmod 5$$

Altra variante di "mettici l'altra radice":
"mettici la parte immaginaria":

es: $\cos(15°) + \cos(30°) + \cos(45°) + \ldots + \cos(345°)$

reale $[\cos(15°) + \cos(30°) + \cos(45°) + \ldots + \cos(345°)$

immag. $[+ i\cdot\sin(15°) + i\cdot\sin(30°) + i\cdot\sin(45°) + \ldots + i\cdot\sin(345°) =$

$$= \exp\left(i\cdot\frac{\pi}{12}\right) + \exp\left(i\cdot\frac{2\pi}{12}\right) + \exp\left(i\cdot\frac{3\pi}{12}\right) + \ldots + \exp\left(i\frac{23}{12}\cdot\pi\right)$$

Progressione geometrica! $z + z^2 + \ldots + z^{23} = \dfrac{z - z^{24}}{1-z}$

con $z = \exp\left(i\frac{\pi}{12}\right)$

$$\mathrm{Re}\left(\frac{\exp\left(\frac{i\pi}{12}\right) - \exp\left(i\cdot\boxed{\frac{24}{12}}\pi\right)}{1 - \exp\left(\frac{i\pi}{12}\right)}\right) = \cos(15°) + \ldots + \cos(345°)$$

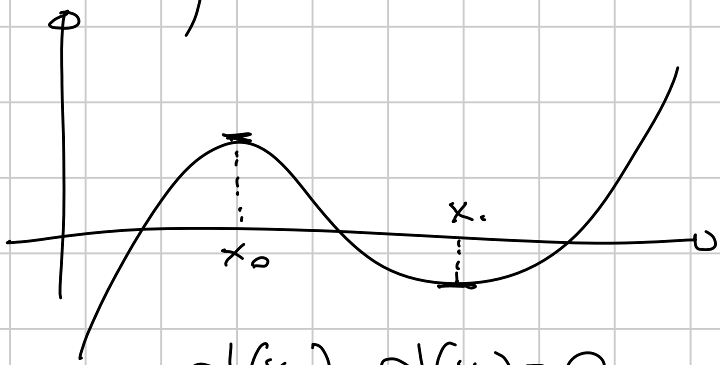
$$= \mathrm{Re}\left(\frac{\exp\left(\frac{i\pi}{12}\right)-1}{1-\exp\left(\frac{i\pi}{12}\right)}\right) = \mathrm{Re}(-1) = -1$$

<u>Derivata</u> di un polinomio:
coefficiente di h^1 nello sviluppo di $p(x+h)$

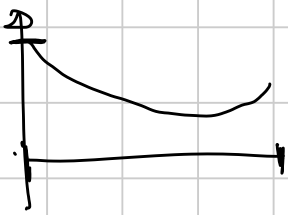
<u>es</u>: $p(x) = x^5$ $\quad p(x+h) = (x+h)^5 = x^5 + \underbrace{5x^4}_{\text{derivata}} h + \ldots$

$p'(x) = 5x^4$

(Risultato: se $p(x)$ ha un massimo/minimo locale in x_0
allora $p'(x_0) = 0$)



$p'(x_0) = p'(x_1) = 0$



<u>Teo</u>: se $q^2(x) \mid p(x) \in \mathbb{R}[x]$,
allora $q(x) \mid p'(x)$

(e quindi $q(x) \mid \mathrm{mcd}(p(x), p'(x))$)

CRITERIO DELLA DERIVATA

Regole calcolo derivate:

1) se $p(x) = x^n$, $p'(x) = n x^{n-1}$.

2) $(\alpha p(x) + \beta q(x))' = \alpha p'(x) + \beta q'(x)$. $(\alpha, \beta \in \mathbb{R})$

$\boxed{3}$) $(p(x) q(x))' = p(x) q'(x) + p'(x) q(x)$.

ES: $p(x) = x^3 + 4x + 2$ $\quad p'(x) = 3x^2 + 4 + 0$

$p''(x) = 6x \quad p'''(x) = 6$

$p''''(x) = 0$

$p'''''(x) = 0$

Dim. criterio derivata:

$p(x) = q(x)^2 r(x) = q(x) \cdot q(x) \cdot r(x)$

$$p'(x) = \underbrace{q'(x) q(x) r(x) + q(x) q'(x) r(x) + q(x) q(x) r'(x)}$$

tutti gli addendi sono multipli di $q(x)$ $\square$

Caso particolare: se $p(x)$ ha una radice doppia $p(x) = (x-\alpha)^2 q(x)$, allora $p'(x)$ ha la stessa radice α

(Generalizzazione: se $p(x)$ ha una radice di molteplicità K, allora hanno la stessa radice anche $p'(x), p''(x) \dots p^{\overbrace{''\dots'}^{K-1 \text{ volte}}}(x)$

ES: voglio fattorizzare $x^4 + 2x^3 - 3x^2 - 4x + 4 =: p(x)$

$p'(x) = 4x^3 + 6x^2 - 6x - 4$

$$\operatorname{mcd}(p, p') = \operatorname{mcd}(p', \underbrace{x^2+x-2}) = x^2+x-2$$

$$\begin{array}{l|l}
x^4 \quad 2x^3 \quad -3x^2 \quad -4x \quad 4 & 4x^3+6x^2-6x-4 \\
x^4+\frac{3}{2}x^3-\frac{3}{2}x^2-x & \hline \\
\hline
// \quad \frac{1}{2}x^3-\frac{3}{2}x^2-3x+4 & \frac{1}{4}x+\frac{1}{8} \\
\quad \frac{1}{2}x^3+\frac{3}{4}x^2-\frac{3}{4}x-\frac{1}{2} & \\
\hline
\quad // \quad -\frac{9}{4}x^2-\frac{9}{4}x+\frac{9}{2} &
\end{array}$$

$\Rightarrow p$ è multiplo di $(x^2+x-2)^2$

<u>Lemma:</u> $p(x)$, $p(x)+1$ hanno almeno $\deg p + 1$ radici distinte: (per tutti i p non costanti)

$$\Big|\{\text{radici di } p(x)\}\Big| + \Big|\{\text{radici di } p(x)+1\}\Big| \geq \deg p + 1$$

<u>dim:</u> criterio della derivata! Poniamo $n = \deg p$

Se $p(x)$ ha radici doppie, sono radici di $\operatorname{mcd}(p, p')$

Se $p(x)+1$ ha radici doppie, sono radici di $\operatorname{mcd}(p+1, p')$

(e queste sono distinte)

$$\#(\text{radici doppie di } p) + \#(\text{radici doppie di } p+1) \leq \underbrace{n-1}_{\substack{\uparrow \\ \text{grado della derivata}}}$$

$$p(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_k)^{m_k} \qquad \sum_i m_i = \sum_i n_i = n$$

$$p(x)+1 = (x-\beta_1)^{n_1}(x-\beta_2)^{n_2}\cdots(x-\beta_h)^{n_h}$$

$$p'(x) = (x-\alpha_1)^{m_1-1}(x-\alpha_2)^{m_2-1}\cdots(x-\alpha_k)^{m_k-1}\cdot$$
$$\cdot(x-\beta_1)^{n_1-1}(x-\beta_2)^{n_2-1}\cdots(x-\beta_h)^{n_h-1}$$
$$\cdot\, r(x)$$

$$n-1 \geq \underbrace{\sum_{i=1}^{k}(m_i-1)}\, + \sum_{i=1}^{h}(n_i-1) = n-k+n-h$$

$$\boxed{k+h \geq n+1.}$$

Teorema (teorema ABC o Mason-Stothers):

Se $a(x)+b(x)=c(x)$, e $\mathrm{mcd}(a,b,c)=1$

$a(x)b(x)c(x)$ ha almeno grado+1 radici distinte,

dove grado $=\max(\deg a, \deg b, \deg c) =: n$

(se a, b, c non sono tutti costanti)

Dim:
$$W = a'b - ab'$$

$\deg W \leq 2n-1$

Tra le radici di W ci sono le radici doppie di a e le radici doppie di b, e anche quelle di c, perché

$$ac' - a'c = a(\cancel{a'}+b') - a'(\cancel{a}+b) = -W.$$

(+ conto con le molteplicità). $\square$

Questo si usava in RMM 18:
Dire se esistono $p(x), q(x) \in \mathbb{R}[x]$ non costanti tali che $p(x)^{10} + p(x)^9 = q(x)^{21} + q(x)^{20}$.

<u>Modo 1</u>: $p^9(x)\big(p(x)+1\big) = q(x)^{20}\big(q(x)+1\big)$ $\;(*)$

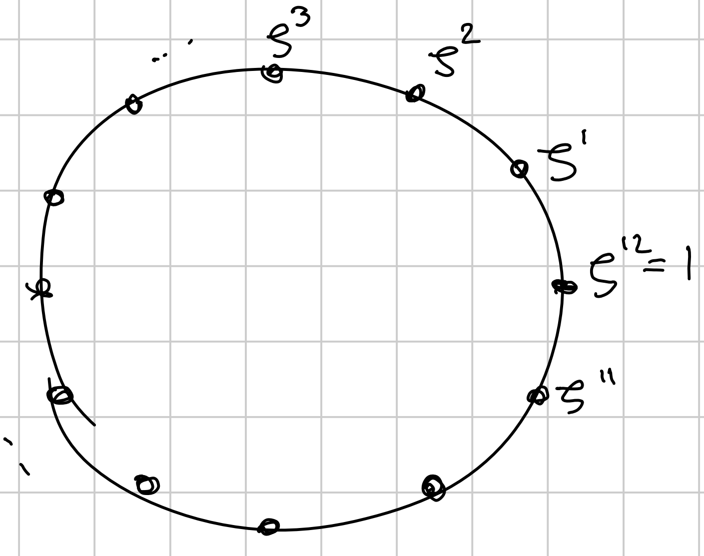
+ lemma di sopra + conti molteplicità.

<u>Modo 2</u>: Derivo la relazione:

$$9p^8(p+1)p' + p^9 p' = 20q^{19}(q+1)q' + q^{20}q' \quad (*)$$

+ combino le due $(*)$, conto gradi e arrivo a un assurdo.

<u>Ciclotomici</u>



$\zeta^2 \;\; (\zeta^2)^2 \;\; (\zeta^2)^3 \cdots (\zeta^2)^6 = 1$
$\Rightarrow \zeta^2$ <u>non</u> è primitiva

$\zeta^5 \;\; (\zeta^5)^2 \;\; (\zeta^5)^3 \cdots (\zeta^5)^{12} = 1$

$(\zeta^5)^{12}$ è il primo uguale a 1

ζ^5 è primitiva

ζ^k primitiva $\Leftrightarrow \mathrm{mcd}(k, 12) = 1$

Ci sono $\varphi(12)$ radici primitive.
Gli altri sono radici primitive di ordine un divisore di 12, per esempio ξ^2 è una radice sesta primitiva

$$x^{12}-1 = \underbrace{(x-\xi^1)(x-\xi^5)(x-\xi^7)(x-\xi^{11})}_{\text{radici 12-esime primitive}}\underbrace{(x-\xi^2)(x-\xi^{10})}_{\text{radici 6e primitive}}\underbrace{(x-\xi^4)(x-\xi^8)}_{\text{radici 3e prime}}\cdot$$

$$\cdot\underbrace{(x-\xi^6)}_{\text{radice 2p.}}\underbrace{(x-\xi^{12})}_{\text{radice 1°p.}}\underbrace{(x-\xi^3)(x-\xi^9)}_{\text{radici 4e primitive}}$$

$$(x+1)\quad(x-1)\quad(x-i)\quad(x+i)$$

$$\Phi_n(x) = \prod_{\substack{\xi \text{ radice n-esima} \\ \text{primitive di 1}}} (x-\xi)$$ ha grado $\varphi(n)$

$$x^n-1 = \prod_{d|n} \Phi_d(x)$$ (confrontando gradi, $n = \sum_{d|n} \varphi(d)$)

__Lemma__: i $\Phi_n(x)$ hanno tutti coeff. interi monici

__Dim__: induzione estesa: $$\Phi_n(x) = \frac{x^n-1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d(x)}$$

Dividendo per poli. monici a coeff. interi, il quoziente è a coeff. interi.

__Fatto__: sono irriducibili in $\mathbb{Q}[x]$ (e $\mathbb{Z}[x]$, per Gauss)

__Fatto__: per ogni $a\in\mathbb{N}$, i divisori primi di $\Phi_n(a)$ sono: $-\ p|n$

- $p \equiv 1 \pmod n$

Esempio di uso: teo: esistono infiniti primi congrui a 1 modulo n, per ogni n intero

Dim: supponiamo per assurdo siano finiti,

$p_1, p_2, \dots p_k$

$$\Phi_n(n p_1 p_2 \cdots p_k)$$

Φ_n ha termine costante $=1$, quindi $\Phi_n(np_1 \cdots p_k) \equiv 1 \pmod{p_i}$ e $\Phi_n(np_1 \cdots p_k) \equiv 1 \ (n)$

$\Rightarrow$ I suoi fattori primi sono "nuovi" primi $\equiv 1 \pmod n$, assurdo.

Def: un polinomio si dice polindromo se

$a(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$

$a_d = a_0$, $a_{d-1} = a_1$, $\dots$ $a_{d-k} = a_k$ ..

es. $3x^3 + 5x^2 + 5x + 3$

Lemma: i ciclotomici sono tutti polindromi

dim: (se ξ^k è primitivo, allora lo è anche ξ^{n-k} ..)

Lemma: $a(x)$ palindromico $\iff x^d \cdot a\left(\frac{1}{x}\right) = a(x)$

$$x^d a\left(\frac{1}{x}\right) = x^d\left(a_d \frac{1}{x^d} + a_{d-1}\frac{1}{x^{d-1}} + \dots + a_1 \frac{1}{x} + a_0\right)$$

$$= a_d + a_{d-1}x + \dots + a_1 x^{d-1} + a_0 x^d$$

Da questo segue che:

Lemma: se $a(x)$ palindromo e $a(\lambda)=0$, allora $a\left(\frac{1}{\lambda}\right) = 0$

e hanno anche la stessa molteplicità: segue da

$a(x) = (x-\lambda)\left(x-\frac{1}{\lambda}\right) b(x)$ con $b(x)$ palindromo

Un poly. palindromo di grado dispari ha la "radice speciale" -1.

$$ax^3 + bx^2 + bx + a = 0$$

I polinomi palindromi di grado pari si possono vedere come polinomi in $\left(x+\frac{1}{x}\right) = z$ (a meno di dividere per potenze)

ES: $\dfrac{ax^4 + bx^3 + cx^2 + bx + a}{x^2} = ax^2 + bx + c + b\frac{1}{x} + a\frac{1}{x^2} =$

$=$ polinomio in 1, $z = x + \frac{1}{x}$, $z^2 = x^2 + \frac{1}{x^2} + 2$

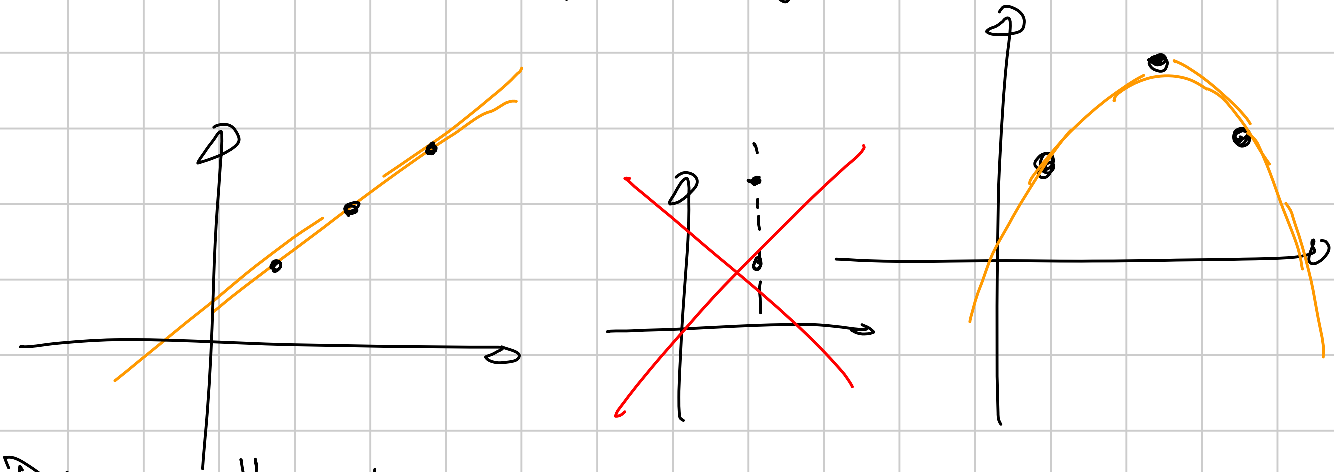
$= az^2 + bz + c - 2a$

(ES: trovare le radici di $x^4 + x^3 + x^2 + x + 1 = 0$)
$= \Phi_5(x)$

(Qualche volta si vedono anche polinomi tali che $a_k = -a_{d-k}$)

Interpolazione polinomiale (o di Lagrange):

<u>Teo</u>: date $n+1$ coppie $(x_1, y_1), (x_2, y_2) \dots$
$\dots (x_{n+1}, y_{n+1})$ in $\mathbb{K}^2$
con x_i distinti a due a due,
esiste uno e un solo polinomio di grado
$\leq n$ tale che $p(x_i) = y_i \ \forall i$



<u>Dim</u>: "Sistemone"

$$a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^n \\ 1 & x_2 & x_2^2 & \cdots & x_2^n \\ \vdots & & \vdots & & \\ 1 & x_{n+1} & x_{n+1}^2 & \cdots & x_{n+1}^n \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_{n+1} \end{bmatrix}$$

Vogliamo dire che la matrice

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^n \\ \vdots & & & \vdots \\ 1 & x_{n+1} & \cdots & x_{n+1}^n \end{bmatrix}$$

è invertibile, cioè che produce sistemi lineari con una e una sola soluzione (non importa il termine noto).

Ci basta considerare

$$\begin{bmatrix} 1 & x_1 & \cdots & x_1^n \\ \vdots & & & \vdots \\ 1 & x_{n+1} & \cdots & x_{n+1}^n \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \qquad (*)$$

e dire che ha solo la soluzione 0.

Interpreto le $(*)$ come condizioni su $b(x) = b_0 + b_1 x + \cdots + b_n x^n$

Ci dicono che $b(x_1) = b(x_2) = \cdots = b(x_{n+1}) = 0$.

$\Rightarrow b$ dev'essere il polinomio 0.

Strategie per costruire esplicitamente questo polinomio:

1. "sistemone" (Vandermonde)
2. "aggiusto un valore senza cambiare gli altri" (Lagrange)

Idea: trovo prima di tutto per ogni i un polinomio $L_i(x)$ tale che

$$L_i(x_1)=0,\ L_i(x_1)=0, \dots\ L_i(x_{i-1})=0,\ L(x_i)=1,$$
$$L_i(x_{i+1})=0 \dots\ L(x_{n+1})=0$$

$$L_i(x)=\frac{(x-x_1)(x-x_2)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)(x-x_{n+1})}{(x_i-x_1)(x_i-x_2)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_{n+1})}$$

Ora, $p(x)=\sum_{i=1}^{n+1} y_i L_i(x)$

$$p(x_k)=\sum_{i=1}^{n+1} y_i L_i(x_k)=y_k L_k(x_k)=y_k$$

$x_1=0,\ x_2=1,\ x_3=3$ $\qquad y_1=a \quad y_2=b \quad y_3=c$

$$L_1(x)=\frac{(x-1)(x-3)}{(0-1)(0-3)} \qquad \begin{cases} L_1(0)=1 \\ L_1(1)=0 \\ L_1(3)=0 \end{cases}$$

$$L_2(x)=\frac{x(x-3)}{(1-0)(1-3)} \qquad \begin{cases} L_2(0)=0 \\ L_2(1)=1 \\ L_2(3)=0 \end{cases}$$

$$L_3(x)=\frac{(x-0)(x-1)}{(3-0)(3-1)} \qquad \begin{cases} L_3(0)=0 \\ L_3(1)=0 \\ L_3(3)=1 \end{cases}$$

$$aL_1(x)+bL_2(x)+cL_3(x)$$

3) "aggiusto un valore per volta senza cambiare i precedenti" Newton

Parto prendendo un polinomio tale che $p(x_0)=y_0$, per esempio $p(x)=y_0$

Poi sommo una "correzione" che cambia valore in x_1 ma non in x_0:

$$y_0 + (x-x_0)\cdot\frac{y_1-y_0}{x_1-x_0}$$

Poi sommo "correzione" che cambia $p(x_2)$ ma lascia invariati $p(x_0), p(x_1)$

$$y_0+(x-x_0)\frac{y_1-y_0}{x_1-x_0} + (x-x_0)(x-x_1)\cdot\frac{y_2 - \dots\dots}{(x_2-x_0)(x_2-x_1)}$$

ES:

$p(0)=3 \quad p(1)=0 \quad p(3)=2$

$$3 + x\cdot(-3) + x(x-1)\cdot\left(\frac{8}{6}\right)$$

$p(0) \quad p(1) \quad p(2) \quad p(3) \quad p(4) \quad \dots\dots$

i coefficienti del metodo-Newton sono la prima colonna della tabella delle differenze finite