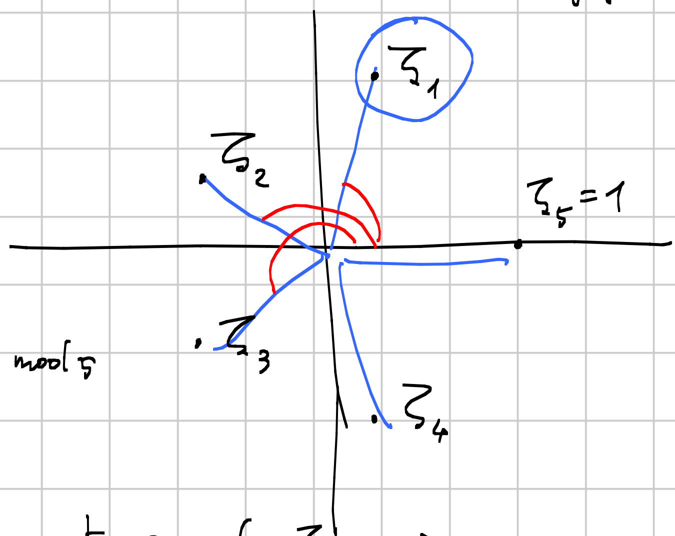
A 1 medio - Polinomi

Radici n-esime dell'unità $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/n\mathbb{Z}$

Su $\mathbb{C}$ ci sono sempre n radici n-esime dell'1 ai vertici di un n-agono regolare inscritto nella circonferenza di centro 0 e raggio 1.



$$\zeta_i \cdot \zeta_j = \zeta_{f(i,j)} = \zeta_{i+j \bmod 5}$$

Tutte le ζ_i sono potenze di $\zeta_1 \Rightarrow$

ζ_1 è $\boxed{\text{radice primitiva}}$

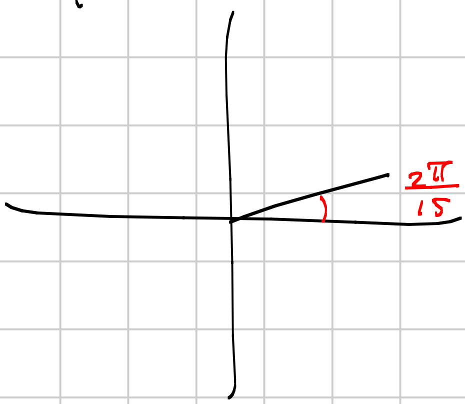
$\zeta_2^2 = \zeta_4 \quad \zeta_2^3 = \zeta_1 \quad \zeta_2^4 = \zeta_3 \quad \zeta_2^5 = \zeta_5 = 1 \qquad x^5 = 1$

Ma anche $\zeta_2, \zeta_3, \zeta_4$, non ζ_5

Le radici prim. di $x^5 = 1$ sono 4

" " $x^{15} = 1$ sono $\varphi(15)$

g^k è generatore $\Leftrightarrow (k, n) = 1$



Come si fattorizza $x^n - 1$? $(\mathbb{C})$

$n = 5 \cdot k$ $\quad (\zeta_1^k)^5 = 1 \quad \zeta_1^{2k} \neq 1 \quad \zeta_1^{3k} \neq 1 \quad \zeta_1^{4k} \neq 1$

ζ_1 è primitiva n-esima $\quad (\zeta_1^{\overset{n}{5k}})^2 = 1^2 = 1$

$x^5 - 1 = 0$

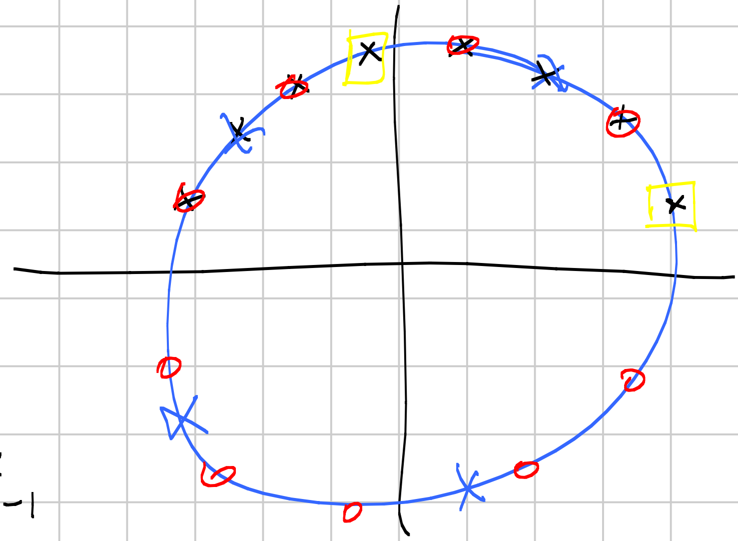
$x^n - 1 = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)\cdots(x - \lambda_n)$

$x^5 - 1 \mid x^n - 1$

$(x-1)(x^4 + x^3 + x^2 + x + 1)$

$n \quad d \mid n \quad x^d - 1 = q_1(x) \cdot q_2(x) \cdots q_k(x)$ allora

$q_i(x) \mid x^n - 1$



n ha divisori

$1, p_1, p_2, p_3, p_1^2, p_1 p_2, \dots, M$

$M =$ max divisore $< n$.

$x^{p_1} - 1 \quad x^{p_1^2} - 1 \quad x^{p_1 p_2} - 1 \quad x^M - 1$

Tutte le radici con ordine $< n$ sono radici di qualcuno dei $x^d - 1$ $\quad d \mid n \quad d < n$

$$x^n - 1 = \prod_{j=1}^{h} q_j(x) \cdot (x - \lambda_{i_1})(x - \lambda_{i_2}) \cdots (x - \lambda_{i_s})$$

$q_j(x) \mid x^d - 1 \quad d < n$

Teorema: $\prod(x - \lambda_i)$ con λ_i primitive è un polinomio a coefficienti razionali. E' il polinomio ciclotomico di grado n $\quad \Phi_n(x)$

$$x^p - 1 = (x-1)\Big(\underbrace{\sum_{i=0}^{p-1} x^i}_{=\Phi_p(x)}\Big)$$ $\Phi_p(x)$ è irriducibile su $\mathbb{Q}$

Perché? se $\Phi_p(x)$ fosse riducibile,

$\Phi_p(x) = a(x)\, b(x)$ con $\lambda_1, \dots, \lambda_m$ radici di $a(x)$
$\overline{\lambda_1}, \dots, \overline{\lambda_m}$ radici di $b(x)$

Però λ_1 è primitiva. $a(x) = x^m + b_{m-1}x^{m-1} + \dots + b_0$

$\lambda_1^m + b_{m-1}\lambda_1^{m-1} + \dots + b_0 = 0$

In queste condizioni, tutte le altre radici primitive dovrebbero anch'esse essere radici di $a(x)$

Perché $b_i \in \mathbb{Q}$ $(x-i)(x+i) = x^2+1$

$$\overline{x^2+1} = x^2+1$$
$$\overline{(x-i)}\,\overline{(x+i)} = (x+i)(x-i)$$

$\overline{z_1} + \overline{z_2} = \overline{z_1+z_2}$ $\overline{z_1}\cdot\overline{z_2} = \overline{z_1 z_2}$

Esistono "isomorfismi" che mandano $\lambda_1 \to \lambda_k$ per ogni λ_k primitiva e lasciano fisso $\mathbb{Q}$.

$a(x)$ $\lambda_1^m + b_{m-1}\lambda_1^{m-1} + \dots + b_0 = 0$

$\sigma : \lambda_1 \to \lambda_k$
$\sigma|_{\mathbb{Q}} = $ identità

$\sigma(a(x)) = a(x)$
$\shortparallel$
$a(\sigma(x))$

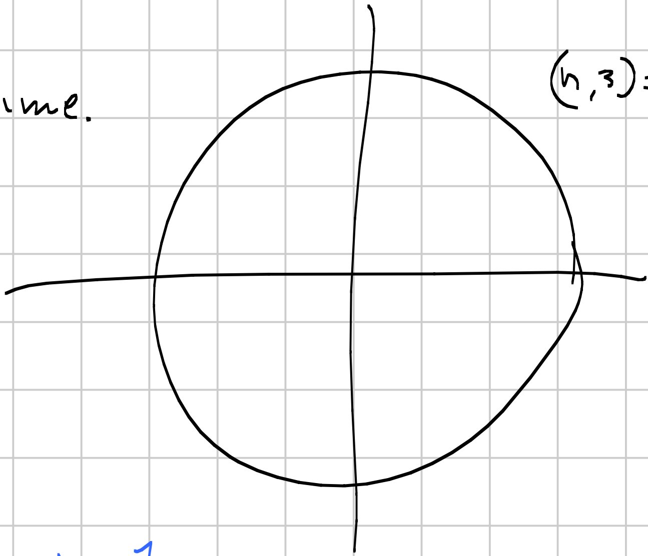
$\sigma(a(\lambda_1)) = \sigma(\lambda_1)^m + b_{m-1}\sigma(\lambda_1)^{m-1} + \dots + b_0$
$\shortparallel$
$\sigma(0) = 0$ quindi anche $\sigma(\lambda_1)$ è radice di a.

Corollario: $x^n - 1 = \prod_{d|n} \Phi_d(x) \longrightarrow n = \sum_{d|n} \varphi(d)$

$\deg \Phi_d(x) = \varphi(d)$

$\lambda_1 \dots \lambda_n$ radici n-esime.

$\sum_{i=1}^{n} \lambda_i^3$



$(n,3)=1$

$\lambda_i^3 = \lambda_j^3$

$\left(\left(\frac{\lambda_i}{\lambda_j}\right)^3 = 1\right) \qquad \left(\frac{\lambda_i}{\lambda_j}\right)^n = 1$

$(\ )^a \cdot (\ )^b = \left(\frac{\lambda_i}{\lambda_j}\right)^1 = 1 \Rightarrow \lambda_i = \lambda_j$

Se $(n,3)=1$ $\quad \lambda_i \to \lambda_i^3$ è iniettiva (e surg.) $\Rightarrow$

$\sum \lambda_i^3 = \sum \lambda_i = 0 \qquad x^n - 1$

Se $(n,3)=3$ l'immagine sono le radici $\frac{n}{3}$-esime

la controimmagine di ciascun λ_i raggiunto è fatta di 3 elementi $\Rightarrow \sum \lambda_i^3 = 3 \sum \bar{\lambda}_j$ $\quad \bar{\lambda}_j$ sono le radici $\frac{n}{3}$-esime. $\Rightarrow \sum \lambda_i^3 = 0$ a meno che $n=3$ nel qual caso fa 3.

$\mathbb{Z}/_{p\mathbb{Z}}$ $\quad p$ primo $\qquad x^n = 1 \qquad$ Ci sono $p-1$ classi di resto non nulle

$f_n : \mathbb{Z}/_{p\mathbb{Z}} \to \mathbb{Z}/_{p\mathbb{Z}}$

$a \mapsto a^n$

f_n è bigettiva se $(n, p-1) \iff$ esiste esattamente una radice.

$n = p-1 \qquad a^{p-1} \equiv 1 \pmod p \qquad p-1$ radici :

$x^{p-1} - 1 = (x-1)(x-2)(x-3) \cdots (x-(p-1))$

$n = kh \qquad (k, p-1) = 1 \qquad h$ ha solo fattori comuni con $p-1$

$x^n = 1 \qquad x^k = 1 \Rightarrow x = 1 \qquad x^h = 1$

$x^4+x^3+x^2+x+1$ dividiamo per x^2

$$x^2+x+1+\frac{1}{x}+\frac{1}{x^2}=0 \qquad y=x+\frac{1}{x}$$

$$y^2=x^2+2+\frac{1}{x^2} \qquad y^2+y-1=0$$

Non esiste formula risolutiva per grado ≥ 5

$p(x)$ con radici $\lambda_1 \dots \lambda_n$ $\quad \deg p(x)=n$.

$$p(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0$$

$$(-1)^i a_{n-i}=\sum_{\substack{i\text{-uple}\\ \text{ordinate}\\ \text{di indici}}} \lambda_{j_1}\cdot\lambda_{j_2}\cdot\ldots\cdot\lambda_{j_i} \qquad s_j=\sum_{i=1}^{n}\lambda_i^j \qquad j=1,\dots,n$$

$$\tilde{a}_i=(-1)^i a_i$$

Newton: $\quad k\,\tilde{a}_k=\sum_{i=1}^{k}(-1)^{i-1}\tilde{a}_{k-i}\,s_i \qquad \tilde{a}_1=s_1$

$$2\tilde{a}_2=-\tilde{a}_1 s_1+s_2$$

$$p(\lambda_j)=0 \qquad \begin{aligned}&\lambda_1^n+\dots+\dots+a_0=0\\ &\vdots\\ &\lambda_j^n+a_{n-1}\lambda_j^{n-1}+\dots+a_1\lambda_j+a_0=0\\ &\vdots\\ &\lambda_n^n+a_{n-1}\lambda_n^{n-1}+\dots+a_0=0\end{aligned}$$

$$\sum\lambda_i^n+a_{n-1}\sum\lambda_i^{n-1}+a_{n-2}\sum\lambda_i^{n-2}+\dots+n a_0=0$$

per $k=n$

$$r(i)=\sum \text{ monomi di grado } k \text{ con 1 incognita alla potenza } i$$
e le altre alla potenza 1

$s_i\cdot\tilde{a}_{k-i}$

$$(\ \ +\lambda_1^i+\ \ )\Big[\underbrace{(\lambda_2\cdots\lambda_{k-i+1})+\cdots}_{\text{non ha }\lambda_1}+\underbrace{\lambda_1\lambda_2\cdots\lambda_{k-i}+\cdots}_{\text{ha }\lambda_1}\Big]$$

$=\lambda_1^i\lambda_2\cdots\lambda_{k-i+1}+$ sta in $r(i)$

$\lambda_1^{i+1}\lambda_2\cdots\lambda_{k-i}$ sta in $r(i+1)$

i

$$s_i\cdot\tilde{a}_{k-i}=r(i)+r(i+1) \qquad i=k \quad \tilde{a}_0=1 \quad s_k$$

Non capita mai due volte lo stesso monomio

$$i=1 \Rightarrow k\tilde{a}_k + r(z)$$

$$\sum (-1)^{i-1} s_i \cdot \tilde{a}_{k-i} = k\tilde{a}_k - s_k$$

$p(x_1 \dots x_n)$ $\quad \sigma : \{1, \dots n\} \to \{1, \dots, n\}$ bigettiva

$\boxed{p \text{ è simmetrico}} \doteq p(x_1, x_2, \dots x_n) = p(x_{\sigma(1)}, \dots, x_{\sigma(n)})$
$\forall$ permutazione σ

$\dfrac{p(x)}{q(x)}$ con p e q simmetrici $\doteq$ $\boxed{\text{funzione razionale simmetrica}}$

Teorema: Ogni funzione raz. simmetrica è funz. razionale nelle funz. simm. elementari $\tilde{a}_1 \dots \tilde{a}_n$.

Dim. Qualunque sia il numero di variabili, il grado 1 va bene [Infatti basta farlo per i polinomi]

$a_1 x_1 + \dots + a_n x_n$ $\qquad a_1 = a_2 = \dots = a_n$

$\shortparallel$

$c \cdot (x_1 + \dots + x_n) = c \cdot \tilde{a}_1$

Induzione su grado e num. di variabili:

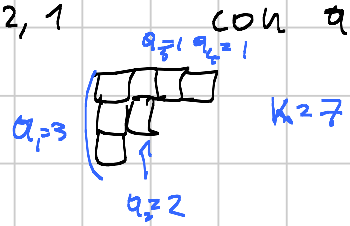
Supp. di saperlo per polinomi di grado $\leq K$, ma con meno variabili o per pol. di grado $< K$ con n variabili

$x_1 > x_2 > x_3 \dots > x_n$ $\qquad$ ordinamento lessicografico

Partizione di k: $a_1, \dots, a_n$ $\quad a_i > 0$ interi $\quad \sum_{i=1}^{n} a_i = k$

$k \qquad k-1, 1 \qquad k-3, 2, 1 \qquad$ con $a_1 \geq a_2 \geq a_3 \geq \dots \geq a_n$

Tabelle di Young:

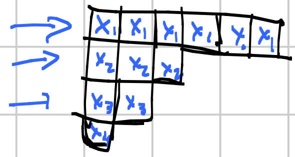


$\tilde{a}_1 \dots \tilde{a}_k$

In $p(x_1 \dots x_n)$ c'è un monomio di testa

$c \cdot x_1^{b_1} x_2^{b_2} \dots x_n^{b_n}$ sia il monomio più grande

Data $\pi = (a_1 \dots a_h)$ partizione, a_1



$$\tilde{a}_\pi(x_1 \dots x_n) = \prod_{i=1}^{h} \tilde{a}_{a_i}$$

$$\deg \tilde{a}_\pi = \sum a_i = k$$

Qual è il termine di testa di $\tilde{a}_\pi$?

In $\tilde{a}_{a_1}$ c'è $x_1 \cdot x_2 \cdot \dots \cdot x_{a_1}$ ed è il suo termine di testa

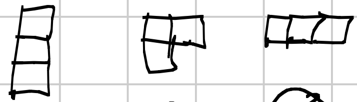
Il mon. di testa di $\tilde{a}_\pi$ è il prodotto dei monomi di testa

Viene $x^\pi \quad x_1^{a_1} \cdots x_h^{a_h}$

$p(x) - c \prod_\pi \tilde{a}_{a_i}$ ha un monomio di testa più piccolo.

Posso finire per induzione

$p(x_1 x_2 x_3) = x_1^3 + x_2^3 + x_3^3$



$x_1 x_2 x_3 \qquad \underline{x_1^2 x_2} \qquad x_1^3$

$p(x_1, x_2, x_3) - \tilde{a}_1^3 =$

$- 3\sum_{sym} x_1^2 x_2 + 6 x_1 x_2 x_3 \qquad 3 x_1^2 x_2$

$p - \tilde{a}_1^3 + 3 \tilde{a}_1 \tilde{a}_2 = 3 x_1 x_2 x_3 = 3 \tilde{a}_3$

$S_3 = \tilde{a}_1^3 - 3 \tilde{a}_1 \tilde{a}_2 + 3 \tilde{a}_3$.

$S_3 - 3\tilde{a}_3 = \tilde{a}_1 (\tilde{a}_1^2 - 3 \tilde{a}_2) =$

$\underline{a^3 + b^3 + c^3 - 3abc}$

$= (a+b+c)\ \underline{(a^2+b^2+c^2-ab-ac-bc)}$

$p(a) \qquad a = -b-c$

$a^3 = -b^3 - c^3 - 3b^2c - 3bc^2$

$a - (-b-c)$

$-3abc = +3b^2c + 3bc^2$

$a^3 + b^3 + c^3 - 3abc = 0$

$(a+b+c)$

Sophie Germain: $a^4 + 4b^4 = (a^2 + 2ab + 2b^2)(a^2 - 2ab + 2b^2)$

$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$

$$(a^2+b^2)(c^2+d^2) = (ad-bc)^2+(ac+bd)^2 =$$
$$= (ad+bc)^2+(ac-bd)^2$$

Polinomi a coeff. interi

Lemma di Gauss: $p(x)$ a coeff. interi monico
se $p(x)$ si scompone come $a(x).b(x)$ sui razionali,
si scompone anche a coeff. interi

Dim. $p(x) = \sum a_i x^i$ $\quad$ $c_p(p(x))$ = max potenza di p
$a_i \in \mathbb{Q}$ $\quad$ contenuta in tutti gli a_i

$$c(p(x)) = \prod_p c_p(p(x))$$

$$c(p(x).q(x)) = c(p(x)).c(q(x))$$

$c_p(p(x)) = p^k$ $\quad$ Il coeff. che ha p^k con grado
più alto sia $\bar{a}$
$c_p(q(x)) = p^h$ $\quad$ " " " " "
$\bar{b}$

In $p(x)\,q(x)$ c'è $\bar{a}.\bar{b}$

$p(x)$ $\quad$ $c(p(x))$ è intero.
$\shortparallel$
$a(x).b(x)$ $\quad$ $c(a(x))$ e $c(b(x))$ sono razionali
con prodotto intero. $(\Rightarrow 1)$

$\dfrac{a(x)}{c(a(x))}$ e $\dfrac{b(x)}{c(b(x))}$ sono a coeff. interi e il prodotto è $p(x)$
$\square$.

Criterio di Eisenstein:
$p(x)$ pol. a coeff. interi, monico
$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$ $\quad$ e $\quad$ p primo
$p \mid a_{n-1}$, $p \mid a_{n-2}$, ... $p \mid a_1$, $p \mid a_0$, ma $p^2 \nmid a_0$
<u>allora</u> p è irriducibile (su $\mathbb{Z}$)

Dim. $a(x)\cdot b(x)$ a,b monici, si cerca un coeff. non multiplo di p, ma non c'è.

$x^4+x^3+x^2+x+1$ $\left(o \ \frac{x^p-1}{x-1}\right)$ p primo sono irriducibili.

$x \to y+1$ $\qquad y^4+5y^3+\cdots+5$

multipli di 5

$p(x) = a_n x^n + a_{n-1}x^{n-1}+\cdots+a_0$

1) a_0 è primo

2) $|a_0| > \sum_{i=1}^{n} |a_i|$ $\Rightarrow$ $p(x)$ è irriducibile.

Dim. 1) $p(x)=a(x)\cdot b(x)$ $\Rightarrow$ il termine noto di a è p o $-p$ quello di b è 1 $(o -1)$ a meno di scambiarli

2) allora b ha una radice complessa z_1 con $|z_1| \leq 1$. Ma z_1 è anche radice di $p(x)$

$a_n z_1^n + a_{n-1}z_1^{n-1}+\cdots+z_1 a_1 + a_0 = 0$

ma $|z_1^k|<1$ $\quad k=1,\dots,n$ $\qquad$ quindi

$|a_0| = |a_n z_1^n + a_{n-1}z_1^{n-1}+\cdots+z_1 a_1| < |\sum |a_i|| < a_0$ per ip.

se $p(x)$ ha coeff interi, $a,b \in \mathbb{Z}$

$a-b \mid p(a)-p(b)$. $\qquad$ v. probl. 1 del Test iniziale.

$p(\bar{x}) \mid q(\bar{x})$ per infiniti valori $\bar{x} \in \mathbb{Z}$.

Allora $p(x) \mid q(x)$.

Dim. $q(x) = p(x)\cdot a(x) + r(x)$.

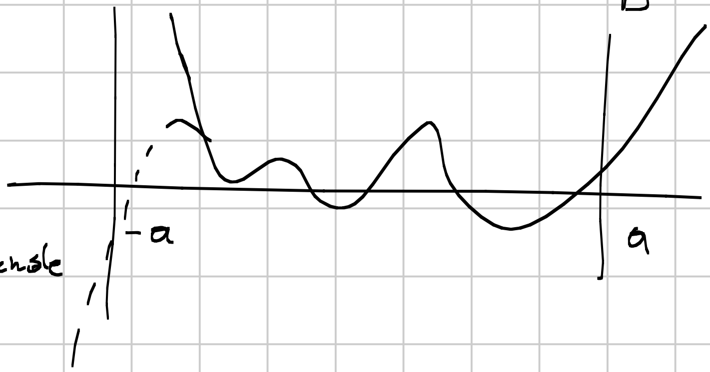
$\frac{q(x)}{p(x)} = a(x) + \frac{r(x)}{p(x)}$. $\qquad \frac{r(x)}{p(x)}$ è intero per ∞ x.

ma $\deg r(x) < \deg p(x)$ $\Rightarrow$ $|p(x)|>|r(x)|$ per

$|x| > M \Rightarrow$ al di fuori, $r(x)$ vale 0 ∞ volte

$\Rightarrow r(x) \equiv 0$.

$\square$



$p(x)$ ha grado n,

quanti sono i $k \leq N$ grande nell'imm. di $p(x)$?
(in "percentuale")

$$p(x+1) - p(x) \quad \text{per } x > 0$$

$\parallel$

è pol. di grado $n-1$ $\Rightarrow$ $n > 1$

$$|p(x+1) - p(x)| \longrightarrow \infty$$

$$\sim c \cdot x^{n-1}$$

Quindi la quantità cercata è $\sim \sqrt[n]{N}$

$p(x)$ è intero $\forall x \in \mathbb{Z} \Rightarrow p(x)$ ha coeff. interi?

$$\frac{x^2+x}{2}$$

i) grado 1, 0
- 0: costante intera, sì
- 1: sì.

grado 2: $p(x+1) - p(x)$ ha grado 1 ed è sempre intero.

$$p(x+1) - p(x) = \underbrace{nx+m}_{} \quad n, m \in \mathbb{Z}?$$

$\updownarrow$

coeff. binomiali. $\qquad \binom{x}{k} = \dfrac{x(x-1)(x-2)\cdots(x-k+1)}{k!}$

$$p(x+1) - p(x) = \binom{x}{k} \quad \Rightarrow \quad p(x) = \binom{x}{k+1}$$

$$nx + m \qquad \binom{x}{1} = x \qquad \binom{x}{0} = 1$$

$$nx + m = n\binom{x}{1} + m\binom{x}{0}$$

$$p(x) = n\binom{x}{2} + m\binom{x}{1} = n \cdot \frac{x(x-1)}{2} + m x$$

$p(x)$ grado k $\quad a_k\binom{x}{k} + a_{k-1}\binom{x}{k-1} + \dots + a_1\binom{x}{1} + a_0\binom{x}{0}$

den $\mid k!$

Polinomi per $n+1$ punti

$(x_0, y_0) - \dots (x_n, y_n)$

$$p(x) = \sum_{i=0}^{n} y_i \cdot \ell_i(x) \qquad \boxed{\begin{array}{l} \ell_i(x_j) = 0 \\ \ell_i(x_i) = 1 \end{array}} \quad i \neq j$$

$$\ell_i(x) = \prod_{\substack{j=1 \\ j \neq i}}^{n} \frac{x - x_j}{x_i - x_j}$$

$p(x)$ a coeff. interi.

$p_2(x) = p(p(x)) \qquad p_3(x) = p(p(p(x)))$

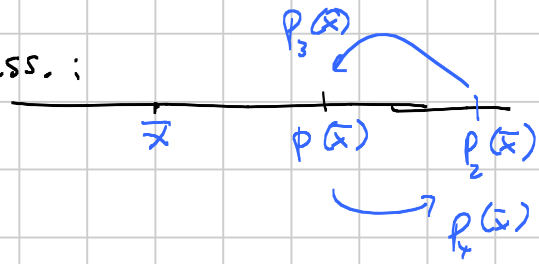
$p_{k+1}(x) = p(p_k(x)) \qquad \exists\, \bar{x} \in \mathbb{Z}$ t.c. $p_n(\bar{x}) = \bar{x}$, $n \in \mathbb{N}$

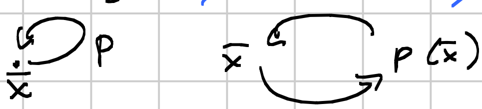
Allora $p(\bar{x}) = \bar{x}$ o $p_2(\bar{x}) = \bar{x}$.

$$p(\bar{x}) - \bar{x} \mid p(p(\bar{x})) - p(\bar{x}) \mid p_3(\bar{x}) - p_2(\bar{x}) \mid \dots \mid p_n(\bar{x}) - p_{n-1}(\bar{x}) \mid p_{n+1}(\bar{x}) - p_n(\bar{x}) = p(\bar{x}) - \bar{x}$$

$$\Rightarrow \begin{cases} p_2(\bar{x}) - p(\bar{x}) = p(\bar{x}) - \bar{x} \\ p_2(\bar{x}) - \cancel{p(\bar{x})} = \bar{x} - \cancel{p(\bar{x})} \end{cases}$$

ass.:





8 : 0 1 2 3 4 5 6 7 $\qquad 1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod 8$

non c'è generatore (radice primitiva 2^a di 1)

p^k p dispari.

$2, 4$

$p^k, 2\cdot p^k$

$x^{p^k}-x$ $\pmod p$ è prodotto di tutti i polinomi irriducibili di grado che $| k$.

Su $\mathbb{R}$	grado 1 e 2	irriduc.
$\mathbb{C}$	grado 1	
$\mathbb{Q}$	tutti i gradi	
$\mathbb{Z}/p\mathbb{Z}$	tutti i gradi	x^p+x-a
		x^n-a