① $P(x) = a_0 + a_1 x + \dots + a_d x^d \in \mathbb{Z}[x]$

- a_0 primo
- $|a_0| > |a_1| + \dots + |a_d|$

Allora $P(x)$ IRRIDUCIBILE

② $P(x), Q(x) \in \mathbb{Z}[x]$ $\quad P(n) \mid Q(n)$ per ∞ $n \in \mathbb{Z}$

Allora $P(x) \mid Q(x)$

③ $P(x) \in \mathbb{Z}[x]$ $\rightarrow$ deg (P) pari

$\rightarrow$ monico

Supponiamo $P(n) = \square$ perfetto per ∞ $n \in \mathbb{Z}$

Allora $P(x) = Q(x)^2$ con $Q(x) \in \mathbb{Z}[x]$

Le due ipotesi servono davvero

④ $P(x) \in \mathbb{R}[x]$. Allora $P(P(P(x))) - x$ è divisibile per $P(x) - x$.

$\boxed{1}$ $P(x) = Q(x) \cdot R(x)$

wlog $|q_0| = 1$

$\rightsquigarrow$ $Q(x)$ ha almeno una radice $\alpha \in \mathbb{C}$ con $|\alpha| \leq 1$

$\rightsquigarrow$ anche $P(x)$ " "

$$a_0 + a_1 \alpha + \dots + a_{d-1} \alpha^{d-1} + a_d \alpha^d = 0$$

troppo grande

$$0 = |a_0 + \dots| \geq |a_0| - |a_1| \cdot |\alpha| - \dots - |a_d| \cdot |\alpha|^d$$

$$\geq |a_0| - |a_1| - \dots - |a_d| > 0$$

$\boxed{2}$ $Q(x) = P(x) \cdot A(x) + R(x)$

$\uparrow$ $\deg R < \deg P$

$\rightsquigarrow \dfrac{Q(x)}{P(x)} = A(x) + \dfrac{R(x)}{P(x)}$

$$\underbrace{\frac{Q(n)}{P(n)}}_{\text{intero}} = \underbrace{A(n)}_{\text{intero}} + \frac{R(n)}{P(n)}$$

anche questo è intero ma è molto piccolo per n grande, quindi è $= 0$

$\rightsquigarrow R(x)$ si annulla ∞ volte $\rightsquigarrow R(x) \equiv 0$.

$\boxed{3}$ $\boxed{\text{Step 1}}$

$$P(x) = x^{2d} + p_{2d-1} x^{2d-1} + p_{2d-2} x^{2d-2} + \dots$$

$$Q(x) = x^{d} + q_{d-1} x^{d-1} + q_{d-2} x^{d-2} + \dots$$

Impongo $P(x) = Q(x)^2$ e cerco i coeff.

$\rightsquigarrow$ $2 q_{d-1} = p_{2d-1}$ $\rightsquigarrow$ trovo q_{d-1}

$2 q_{d-2} + q_{d-1}^2 = p_{2d-2}$ $\rightsquigarrow$ trovo q_{d-2}

In questo modo li trovo fino a q_0 e ottengo

$$P(x) = Q(x)^2 + R(x)$$

$\uparrow$ $\deg R \leq d-1$

$\boxed{\text{Step 2}}$ $\underbrace{P(n)}_{\square} = \underbrace{Q(n)^2}_{\square} + R(n)$

$\rightsquigarrow R(n)$ è "abbastanza grande" cioè $|R(n)| \geq 2|Q(n)| - 1$

$\uparrow$ non può essere vera per n grande per ragioni di grado

$\rightsquigarrow R(n) = 0$ per n grande

$\rightsquigarrow R(x) \equiv 0$.

$\boxed{\text{Step 1.5}}$ A priori sappiamo solo che $Q(x) \in \mathbb{Q}[x]$

Si aggiusta (lascio i dettagli) come nel Lemma di Gauss.

$\boxed{4-1}$ Congruenze mod $Q(x) = P(x) - x$

$P(x) \equiv x \pmod{Q(x)}$

$\leadsto P(P(x)) \equiv P(x) \equiv x \pmod{Q(x)}$

e così via ☺

<u>Lemma</u> $A(x) \equiv B(x) \pmod{Q(x)}$

Allora $P(A(x)) \equiv P(B(x)) \pmod{Q(x)}$

[Ovvio per le potenze perfette, poi si estende]

$\boxed{4-2}$ Basta dim. che le radici di $P(x) - x$ sono anche radici di $P(P(P(x))) - x$

Questo è ovvio se le radici hanno molteplicità 1, per le radici con molteplicità è più delicato

Si potrebbe derivare r abbia molteplicità 2:

$P(r) - r = 0$ $\qquad P'(r) - 1 = 0$

$P(P(r)) - r = 0$ $\qquad [P(P(x)) - x]' = P'(P(x)) \cdot P'(x) - 1$

se metto $x = 0$ viene $\qquad P'(r) \cdot P'(r) - 1 = 0$

(5) $P(x) \in \mathbb{Z}[x]$. Sia $a \in \mathbb{Z}$ t.c. $P^{(2024)}(a) = a$

$P(P(P\ldots)))$

Allora $P(P(a)) = a$.

(6) $P(x) \in \mathbb{Z}[x]$. L'insieme dei primi che dividono $P(n)$ per un qualche n è infinito.

intero

(7) $P(x) \in \mathbb{R}[x]$. Trovare $M \in \mathbb{R}$ (effettivo, quindi in funzione dei coeff. di $P(x)$) tale che

$$x \in \mathbb{R} \text{ e } P(x) = 0 \implies |x| \leq M$$

(8) Cartesio. Sia $P(x) \in \mathbb{R}[x]$.
Allora le radici reali positive di $P(x)$ sono $\leq$ del numero delle variazioni di segno tra i coeff. di $P(x)$, escludendo quelli nulli.
Inoltre i 2 numeri hanno la stessa parità.

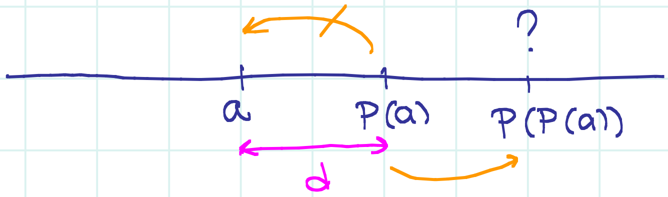
(9) Caratterizzare tutti i $P(x) \in \mathbb{R}[x]$ o in $\mathbb{Z}[x]$ t.c.

$$P(x) = P(2023 - x) \qquad \forall x \in \mathbb{Z}.$$

$\boxed{5}$ $b-a \mid P(b)-P(a)$ $\qquad b = P(a)$

$P(a)-a \mid P(P(a))-P(a) \mid P^{(3)}(a) - P^{(2)}(a)$ e così via

Quindi $|P^{(k+1)}(a) - P^{(k)}(a)| = d$ fisso



$\boxed{6.1}$ Se i primi coinvolti sono solo $p_1, \dots, p_k$, allora provo a scegliere

$$n = p_1 \cdot \ldots \cdot p_k \cdot \text{termine noto}$$

$\boxed{6.2}$ • Quanti numeri $k \in \mathbb{Z}$ con $|k| \leq M$ sono valori assunti dal polinomio?

$\sim \sqrt[d]{M}$ con d = grado

• Quanti ... contengono meno di ℓ primi fissati?

Gli esponenti sono $\leq \log_2 M$

Quindi sono $\leq (\log_2 M)^\ell$

Si conclude osservando che $\sqrt[d]{M} >> (\log_2 M)^\ell$ per M grande

$\boxed{7}$ Idea: se $|x|$ è "grande", allora $|x|^d$ si "mangia" tutto il resto

$$|P(x)| = |a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0|$$

$$\geq |a_d| \cdot |x|^d - |a_{d-1}| \cdot |x^{d-1}| - \ldots - |a_1| \cdot |x| - |a_0|$$

$$= |x|^d \underbrace{\left\{ |a_d| - \frac{|a_{d-1}|}{|x|} - \ldots - \frac{|a_0|}{|x|^d} \right\}}_{>0}$$

se $\quad |x| \geq \max\{|a_{d-1}|, \dots, |a_0|, 1\} \cdot (d+1)$

$\boxed{9}$ $Q(x) = P\left(\frac{2023}{2}+x\right) \rightsquigarrow Q(x) = Q(-x)$

$\rightsquigarrow Q(x) = A(x^2)$

$$\rightsquigarrow P(x) = A\left(\left(x-\frac{2023}{2}\right)^2\right) = B(x(2023-x))$$

$$\parallel$$

$$A\left(x^2-2023x+\frac{2023^2}{4}\right)$$

—o—o—

$\boxed{\text{IMO } 1993\_1}$ $x^n+5x^{n-1}+3$ è irriducibile in $\mathbb{Z}[x]$.

$\boxed{\text{IMO } 2002\_3}$ Trovare (m,n) t.c.

$$\frac{a^m+a-1}{a^n+a^2-1} \in \mathbb{Z} \quad \text{per infiniti } a \in \mathbb{Z}$$

[Due casi da trattare: $m \geq 2n$ e $m \leq 2n-1$]

$$x^n+x^2-1 \mid x^m+x^{m-n+2}-x^{m-n}$$
$$x^n+x^2-1 \mid x^m+x-1$$

$$\rightsquigarrow x^n+x^2-1 \mid x^{m-n+2}-x^{m-n}-x+1$$

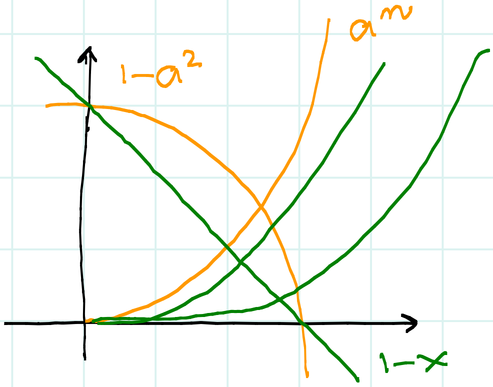
$\rightsquigarrow n \leq m-n+2 \rightsquigarrow m \geq 2n-2$

$\rightsquigarrow$ sostituisco i 2 valori

$\boxed{m=2n-1}$ $x^n+x^2-1 \mid \cancel{x^{n+1}}-x^{n-1}\cancel{-x}+\cancel{1}$

$$(x^n+x^2-1)(x-1) = \cancel{x^{n+1}}-x^n+x^3-x^2\cancel{-x}+\cancel{1}$$

$\boxed{m=2n-2}$ $x^n+x^2-1 \mid x^n-x^{n-2}-x+1 \rightsquigarrow$ NO BUONO



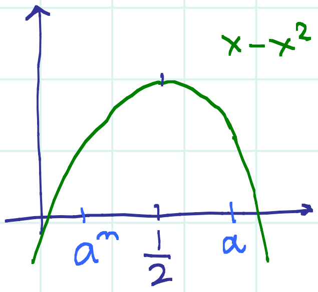
Idea: se $m=2n$, l'incrocio verde è a dx dell'incrocio arancio

Quindi

$$a^{2n}+a-1 < a^n+a^2-1$$

$a - a^2 < a^n - a^{2n}$ $f(a) < f(a^n)$ con $f(x) = x - x^2$

$\frac{1}{2} < a^n < a < 1$



Basta che $a^n + a > 1$

Ma sappiamo che $a^n + a^2 = 1$

e quindi

$1 = a^n + a^2 < a^n + a$ ☺

— o — o —

(a) $A(x)$ e $B(x)$ in $\mathbb{R}[x]$ $\deg(A) > \deg(B)$

$n A(x) + B(x)$ ha almeno una radice reale per ∞ n interi

Allora $A(x)$ ha almeno una radice reale

(b) ... in $\mathbb{Z}[x]$ ...

$p A(x) + B(x)$ ha almeno una radice $\in \mathbb{Q}$ per ∞ p primi

Allora $A(x)$ ha almeno una radice $\in \mathbb{Q}$.

(a) $A(x) + \frac{1}{n} B(x) = 0$ Supponiamo abbia radice x_k per $n_k \to +\infty$

$\boxed{\text{Step 1}}$ $\exists\, M \in \mathbb{R}$ t.c. $|x_k| \leq M$ (bound effettivo)

$\boxed{\text{Step 2}}$ A meno di sottosuccessioni $x_k \longrightarrow x_\infty \in [-M, M]$

$\boxed{\text{Step 3}}$ $A(x_\infty) = 0$

$$0 = A(x_k) + \underbrace{\frac{1}{n_k} B(x_k)}_{\downarrow\, 0} \longrightarrow A(x_\infty)$$

(b) $\frac{k}{p}$ radice di $\quad pA(x) + B(x)$ $\qquad A(x) = x^d + a_{d-1}x^{d-1} + \dots$

$$B(x) = \underset{\substack{\uparrow \\ \text{anche } = 0}}{b_{d-1}} x^{d-1} + \dots$$

$$pA\left(\frac{k}{p}\right) + B\left(\frac{k}{p}\right) = \cancel{p} \cdot \frac{k^d}{p^{d-1}} + p\, a_{d-1} \frac{k^{d-1}}{p^{d-1}} + b_{d-1} \frac{k^{d-1}}{p^{d-1}}$$

+ roba con meno p al denom.

Molt. per p^{d-1} : $p \mid k^d + b_{d-1}k^{d-1} = k^{d-1}(k + b_{d-1})$

$$\Rightarrow \quad p \mid k + b_{d-1} \qquad\qquad k + b_{d-1} = M_p p$$

$$\Rightarrow \quad \frac{k}{p} = M_p - \frac{b_{d-1}}{p}$$

$\rightsquigarrow$ M_p è limitato $\rightsquigarrow$ costante su una s. succ.

$$A\left(M - \frac{b_{d-1}}{p}\right) + \frac{1}{p} B\left(M - \frac{b_{d-1}}{p}\right) = 0$$

$$\rightsquigarrow \quad A(M) = 0$$