Alg. Lin. 7/10/15

2.3.3 $x^2 = p$ non ha soluz. in $\mathbb{Q}$ se $p > 2$ è primo

"$\sqrt{p} \notin \mathbb{Q}$"

P.a. sia $\frac{n}{m}$ soluz. n, m primi tra loro.

$\left(\frac{n}{m}\right)^2 = p \Rightarrow n^2 = p \cdot m^2 \Rightarrow p$ divide n^2

$\Rightarrow p$ divide $n \Rightarrow n = pk$

$\Rightarrow p^2 \cdot k^2 = p \cdot m^2 \Rightarrow m^2 = p \cdot k^2 \Rightarrow p$ divide m^2

$\Rightarrow p$ divide m : Assurdo n, m hanno il fattore comune p.

2.3.4 $\mathcal{P}(S) = \{$tutti i sottoinsiemi di $S\}$.

$\mathcal{P}(\{a,b,c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}$

3 — $8 = 2^3$

Se S ha n elementi allora $\mathcal{P}(S)$ ha 2^n.

Per induzione: $n = 0$ $S = \emptyset$, $\mathcal{P}(S) = \{\emptyset\}$

$\Rightarrow 2^0 = 1$ el.

$n = 1$ $S = \{a\}$ $\mathcal{P}(S) = \{\emptyset, \{a\}\}$

$\Rightarrow 2^1 = 2$ el.

P.I: Supponiamo che $\mathcal{P}(S)$ abbia 2^n el. per S con n elem. Devo vedere che se T ha $n+1$ el. allora $\mathcal{P}(T)$ ne ha 2^{n+1}.

Scelgo $t_0 \in T$ e pongo $S = T \setminus \{t_0\}$.

$$\mathcal{P}(T) = \mathcal{P}(S) \cup \{ A \cup \{t_0\} : A \in \mathcal{P}(S) \}$$

elenco senza ripetizioni

$$\Longrightarrow 2^n + 2^n = 2^{n+1} \quad \text{el} \qquad \square$$

2.3.5 $9^{n+1} + 2^{6n+1}$ è div. per 11 $\forall n$

$n = 0$: $9 + 2 = 11$ ✓

I.I. Sapendo che $9^{n+1} + 2^{6n+1} = 11 \cdot k$

provo che $9^{(n+1)+1} + 2^{6(n+1)+1} = 11 \cdot h$ _

$$9 \cdot 9^{n+1} + 64 \cdot 2^{6n+1} =$$

$$= 9 \cdot (11k - 2^{6n+1}) + 64 \cdot 2^{6n+1}$$

$$= 9 \cdot 11k + (-9 + 64) \cdot 2^{6n+1}$$

$$= 11 \cdot (9k + 5 \cdot 2^{6n+1}) \quad \checkmark$$

2.3.6. $$\sum_{j=0}^{n} j^2 = \frac{n(n+1)(2n+1)}{6}$$

È intero: num div. per 6 poiché

div per 2: n o $n+1$ pari ✓

div per 3: resto di $n:3$ può essere $0, 1, 2$

se 0 n div. per 3

se 2 $n+1 = (3k+2)+1 = 3(k+1)$ div. per 3

se 1 $2n+1 = 2(3k+1)+1 = 6k+3$
$= 3(2k+1)$ div per 3
✓

$n = 0$ $\quad \sum_{j=0}^{0} j^2 = 0 \quad \dfrac{0(0+1)(2\cdot 0+1)}{6} = 0$ ✓

$n = 1$ $\quad \sum_{j=0}^{1} j^2 = 1 \quad \dfrac{1\cdot(1+1)(2\cdot 1+1)}{6} = 1$ ✓

P.I. Suppongo $\sum_{j=0}^{n} j^2 = \dfrac{n(n+1)(2n+1)}{6}$.

Devo vedere che:

$$\sum_{j=0}^{n+1} j^2 = \frac{(n+1)(n+2)(2n+3)}{6}$$

$$\downarrow$$

$$\sum_{j=0}^{n} j^2 + (n+1)^2$$

$$= \frac{n(n+1)(2n+1)}{6} + (n+1)^2$$

$$= \frac{n+1}{6}\left(2n^2 + n + 6n + 6\right) = \frac{n+1}{6}\left(2n^2 + 7n + 6\right)$$

✓

2.3.7 Provare che $f_n = \underbrace{\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)}_{\text{lo chiamo } a_n}$

$$\begin{cases} f_0 = 0 \quad f_1 = 1 \\ f_{n+2} = f_n + f_{n+1} \end{cases}$$

Basta vedere che $\begin{cases} a_0 = 0 \quad a_1 = 1 \\ a_{n+2} = a_n + a_{n+1} \end{cases}$

$$a_0 = \frac{1}{\sqrt{5}}(1-1) = 0 \quad \checkmark$$

$$a_1 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = 1 \quad \checkmark$$

Osservo: $\gamma_\pm = \frac{1 \pm \sqrt{5}}{2}$ sono le soluz:

$$1 \cdot x^2 (-1) x - 1 = 0$$

ovvero $x^2 = 1 + x$

$$\Rightarrow \gamma_\pm^2 = 1 + \gamma_\pm$$

$$a_n = c_+ \cdot \gamma_+^n + c_- \cdot \gamma_-^n$$

$$a_{n+2} = c_+ \cdot \gamma_+^{n+2} + c_- \cdot \gamma_-^{n+2}$$

$$= c_+ \cdot \gamma_+^n \cdot \underbrace{\gamma_+^2}_{1+\gamma_+} + c_- \cdot \gamma_-^n \cdot \underbrace{\gamma_-^2}_{1+\gamma_-}$$

$$= \underbrace{c_+ \cdot \gamma_+^n + c_- \cdot \gamma_-^n}_{a_n} + \underbrace{c_+ \cdot \gamma_+^{n+1} + c_- \cdot \gamma_-^{n+1}}_{a_{n+1}} \quad \checkmark$$

2.3.8. Principio di induzione completa:
Se $p(0)$ è vera e supponendo vere $p(0), p(1), \dots, p(n-1), p(n)$ si deduce

che $P(n+1)$ è vera, allora $P(n)$ è vera $\forall n$.

Definisco $Q(n) = P(0)$ e $P(1)$ e ... e $P(n)$.

Dimostro $Q(n)$ per induzione:

$Q(0) = P(0)$ ✓

$Q(n) = P(0)$ e $P(1)$ e ... e $P(n)$

$\Rightarrow P(n+1) \Rightarrow Q(n+1)$ ✓

$\Rightarrow Q(n)$ vera $\forall n \Rightarrow P(n)$ vera $\forall n$.

2.3.9. Ricordo: $p \in \mathbb{N}$ è primo se ogni volta che $p = a \cdot b$ con $a, b \in \mathbb{N}$ si ha $a = 1$ oppure $b = 1$.

Provo per induz. completa che ogni $n \in \mathbb{N}$ è prodotto di primi ($n > 0$).

$n = 1$ primo (forse)
$n = 2$ primo (sicuro).

P.I. (Induz. completa): Supponga che tutti gli interi $\leq n$ siano prodotti di primi.
Lo dimostro per $n+1$.

$n+1$ primo?

- sì → ok
- no: $n+1 = a \cdot b$
  con $a > 1$, $b > 1$
  $\Rightarrow a \cdot b < n+1$
  cioè $a \cdot b \leq n$
  $\Rightarrow$ (ip. induttiva) a, b prodotto di primi

$\Rightarrow$ anche $n+1$. ✓

2.3.10. Esistono infiniti primi.

Per assurdo supponga che siano N:

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \dots,\ p_N.$$

Considero il numero $n = p_1 \cdot p_2 \cdots p_N + 1$.

Lui deve essere prodotto di primi

$\Rightarrow$ deve essere divisibile per qualche p_j.

Tuttavia la divisione $n : p_j$ ha resto 0 1.

assndo –

2.3.11 $A \subseteq \mathbb{R}$

m è minimo di A se

- $m \in A$
- $m \leq a \quad \forall a \in A$

- Non sempre c'è : $\mathbb{Z}$, $(0, +\infty)$
- Se c'è è unico : se ho minimi $m_1, m_2 \Rightarrow m_1 \leq m_2$ (m_1 min, $m_2 \in A$)

$m_2 \leq m_1$ (m_2 min, $m_1 \in A$)

$\Rightarrow m_1 = m_2$.

Principio del min: $A \subset \mathbb{N}$, $A \neq \emptyset$ $\Rightarrow$ ha minimo.

Oss: basta vederlo se A è finito;
infatti dato $A \neq \emptyset$, sia $n \in A$
e considero $A' = \{0, 1, \dots, n\} \cap A$.
Esso è finito e se ha minimo esso

è anche il minimo di A.

Provo per induz. sul numero di el. che $A \subset \mathbb{N}$, $A \neq \emptyset$ ha min.

Base: $A = \{n\} \Rightarrow \min(A) = n$ ✓

Induttivo: Supponiamo che esista il min per ogni insieme con k elementi. Lo dimostro per $k+1$. Prendo A con

$k+1$ elementi. Scelgo a_0 a caso in A.

$a_0 \neq \min(A)$ → sì ok

→ no $\min(A \setminus \{a_0\})$ è anche il $\min(A)$.

2.3.12 Divisione euclidea:

Dati $n, m \in \mathbb{Z}$ con $m > 0$

esisto e sono unici $q, r \in \mathbb{Z}$ t.c.

$$n = q \cdot m + r \qquad \text{con } 0 \le r < m$$

$19 : 5$

$19 = 2 \cdot 5 + 9$ no

$= 3 \cdot 5 + 4$

Infatti: Esistenza

$$R = \{ n - k \cdot m : k \in \mathbb{Z} \} \cap \mathbb{N}$$

Dico che $R \neq \emptyset$.

Se $n \geq 0$ basta prendere $k = 0$ e trovo $n \in R$

se $n < 0$ prendo $k = n$ e trovo

$$\underset{\geq 0}{n}(\underset{\leq 0}{1-n}) \geq 0$$

(Es: $-19 : 5$

$-19 = (-4) \cdot 5 + 1$.)

Prendo r il minimo di R; $r = n - q \cdot m$.
Devo vedere che $r < m$

$$r = n - q \cdot m$$

$$\Rightarrow r - m = n - (q+1) \cdot m$$

è ≥ 0 e quindi sta in R; è $< r$
assurdo perché $r = \min(R)$ -

<u>Unicità</u>: sia $n = q_1 \cdot m + r_1$ $\quad 0 \leq r_1 < m$

$n = q_2 \cdot m + r_2$ $\quad 0 \leq r_2 < m$

$\Longrightarrow \quad r_1 - r_2 = (q_2 - q_1) \cdot m$

$\Longrightarrow \quad |r_1 - r_2| = |q_2 - q_1| \cdot m$

Ora: $|r_1 - r_2| < m$ e $|r_1 - r_2|$ è multiplo di m

$\Longrightarrow |r_1 - r_2| = 0$ e $|q_2 - q_1| = 0$

$\Longrightarrow r_2 = r_1$ e $q_2 = q_1$.

2.3.13 Dati $f(x), g(x) \in \mathbb{R}[x]$ con $\deg(g(x)) > 0$

esistono unici $q(x)$, $r(x)$ t.c.

$$f(x) = q(x) \cdot g(x) + r(x)$$

$f(x)$: dividendo; $g(x)$: divisore; $q(x)$: quoziente; $r(x)$: resto

con $\deg(r(x)) < \deg(g(x))$

$$7x^3 - 2x^2 + 5x - 4 \quad : \quad 2x + 1$$

$$7x^3 - 2x^2 + 5x - 4 = \underbrace{\left(\frac{7}{2}x^2\right)}_{q(x)} \cdot (2x+1) \underbrace{- \frac{11}{2}x^2 \ldots}_{r(x)}$$

NO

$$= \left(\frac{7}{2}x^2 - \frac{11}{4}x\right)(2x+1) + \dots$$

No me mejora

$$= \left(\frac{7}{2}x^2 - \frac{11}{4}x + ?\right)(2x+1) + ?$$ Sí

Esistenza:

I caso: se $\exists\, q(x)$ t.c. $f(x) = q(x)\, g(x)$ ok

II caso:

$$R = \{ f(x) - q(x)\cdot g(x) : q(x) \in \mathbb{R}[x] \}$$

Prendo $r(x)$ t.c. il suo grado sia il minimo possibile in R.

$$f(x) - q(x) \cdot g(x) = r(x)$$

Se $\deg(r(x)) > \deg(g(x))$ posso sostituirlo con uno di grado più basso. [...]

Unicità:

$$f(x) = q_1(x) \cdot g(x) + r_1(x)$$
$$f(x) = q_2(x) \cdot g(x) + r_2(x)$$

$$\Rightarrow r_1(x) - r_2(x) = \left(q_2(x) - q_1(x)\right) \cdot g(x)$$

$\deg(r_1(x) - r_2(x)) < \deg(g(x))$

mas $r_1(x) - r_2(x)$ é multiplo de $p(x)$

$\Rightarrow$ é 0 -