INDUZIONE E COMPLEMENTI

Titolo nota 29/09/2021

Induzione Sia r un numero reale t.c. $r + 1/r$ è razionale. Dimostrare che $r^n + 1/r^n$ è un numero razionale per ogni $n \in \mathbb{N}$

Soluzione

PASSO BASE: $n = 1$ $\quad r^1 + \frac{1}{r^1}$ è razionale per ipotesi

PASSO INDUTTIVO: ~~supponiamo di sapere che $r^n + 1/r^n \in \mathbb{Q}$~~

Supponiamo di sapere (induzione forte) che

$r^k + \frac{1}{r^k} \in \mathbb{Q}$ per tutti i $k \leq n$

Vorrei dim. che $r^{n+1} + \frac{1}{r^{n+1}} \in \mathbb{Q}$

$$\underbrace{\left(r^n + 1/r^n\right)}_{\text{razionale per hp. induttiva}} \cdot \underbrace{\left(r + 1/r\right)}_{\text{razionale per hp del probl}} = r^{n+1} + \frac{1}{r^{n+1}} + \underbrace{r^{n-1} + \frac{1}{r^{n-1}}}_{\text{razionale per ipotesi induttiva}}$$

Per differenza anche $r^{n+1} + \frac{1}{r^{n+1}} = \left(r^n + \frac{1}{r^n}\right)\left(r + \frac{1}{r}\right) - \left(r^{n-1} + \frac{1}{r^{n-1}}\right)$

è anch'esso razionale.

$$r^{n+1} + \frac{1}{r^{n+1}} = r \cdot \left(r^n + \frac{1}{r^n}\right) + \frac{1}{r}\left(r^n + \frac{1}{r^n}\right)$$

$$- r^{n-1} - 1/r^{n-1} =$$

$$= \left(r^n + \frac{1}{r^n}\right)\left(r + \frac{1}{r}\right) - \left(r^{n-1} + 1/r^{n-1}\right)$$

Es Siano $a, b \in \mathbb{R}$ t.c. $a+b \in \mathbb{Q}$ e $ab \in \mathbb{Q}$

Allora $a^n + b^n \in \mathbb{Q} \quad \forall n \geq 1$

Oss Esistono effettivamente numeri $r \in \mathbb{R} \setminus \mathbb{Q}$ tali che $r + 1/r \in \mathbb{Q}$

$$r + \frac{1}{r} = q \iff r^2 + 1 = rq \iff r^2 - rq + 1 = 0$$

$$r = \frac{q \pm \sqrt{q^2 - 4}}{2}$$

$q = 3$ $\qquad r = \dfrac{3 + \sqrt{5}}{2} \qquad r^{-1} = \dfrac{2}{3+\sqrt{5}} = \dfrac{2(3-\sqrt{5})}{(3+\sqrt{5})(3-\sqrt{5})}$

$$= \left(\frac{1+\sqrt{5}}{2}\right)^2 \qquad = \frac{3-\sqrt{5}}{2}$$

Oss $r + \frac{1}{r}$ intero $\Rightarrow$ $r^n + 1/r^n$ intero $\forall n$ (stessa dimostrazione)

Altro esempio Dim. che $\forall n \geq 14$ esistono interi non-negativi x, y tali che $n = 3x + 8y$

Soluz. $\boxed{n = 14}$ $x = 2,\ y = 1$ PASSO BASE

$\boxed{n = 15}$ $x = 5,\ y = 0$

$\boxed{n = 16}$ $x = 0,\ y = 2$

PASSO INDUTTIVO Supponiamo che esistano $x', y' \in \mathbb{N}$ tali che $3x' + 8y' = n - 3$. Allora

$$3(x' + 1) + 8y' = n$$

Induzione con tesi più forte

Dim. che $\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{5}{6} \cdot \ldots \cdot \frac{2n-1}{2n} < \frac{1}{\sqrt{3n}} \quad \forall n \geq 1$

$$\prod_{i=1}^{n} \frac{2i-1}{2i}$$

Proviamo per induzione.

PASSO BASE $\frac{1}{2} < \frac{1}{\sqrt{3}} \iff \sqrt{3} < 2$ OK

PASSO INDUTTIVO

$$\underbrace{\frac{1}{2} \cdot \frac{3}{4} \cdot \ldots \cdot \frac{2n-1}{2n}}_{A} \cdot \underbrace{\frac{2n+1}{2n+2}}_{B} \overset{?}{<} \underbrace{\frac{1}{\sqrt{3(n+1)}}}_{C}$$

Per hp. induttiva so che $A < \frac{1}{\sqrt{3n}}$ (D). Quindi basterebbe dimostrare che

$$\frac{1}{\sqrt{3n}} \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{3(n+1)}} \quad (\star)$$

Tesi: $A \cdot B < C$. So $A < D$. Se riesco a dim. $D \cdot B \leq C$, allora

$$A \cdot B < D \cdot B \leq C$$

(*)

$$\iff \sqrt{n+1} \cdot (2n+1) \leq \sqrt{n} \cdot (2n+2)$$

$$\iff (n+1) \cdot (2n+1)^2 \leq n \cdot (2n+2)^2$$

$$\iff (n+1)(4n^2+4n+1) \leq n(4n^2+8n+4)$$

$$\iff 4n^3 + 4n^2 + n + 4n^2 + 4n + 1 \leq 4n^3 + 8n^2 + 4n$$

Dimostriamo invece $\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}$ FAILURE!

PASSO BASE $\frac{1}{2} \leq \frac{1}{\sqrt{4}}$ vero

PASSO INDUTTIVO $\quad \frac{1}{2} \cdots \frac{2n-1}{2n} \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{3(n+1)+1}}$

Per hp. ind. so $\frac{1}{2} \cdots \frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}$, mi basta dim.

$$\frac{1}{\sqrt{3n+1}} \cdot \frac{2n+1}{2n+2} \leq \frac{1}{\sqrt{3n+4}}$$

$$\Leftrightarrow \quad (3n+4)(2n+1)^2 \leq (3n+1) \cdot 4 \cdot (n+1)^2$$

$$(3n+1) \cdot \left[(2n+1)^2 - 4(n+1)^2 \right] + 3(2n+1)^2 \leq 0$$

$$(3n+1) \cdot \left[4n^2 + 4n + 1 - 4n^2 - 8n - 4 \right] + 3(2n+1)^2 \leq 0$$

$$(3n+1)(-4n-3) + 3(4n^2 + 4n + 1) \leq 0$$

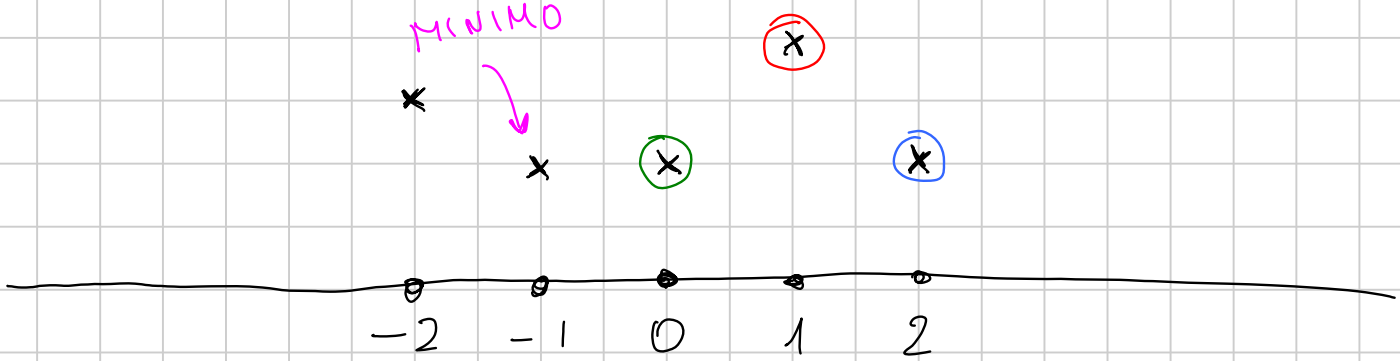
$$-12n^2 - 9n - 4n - 3 + 12n^2 + 12n + 3 \leq 0$$

$$\Leftrightarrow \quad n \geq 0$$

Una funzione Sia $f: \mathbb{Z} \longrightarrow \mathbb{N}$ una funzione tale che

$$f(n) = \frac{f(n+1) + f(n-1)}{2} \quad \|$$

Dimostrare che f è costante



IDEA Sia $m = \min f(\mathbb{Z})$: questo minimo esiste perché $f(\mathbb{Z})$ è un sottoins. non vuoto di $\mathbb{N}$. Sia $x \in \mathbb{Z}$ tale che $f(x) = m$. Considero

$$m = f(x) = \frac{f(x+1) + f(x-1)}{2} \geq \frac{m+m}{2} = m$$

$\geq$ in realtà è un $=$. In particolare $f(x+1) = f(x-1) = m$

In effetti: da un lato $f(x+1) \geq m$ perché m è minimo

dall'altro, se valesse $f(x+1) > m$ avrei

$$\frac{f(x+1) + f(x-1)}{2} > \frac{m+m}{2} = m, \text{ assurdo}$$

Abbiamo dimostrato:

Lemma Se $x \in \mathbb{Z}$ è tale che $f(x) = \min f(\mathbb{Z})$, allora

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

Sia di nuovo $x \in \mathbb{Z}$ t.c. $f(x) = m = \min f(\mathbb{Z})$. Consideriamo

$$S_+ = \{ t \in \mathbb{Z} \mid t \geq x \text{ e } f(t) > m \}$$

La mia tesi è che S_+ sia VUOTO. Se per assurdo S_+ NON fosse vuoto avrebbe minimo (perché è limitato dal basso). Sia $t_0 = \min S_+$. Allora:

- $t_0 = x$ No, perché $x \notin S_+$ in quanto $f(x) = m$

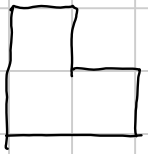
• $t_0 > x$: allora $f(t_0 - 1) \begin{cases} < m \\ = m \\ > m \end{cases}$ NO, m è minimo
NO, $t_0 - 1 \notin S_+$

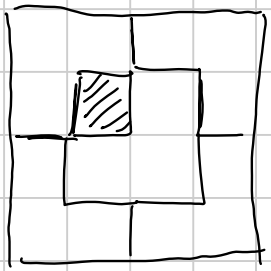
Il lemma mi dice che $f(t_0) = f(t_0 - 1) = m$, assurdo perché $t_0 \in S_+$ (e quindi $f(t_0) > m$)

Quindi: $S_+ = \emptyset$, cioè $\forall t \geq x$ si ha $f(t) \leq m$

Ma d'altro canto $f(t) \geq m$ per def. di $m \Rightarrow f(t) = m$ $\forall t \geq x$. Lo stesso ragionamento mostra $f(t) = m$ $\forall t \leq x$.

Oss $f'(n) := f(2x - n)$

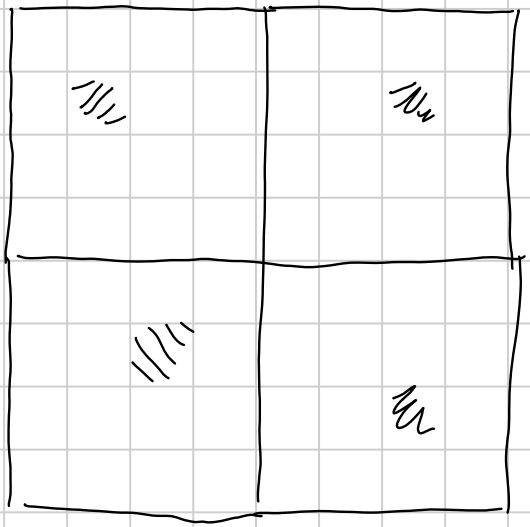
Tromini 



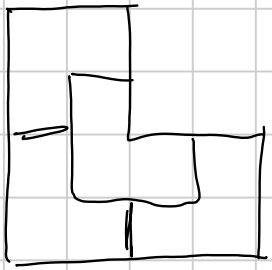
Consideriamo una griglia $2^n \times 2^n$, $n \geq 2$

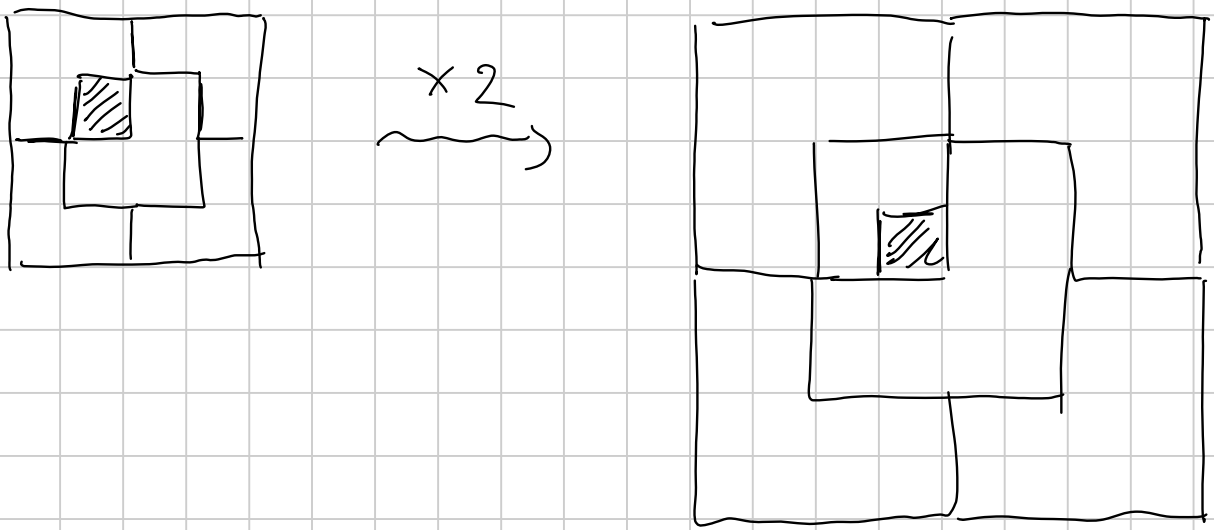
Voglio dim. che è possibile coprirla con tromini lasciando un unico buco IN UNO DEI 4 QUADRATI CENTRALI.

Induzione. Il caso base l'abbiamo fatto.

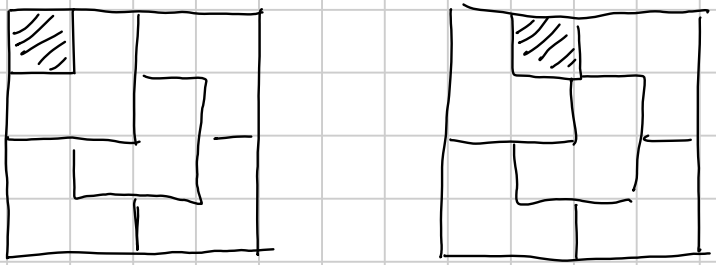


Una possibilità è costruire un MEGATROMINO



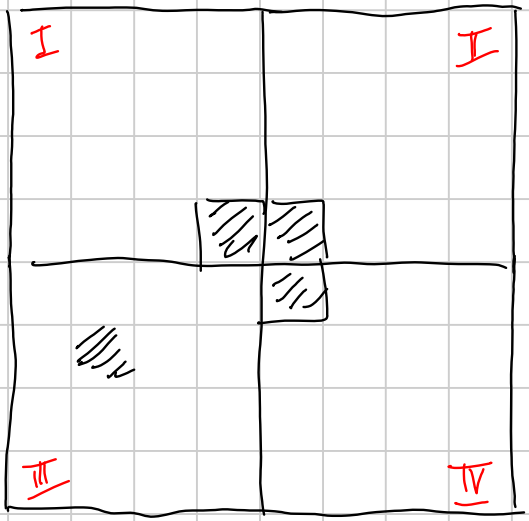


Tesi più forte: posso lasciare il buco in QUALSIASI casella

Caso base 

(idea migliore: faccio $n=1$)

Passo induttivo Dato un quadrato $2^{n+1} \times 2^{n+1}$ e la scelta di una casella



Sul quadrante III: riempio tutto tranne il buco

Su I, II, IV: riempio tutto lasciando un buco nell'angolo al centro. Poi tappo il buco centrale

Fibonacci $F_0 = 0, \quad F_1 = 1, \quad F_{n+1} = F_n + F_{n-1}$

Binet: $F_n = \dfrac{\phi^n - (-\phi)^{-n}}{\sqrt{5}}, \quad \phi = \dfrac{1+\sqrt{5}}{2}$

Induzione: per $n=0$ OK, $n=1$ $\dfrac{\phi - (-\phi)^{-1}}{\sqrt{5}}$

$$\phi^{-1} = -\frac{1-\sqrt{5}}{2} \iff -\phi^{-1} = \frac{1-\sqrt{5}}{2}$$

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

Devo vedere che $F_{n+1} \overset{?}{=} \dfrac{\phi^{n+1} - (-\phi)^{-(n+1)}}{\sqrt{5}}$ sapendo che $F_n = \dfrac{\phi^n - (-\phi)^{-n}}{\sqrt{5}}$ $\quad F_{n-1} = \dfrac{\phi^{n-1} - (-\phi)^{1-n}}{\sqrt{5}}$

$$F_{n+1} = F_n + F_{n-1} = \frac{\phi^n + \phi^{n-1} - \left[(-\phi)^{-n} + (-\phi)^{1-n}\right]}{\sqrt{5}}$$

$$\phi^n + \phi^{n-1} \overset{?}{=} \phi^{n+1} \iff \phi + 1 = \phi^2 \quad (*)$$

, ovvero: mi sto

chiedendo se ϕ soddisfi $x+1 = x^2$

$$x^2 - x - 1 = 0$$

ha soluz $\dfrac{1 \pm \sqrt{1+4}}{2}$

e quindi ϕ rispetta $(\star)$

Tentativo: $F_n = \lambda^n$ (ci riuscirò?)

$$F_{n+1} = \lambda^{n+1} = F_n + F_{n-1} = \lambda^n + \lambda^{n-1}$$

$$\Leftrightarrow \quad \lambda^2 = \lambda + 1 \qquad \lambda = \frac{1 \pm \sqrt{5}}{2}$$

CALCOLO COMBINATORIO

Titolo nota 06/10/2021

Successioni per ricorrenza

$$\begin{cases} a_0 = 0 \qquad a_1 = 1 \\ a_{n+1} = 3a_n - 2a_{n-1} \end{cases} \qquad (*)$$

Altra volta: $a_n = \lambda^n$

$(*)$ $\lambda^{n+1} = 3\lambda^n - 2\lambda^{n-1}$ $\rightsquigarrow$ $\lambda^2 = 3\lambda - 2$ $\quad \lambda \neq 0$

$\Leftrightarrow \quad \lambda^2 - 3\lambda + 2 = 0$

$\Leftrightarrow \quad \lambda = 1, 2$

Oss chiave Se b_n, c_n sono successioni che soddisfano

(*), allora anche $d_n = k \cdot b_n + h \cdot c_n$ rispetta (*),

per qualsiasi $k, h \in \mathbb{R}$ o $\mathbb{C}$

Infatti: $d_{n+1} = k \cdot b_{n+1} + h \cdot c_{n+1}$

$= k \cdot (3b_n - 2b_{n-1}) + h \cdot (3c_n - 2c_{n-1})$

$= 3 \cdot (k \cdot b_n + h \cdot c_n) - 2 \cdot (k \cdot b_{n-1} + h \cdot c_{n-1})$

$= 3 d_n - 2 d_{n-1}$

Oss. $b_n = 1$ è una soluz. di (*)

$c_n = 2^n$ " " " " (*)

$\Rightarrow$ $d_n = k + h \cdot 2^n$ è una soluz. $\forall k, h$

Se impongo $d_0 = 0$ e $d_1 = 1$, cioè

$$\begin{cases} 0 = d_0 = k + h \\ 1 = d_1 = k + 2h \end{cases} \iff \begin{matrix} k = -1, \\ h = 1 \end{matrix}$$

Quindi: la successione $e_n = -1 + 2^n$ rispetta $e_0 = 0$, $e_1 = 1$ (*)

e quindi (induzione) $e_n = a_n$

Oss Se ho $a_{n+1} = c_1 \cdot a_n + c_0 \cdot a_{n-1}$ e l'eqz

$$\lambda^2 = c_1 \lambda + c_0$$

ha un'unica soluz. λ_0, allora possiamo ripetere il ragion. con λ_0^n e $n \cdot \lambda_0^n$

$(*)\ a_{n+1} = 2a_n - a_{n-1}$ $\qquad \lambda^2 = 2\lambda - 1$

$a_n = 1$ $\qquad \Leftrightarrow \quad (\lambda - 1)^2 = 0$

$a_n = n$

Binomio di Newton $\qquad (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$

Dim. Per induzione. Passo base: $n = 1$

$$a + b = \underbrace{\binom{1}{0} \cdot a^0 \cdot b^{1-0}}_{b} + \underbrace{\binom{1}{1} \cdot a^1 \cdot b^{1-1}}_{a}$$

Passo induttivo: $\qquad (a+b)^{n+1} = (a+b)^n (a+b)$

$$= \left(\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \right) (a+b)$$

$$= \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^{i} b^{n+1-i}$$

$j = i+1$

$$= \sum_{j=1}^{n+1} \binom{n}{j-1} a^{j} b^{n+1-j} + \sum_{j=0}^{n+1} \binom{n}{j} a^{j} b^{n+1-j}$$

per $j = n+1$ trovo $\binom{n}{n+1} a^{n+1} b^{0} = 0$

dove definiamo $\binom{n}{-1} = 0$

$$= \sum_{j=0}^{n+1} \left[\binom{n}{j-1} + \binom{n}{j} \right] a^{j} b^{n+1-j}$$

$$= \sum_{j=0}^{n+1} \binom{n+1}{j} a^{j} b^{n+1-j}$$

Sottoinsiemi pari / dispari

Sia A un insieme finito, $A \neq \emptyset$

$$2^{n-1} = \left| \underbrace{\{ X \subseteq A : |X| \text{ pari} \}}_{\wp} \right| = \left| \underbrace{\{ Y \subseteq A : |Y| \text{ dispari} \}}_{\Omega} \right|$$

1. Trovare una bigezione
2. Somma dei coeff. binom. è 2^n / diff. fra coeff. pari e dispari
3. Induzione

1) Se A ha card. dispari: la funz.

$$f : \wp \longrightarrow \Omega$$

$$X \longmapsto A \setminus X$$

è ben definita ($|A \setminus X| = |A| - |X| =$ dispari − pari = dispari)

ed è una bigezione (con inversa $\Omega \longrightarrow \Omega$)

$Y \longmapsto A \setminus Y$

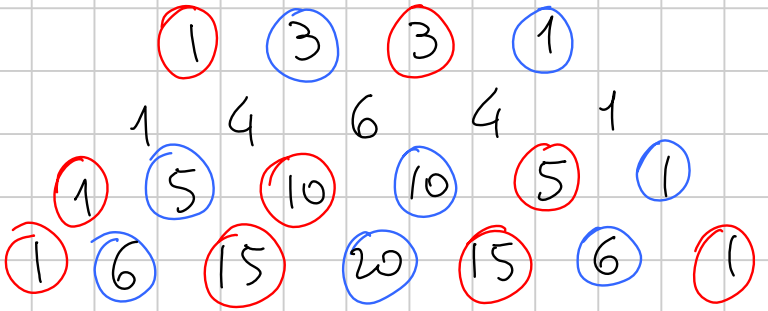
2) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots + \binom{n}{2k} = \binom{n}{1} + \binom{n}{3} + \dots + \binom{n}{2h-1}$

$2k \le n$ $\qquad$ $2h-1 \le n$

Se n dispari, uso $\binom{n}{1} = \binom{n}{n-1}$ $\qquad$ $\binom{n}{3} = \binom{n}{n-3}$ e si conclude

$\sum_{i=0}^{n} (-1)^i \binom{n}{i} \neq 0$: in effetti il binomio di Newton dice

$0 = (-1+1)^n = \sum_{i=0}^{n} \binom{n}{i} (-1)^i (1)^{n-i}$



3. Per induz. sulla cardinalità di A. Per $|A| = 1$, gli unici sottoins. sono $\emptyset$ (pari) e A (dispari).

Da n a $n+1$. Sia $|A| = n+1$; senza perdita di generalità,

$$A = \{1, 2, \dots, n+1\}$$

$$\{X \subseteq A : |X| \text{ pari}\} = \{X \subseteq A : |X| \text{ pari}, X \subseteq \{1, \dots, n\}\}$$

Unione disgiunta $\longrightarrow \amalg \{X \subseteq A : |X| \text{ pari}, n+1 \in X\}$

$$\left|\{X \subseteq A : |X| \text{ pari}\}\right| = \left|\{X \subseteq \{1,\dots,n\} : |X| \text{ pari}\}\right|$$

$$+ \left|\{Y \subseteq \{1,\dots,n\} : |Y| \text{ dispari}\}\right|$$

$$\overset{\text{hp. ind.}}{=} 2^{n-1} + 2^{n-1} = 2^n$$

C'è una biiez.

$$\{X \subseteq A : |X| \text{ pari}, n+1 \in X\} \longleftrightarrow \{Y \subseteq \{1,\dots,n\} : |Y| \text{ dispari}\}$$

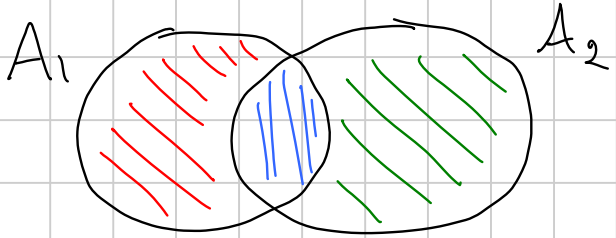
$$X \longmapsto X \setminus \{n+1\}$$

$$Y \cup \{n+1\} \longleftarrow Y$$

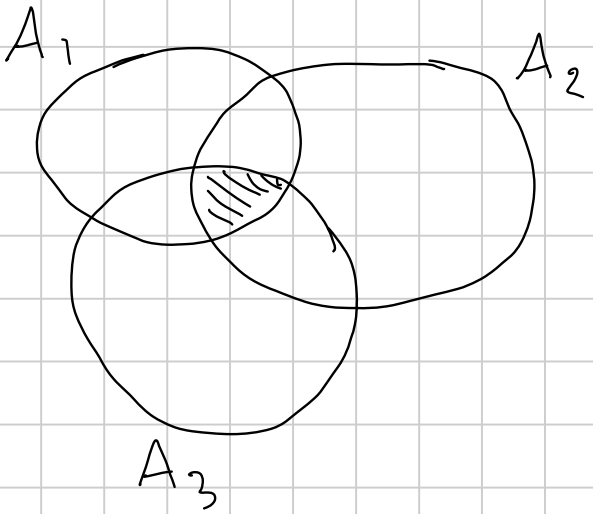
$$\left|\{Y \subseteq A : |A| \text{ dispari}\}\right| = \left|\wp(A)\right| - \left|\{X \subseteq A : |X| \text{ pari}\}\right|$$

$$= 2^{n+1} - 2^n = 2^n$$

Principio di inclusione – esclusione



$$|A_1 \cup A_2| =$$
$$\left(|A_1| - |A_1 \cap A_2|\right) + \left(|A_2| - |A_1 \cap A_2|\right)$$
$$+ |A_1 \cap A_2|$$
$$= |A_1| + |A_2| - |A_1 \cap A_2|$$



$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3|$$
$$- |A_1 \cap A_2| - |A_2 \cap A_3| - |A_3 \cap A_1|$$
$$+ |A_1 \cap A_2 \cap A_3|$$

$$|A_1 \cup A_2 \cup \dots \cup A_n| = \sum_{\substack{I \subseteq \{1,\dots,n\} \\ I \neq \emptyset}} (-1)^{|I|+1} \left| \bigcap_{i \in I} A_i \right|$$

Se $n=3$: i sottoinsiemi I sono

$\{1\}$ $\{2\}$ $\{3\}$ $\quad |A_1| + |A_2| + |A_3|$

$\{1,2\}$ $\{2,3\}$ $\{3,1\}$ $\quad -(|A_1 \cap A_2| + |A_2 \cap A_3| + |A_3 \cap A_1|)$

$\{1,2,3\}$ $\quad + |A_1 \cap A_2 \cap A_3|$

Dim 1 Sia x un elemento di $A_1 \cup \dots \cup A_n$, che compare in r insiemi. Questo x contribuisce:

$$+\binom{r}{1} - \binom{r}{2} + \binom{r}{3} - \dots + (-1)^{r+1}\binom{r}{r} \overset{?}{=} 1 = \binom{r}{0}.$$

sì, perché $\sum (-1)^i \binom{n}{i} = 0$ □

Dim 2 Dato un sottoinsieme $A \subseteq X$ chiamiamo FUNZIONE CARATTERISTICA DI A la funzione

$$\mathbb{1}_A : X \longrightarrow \{0,1\}$$

$$x \longmapsto \begin{cases} 1, & x \in A \\ 0, & x \notin A \end{cases}$$

In particolare: $\sum_{x \in X} \mathbb{1}_A(x) = |A|$

$$\mathbb{1}_{A_1} \cdot \mathbb{1}_{A_2} = \mathbb{1}_{A_1 \cap A_2}$$

$$\mathbb{1}_{A_1 \cup A_2} = 1 - \mathbb{1}_{{}^c(A_1 \cup A_2)}$$

$$= 1 - \mathbb{1}_{{}^cA_1 \cap {}^cA_2}$$

$$= 1 - \mathbb{1}_{{}^cA_1} \cdot \mathbb{1}_{{}^cA_1}$$

$$= 1 - (1 - \mathbb{1}_{A_1})(1 - \mathbb{1}_{A_2})$$

$$\mathbb{1}_{A_1 \cup A_2 \cup \dots \cup A_m} = 1 - (1 - \mathbb{1}_{A_1}) \dots (1 - \mathbb{1}_{A_m})$$

$$= \mathbb{1}_{A_1} + \dots + \mathbb{1}_{A_m} - \sum_{i<j} \underbrace{\mathbb{1}_{A_i} \mathbb{1}_{A_j}}_{\mathbb{1}_{A_i \cap A_j}} + \sum_{i<j<k} \mathbb{1}_{A_i} \mathbb{1}_{A_j} \mathbb{1}_{A_k} - \dots$$

$$|A_1 \cup \dots \cup A_m| = |A_1| + \dots + |A_m| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \dots$$

$$|A_1 \cup \dots \cup A_m| = \sum_{j=1}^{m} (-1)^{j+1} \sum_{\substack{I \subseteq \{1,\dots,m\} \\ |I| = j}} \left| \bigcap_{i \in I} A_i \right| .$$

□

Stars & bars

Trovare il n° di soluz. intere positive dell'eqz

$$(\star) \quad x_1 + \dots + x_k = n$$

Es $n = 5$, $k = 3$

$3+1+1$ $\quad$ $1+3+1$ $\quad$ $1+1+3$

$2+2+1$ $\quad$ $2+1+2$ $\quad$ $1+2+2$

$***|*|*$ $\quad$ $3+1+1$

$**|*|**$ $\quad$ $2+1+2$

Ci sono tante soluz. di $(\star)$ quanti modi di "inserire" $k-1$ sbarrette fra n stelline, il che si fa in $\binom{n-1}{k-1}$

modi diversi.

Variante: addendi ≥ 0

$$x_1 + \dots + x_k = n \qquad \text{con } x_i \text{ interi} \geq 0$$

$$\updownarrow$$

$$(x_1 + 1) + (x_2 + 1) + \dots + (x_k + 1) = n + k$$

Il n° di soluz. è quindi $\binom{n+k-1}{k-1}$

ANAGRAMMI

Titolo nota 07/10/2021

CANE AECN

↳ $4!$ anagrammi

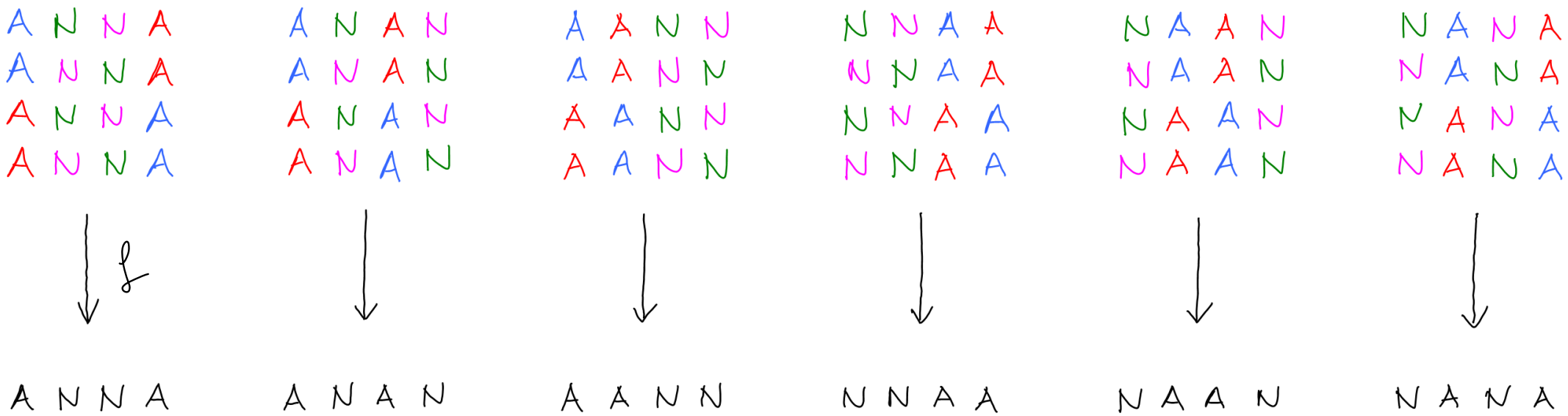
ANNA ha 6 / ~~$4!$~~ / $3!$ / $\frac{4!}{2!2!}$ anagrammi

No!

Un anagramma di "ANNA" corrisponde alla scelta di 2 caselle su 4 in cui scrivere "N" $\rightsquigarrow \binom{4}{2}$

MAMMA

$$\binom{5}{2} = \binom{5}{3}$$



$X = \{$ anagrammi di ANNA $\} \xrightarrow{f} \{$ anagrammi di ANNA $\}$

$= Y$

La funzione f è 4 - a - 1, cioè:

NANA $\quad \forall y \in Y, \quad |f^{-1}(y)| = 4$

"$y \in Y$: chi è $f^{-1}(y)$? Sono tanti quanti i modi di

colorare le A (2) × modi di colorare le N (2)

$\#\{\text{anagrammi di ANNA}\} = \frac{1}{4}\,\#\{\text{anagrammi di ANNA}\} = 6$

MAMMALUCCO 10 lettere

$\{\text{anagrammi di } M_1\, A_1\, M_2\, M_3\, A_2\, L_1\, U_1\, C_1\, C_2\, O_1\} = 10!$

$\downarrow g$

$\{\text{" "} \quad \text{MAMMALUCCO}\} \ni y$

$|g^{-1}(y)| = 3! \times 2! \times 2! \times 1! \times 1! \times 1! = 24$

↳ n° di modi di aggiungere i pedici $\{1,2,3\}$ alle 3 lettere M

$$\#\{\text{anagr. di MAMMALUCCO}\} = \frac{10!}{3!\,2!\,2!}$$

$$\#\text{anagrammi } AAAAAABBBCCDDD = \frac{13!}{5!\,3!\,2!\,3!}$$

In generale: una parola con n_1 lettere di "tipo 1", n_2 di "tipo 2", ..., n_k di "tipo k" ha

$$\binom{n_1+\dots+n_k}{n_1, n_2, \dots, n_k} = \frac{(n_1+n_2+\dots+n_k)!}{n_1!\,n_2!\cdots n_k!}$$

$$\binom{a+b}{a} = \frac{(a+b)!}{a!\,b!}.$$

Coefficienti MULTINOMIALI

$$\binom{7}{3,2,2} = \frac{7!}{3!2!2!}$$

A A A B B C C

$$\binom{n}{n_1, \dots, n_k}$$

Il coeff. multinomiale rappresenta il n° di modi di dividere n oggetti in k gruppi in modo che il 1° gruppo abbia n_1 elementi, il secondo ne abbia n_2, ..., il k-esimo ne abbia n_k

36 biglie. Ne voglio colorare 12 R
12 B
4 V
2 G.

Lo posso fare in $\frac{36!}{12!\,12!\,4!\,2!\,6!}$ modi (6 "trasparenti")

Funzioni suriettive

Siano X, Y insiemi con m, n elem. rispettivamente, $m \geq n$. Determinare $\#\{ f : X \to Y \text{ suriettive} \}$

Idea 0: $X = N_m = \{1, 2, \dots, m\}$ $Y = N_n$

Idea 1: contare le funzioni NON suriettive

$\#\{\text{funz. surj.}\} = n^m - \#\{\text{funz. non surjettive}\}$

Idea 2: Sia $F_i = \{ f : X \to Y \mid i \notin f(X) \}$

$$\{\text{funz. non suriettive}\} = \bigcup_{i=1}^{n} F_i$$

$$|\{\text{funz. non surj.}\}| = \left|\bigcup_{i=1}^{n} F_i\right| = |F_1| + |F_2| + \dots + |F_n| - \left(|F_1 \cap F_2| + |F_1 \cap F_3| + \dots\right) + \left(|F_1 \cap F_2 \cap F_3| + \dots\right) - \dots$$

$$F_1 = \{ f : X \to \{2, 3, \dots, n\} \} \qquad |F_1| = (n-1)^m$$

$$F_1 \cap F_2 = \{ f : X \to \{3, 4, \dots, n\} \} \qquad |F_1 \cap F_2| = (n-2)^m$$

$$|F_{i_1} \cap \dots \cap F_{i_k}| = (n-k)^m \qquad i_1, \dots, i_k \text{ tutti diversi}$$

$$\left|\bigcup_{i=1}^{n} F_i\right| = n \cdot (n-1)^m - \binom{n}{2}(n-2)^m + \binom{n}{3}(n-3)^m$$

$$|F_1| + \dots + |F_n| \qquad - \dots + (-1)^{n+1}\binom{n}{n}\cdot(n-n)^m$$

$$\#\{\text{funz. suriettive}\} = n^m - n(n-1)^m + \binom{n}{2}(n-2)^m - \dots$$

$$= \sum_{i=0}^{n} \binom{n}{i}(n-i)^m \cdot (-1)^i$$

Esercizi

Sia X un insieme con 100 elementi. Quante coppie di sottoinsiemi (A, B) di X esistono tali che $\#(A \cap B) = 30$?

E con $\#(A \cup B) = 30$?

$|A| = \#A$

$\binom{100}{30} \cdot 3^{70}$ → Devo scegliere l'insieme $A \cap B$ (in $\binom{100}{30}$ modi)

Per ognuno dei 70 elementi non nell'intersez. ho 3 scelte: metterlo in A, metterlo in B, non metterlo né in A né in B

Preliminare: dato un sottoinsieme $C \subseteq X$ con $|C| = 30$, dire quante sono le coppie (A, B) con $A \cap B = C$.

(3^{70}).

La risposta al probl. originale è:

$$\sum_{\substack{(A,B) \text{ con} \\ |A \cap B| = 30}} 1 = \sum_{\substack{C \subseteq X \\ |C| = 30}} \boxed{\sum_{\substack{(A,B) \text{ t.c.} \\ A \cap B = C}} 1}$$

$$= \sum_{\substack{C \subseteq X \\ |C| = 30}} 3^{70} = 3^{70} \cdot \binom{100}{30}$$

$$\{(A,B) : A \cap B = C\} \longleftrightarrow \{\text{terne } (D,E,F) \quad D,E,F \subseteq X \setminus C, \text{ disgiunti, e t.c. } D \cup E \cup F = X \setminus C\}$$

$$(A,B) \overset{f}{\longmapsto} \begin{array}{l} D = A \setminus C \\ E = B \setminus C \\ F = X \setminus (A \cup B) \end{array}$$

$$\begin{array}{l} A = D \cup C \\ B = E \cup C \end{array} \overset{g}{\longleftarrow\!\!\!|} (D,E,F)$$

$$\{\text{terne } D,E,F \text{ come sopra}\} \longleftrightarrow \{h : X \setminus C \longrightarrow \{1,2,3\}\}$$

$$(h^{-1}(1), h^{-1}(2), h^{-1}(3)) \longleftarrow h$$

$$(D,E,F) \longmapsto h(x) = \begin{cases} 1 & \text{se } x \in D \\ 2 & \text{se } x \in E \\ 3 & \text{se } x \in F \end{cases}$$

(A,B) $\#(A \cup B) = 30$: quante sono?

$$\binom{100}{30} \cdot 3^{30}$$

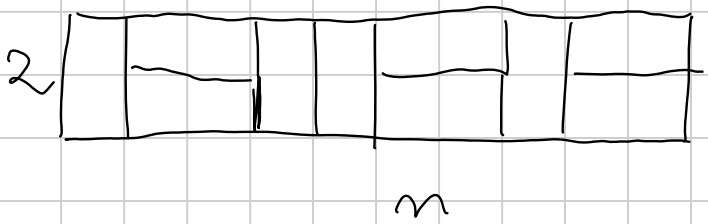
Variante: terne ordinate (A,B,C) di sottoinsiemi di $\{1,\dots,n\}$

tali che $A \cup B \cup C = \{1, \dots, n\}$? 7^n

$\downarrow$

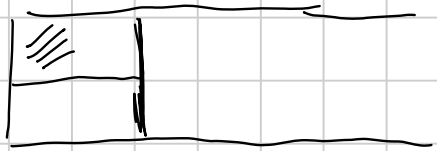
$(2^3 - 1)^n$

Tessere



Numero di tassellazioni della griglia $2 \times n$ con pezzi 1×2

Guardo una tassellazione della $2 \times n$



Data una tassellaz. ne produco o una della $2 \times (n-1)$

o una della $2 \times (n-2)$

$$\#\{\text{tass. } 2\times n\} = \#\{\text{tass } 2\times(n-1)\} + \#\{\text{tass } 2\times(n-2)\}$$

$$\overset{\shortparallel}{T_n}$$

$$f: \{\text{tass } 2\times n\} \longrightarrow \{\text{tass } 2\times(n-1)\} \amalg \{\text{tass } 2\times(n-2)\}$$

$f(\square T) = T$ $\qquad$ $\overset{\Psi}{T}$

$f(\square\!\square T) = T$

Sappiamo: $\begin{cases} T_n = T_{n-1} + T_{n-2} \\ T_1 = 1 \\ T_2 = 2 \end{cases}$

$F_0 = 0,\ F_1 = 1,\ F_2 = 1,$

$F_3 = 2, \ldots$

$T_k = F_{k+1}$

Esercizio 36

$X = \{1, \dots, 100\}$. Contare i sottoins. A di X t.c.

$|A| = 96$ e la somma degli el. di A è pari

- 50 pari, 46 dispari
- ~~49 pari, 47 "~~
- 48 " , 48 "
- ~~47 " 49 "~~
- 46 " 50 "

$$\binom{50}{50} \times \binom{50}{46} + \binom{50}{48} \times \binom{50}{48} + \binom{50}{46} \times \binom{50}{50}$$

$$\sum_{a \in A} a \quad \text{pari} \qquad\qquad \sum_{x \in X} x = \frac{100 \cdot 101}{2} = 5050$$

$$\sum_{a \notin A} a = \sum_{a \in X \setminus A} a = \underbrace{\sum_{x \in X} x}_{\text{pari}} - \underbrace{\sum_{a \in A} a}_{\text{pari}} \quad \text{pari}$$

$$\binom{50}{4} + \binom{50}{2}\binom{50}{2} + \binom{50}{4}$$

Titolo nota

Double counting

(44) $$\sum_{k=0}^{n} k \cdot \binom{n}{k} = n \cdot 2^{n-1} \qquad \forall n \geq 1$$

Consideriamo n persone. Vogliamo formare una squadra con alcune di queste persone e nominare un capitano. In quanti modi si può fare?

n (scelte per il capitano) $\times$ 2^{n-1} (il n° di sottoinsiemi di $\{n \text{ persone}\} \setminus \{\text{capitano}\}$)

Oppure: squadre da 1 persona $\binom{n}{1}$ x 1 scelta capit.

" " 2 " $\binom{n}{2}$ x 2 " "

$\vdots$

$\binom{n}{k}$ x k " "

$$\sum_{k=0}^{n} k \binom{n}{k} = n \cdot 2^{n-1}$$

$$X = \left\{ (S, c) : \begin{array}{l} S \subseteq \{1, \dots, n\} \\ c \in S \end{array} \right\}$$

Calcoliamo $|X|$ in due modi:

- Per c ho n possibilità; fissato c, i sottoinsiemi S di $\{1, \dots, n\}$ che contengono c sono in bigezione con i sottoins. di $\{1, \dots, n\} \setminus \{c\}$, che sono 2^{n-1}

- $$|X| = \sum_{S \subseteq \{1,\dots,n\}} |S| = \sum_{k=0}^{n} \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S| = k}} |S|$$

$$= \sum_{k=0}^{n} \sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S| = k}} k = \sum_{k=0}^{n} k \left(\sum_{\substack{S \subseteq \{1,\dots,n\} \\ |S| = k}} 1 \right)$$

$$= \sum_{k=0}^{n} k \cdot \binom{n}{k}$$

$$\sum_{k=0}^{n} k^2 \binom{n}{k} = (n^2+n)\cdot 2^{n-2}$$

$$\sum_{k=1}^{n} k^2 \frac{n!}{k!(n-k)!} = \sum_{k=1}^{n} k^2 \frac{n(n-1)!}{k\cdot(k-1)!(n-k)!}$$

$$= n \sum_{k=1}^{n} k \binom{n-1}{k-1} = n \sum_{k=1}^{n} \{ \underbrace{(k-1)}_{j} \binom{n-1}{k-1} + \binom{n-1}{k-1} \}$$

$$= n \sum_{j=0}^{n-1} \{ j \binom{n-1}{j} + \binom{n-1}{j} \} = n \cdot [(n-1)\cdot 2^{n-2} + 2^{n-1}]$$

$$= n \cdot 2^{n-2} \cdot (n-1+2) = n(n+1)\,2^{n-2}$$

Conteggi di divisori

Dato n intero positivo calcolare $d(n)$ = n° divisori interi positivi di n.

$10'000 = 10^4 = 2^4 \cdot 5^4$ $\rightsquigarrow$ divisori $2^a \cdot 5^b$

a: 5 scelte $(0,1,2,3,4)$

b: " " "

$\Rightarrow$ 25 divisori

$n = p_1^{e_1} \dots p_k^{e_k}$ ha tutti divisori della forma

$p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$

con $0 \le a_i \le e_i$ $\rightsquigarrow$ $e_i + 1$ scelte per a_i

$$d(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

- Determinare il n° delle terne ord. (x, y, z) di interi positivi tali che $xyz = 10^{100} = 2^{100} 5^{100}$
  (stessa domanda con $x^2 yz = 10^{100}$)

$$x = 2^{a_1} 5^{b_1} \qquad y = 2^{a_2} 5^{b_2} \qquad z = 2^{a_3} 5^{b_3}$$

$$\begin{cases} a_1 + a_2 + a_3 = 100 \\ b_1 + b_2 + b_3 = 100 \end{cases} \rightsquigarrow \binom{100+3-1}{3-1} = \binom{102}{2}$$

Risposta: $\binom{102}{2}^2$

$$X^2 Y Z = 2^{2a_1} 5^{2b_1} \cdot 2^{a_2} \cdot 5^{b_2} \cdot 2^{a_3} 5^{b_3} = 2^{100} 5^{100}$$

(1) $2a_1 + a_2 + a_3 = 100$ $\qquad a_1, a_2, a_3 \geq 0$

(2) $2b_1 + b_2 + b_3 = 100$

$\rightarrow a_3 = 100 - 2a_1 - a_2 \geq 0$

a_1 va fra 0 e 50

Fissato a_1, a_2 varia da 0 a $100 - 2a_1$

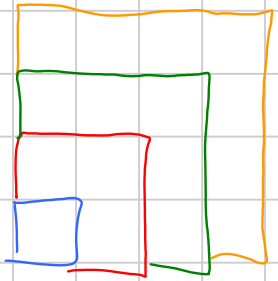
N° soluz eqz. (1): $\sum_{a_1=0}^{50} (101 - 2a_1) =$

$$= \sum_{a_1=0}^{50} 101 - 2\sum_{a_1=0}^{50} a_1 = 51 \cdot 101 - 2 \cdot \frac{50 \cdot 51}{2}$$

$$= 51 \cdot (101 - 50) = 51^2$$

Risultato: 51^4

Es. $1 + 3 + 5 + \dots + (2n-1) = n^2$



MCD $\boxed{(3^a - 1,\ 3^b - 1) = (3^a - 1 - 3^{a-b}(3^b - 1),\ 3^b - 1)}$

$a \geq b$

$$(a, b) = (a - kb, b)$$

$$= \left(3^a - 1 - 3^a + 3^{a-b}, 3^b - 1\right) = \boxed{\left(3^{a-b} - 1, 3^b - 1\right)} \quad a - b \geq b$$

$$= \begin{cases} \left(3^{a-2b} - 1, 3^b - 1\right) & \\ \left(3^{a-b} - 1, 3^{b-(a-b)} - 1\right) & a - b < b \end{cases}$$

$$\left(3^c - 1, 3^d - 1\right)$$

Osservazioni • Dopo n passi di questo tipo, mostro che

$$\left(3^a - 1, 3^b - 1\right) = \left(3^{a_n} - 1, 3^{b_n} - 1\right) \quad a_n \geq b_n$$

- $\max\{a_n, b_n\}$ è una successione di interi non negativi e decrescenti
- definitivamente questo max è 0
- inoltre $\{a_{n+1}, b_{n+1}\} = \{a_n - b_n, b_n\}$
- $\mathrm{mcd}(a_{n+1}, b_{n+1}) = \mathrm{mcd}(a_n, b_n)$

Es $(3^{25}-1,\ 3^{16}-1) = (3^{25}-1-3^9(3^{16}-1),\ 3^{16}-1)$

$= (3^9-1,\ 3^{16}-1) = (3^9-1,\ 3^7-1)$

$= (3^7-1,\ 3^2-1) = (3^5-1,\ 3^2-1) = (3^3-1,\ 3^2-1)$

$$= \left(3^1 - 1, 3^2 - 1\right) = \left(3^1 - 1, 3^1 - 1\right)$$

$$= \left(3^1 - 1, 3^0 - 1\right)$$

$$(M, m) = (M - m, m)$$

$$(25, 16) = (16, 9) = (9, 7) = (7, 2) = \dots$$

$$(a, b) \to \dots \to (d, 0) = d = (a, b)$$

$$\left(3^a - 1, 3^b - 1\right) = \dots = \left(3^d - 1, 3^0 - 1\right) = 3^d - 1$$

$$= 3^{(a,b)} - 1.$$

$$\left(3^a-2,\ 3^b-2\right) = \left(3^a-2-3^{a-b}\left(3^b-2\right),\ 3^b-2\right)$$

$$= \left(2\cdot 3^{a-b}-2,\ 3^b-2\right)$$

Analogo con polinomi

Studiare $\left(n^3+n+3,\ 2n+1\right)$ al variare di $n \in \mathbb{N}$.

$$\left(n^3+n+3,\ 2n+1\right) = \left(2n^3+2n+6,\ 2n+1\right)$$

$2n+1$ è dispari

$$= \left(2n^3+2n+6 - n^2\left(2n+1\right),\ 2n+1\right)$$

$$= \left(2n+6-n^2,\ 2n+1 \right)$$

$$= \left(4n+12-2n^2+n(2n+1),\ 2n+1 \right)$$

$$= \left(4n+12+n,\ 2n+1 \right) = \left(5n+12,\ 2n+1 \right)$$

$$= \left(5n+12-2(2n+1),\ 2n+1 \right) = \left(n+10,\ 2n+1 \right)$$

$$= \left(n+10,\ (2n+1)-2(n+10) \right) = \left(n+10,\ -19 \right)$$

$$= \begin{cases} 19 & \text{se } 19 \mid n+10 \iff n+10 \equiv 0\ (19) \\ 1 & \text{altrimenti} \end{cases}$$

$$\Updownarrow$$

$$n \equiv 9\ (19) \iff n+19 \equiv 9\ (19)$$

$n + 10 \equiv 0 \ (19) \iff$ $\boxed{n \equiv -10 \ (19)}$

Una diofantea lineare

$$11x + 41y = 2$$

1) Ammette soluz. intere? Se e solo se $(11, 41) \mid 2$ ($\frac{1}{11}$)

2) Quante soluz. rispettano $|x|, |y| \leq 100$?

Troviamo una soluz. intera.

$$41 = 11 \cdot 3 + 8$$

$$11 = 8 \cdot 1 + 3$$

$$8 = 3 \cdot 2 + 2$$

$3 = 2 \cdot 1 + 1$

$\mathrm{mcd}(41, 11) = 1 = 3 - 2 = 3 - (8 - 3 \cdot 2)$

$= 3 \cdot 3 - 8 \cdot 1$

$= (11 - 8) \cdot 3 - 8 \cdot 1$

$= 11 \cdot 3 - 8 \cdot 4$

$= 11 \cdot 3 - (41 - 3 \cdot 11) \cdot 4$

$= 15 \cdot 11 - 4 \cdot 41$

$x_0 = 15, \quad y_0 = -4$ è una soluzione di

$$11 x_0 + 41 y_0 = 1$$

$$11 \cdot (2x_0) + 41 \cdot (2y_0) = 2$$

Idea Se x', y' è un'altra soluzione, scrivo

$$x' = 30 + z \qquad y' = -8 + w$$

$$11 \cdot (x') + 41 \cdot (y') = 2$$

$$11 \cdot (30 + z) + 41 \cdot (-8 + w) = 2$$

$$11z + 41w + \underbrace{30 \cdot 11 - 8 \cdot 41}_{2} = 2$$

$$11z = -41w \Rightarrow 11 \mid 11z = -41w$$

$$(11, 41) = 1 \Rightarrow 11 \mid w$$

$$w = 11\,w' \qquad 11z = -41 \cdot 11\,w'$$

$$z = -41\,w' \qquad z = -41\,w'$$

Conclusione Ogni soluz. di $11x + 41y = 2$ è della forma $(x', y') = (30 - 41w', -8 + 11w')$.

per qualche intero w'.

$(71, -19)$, $(30, -8)$, $(-11, 3)$, $(-52, 14)$,

$(-93, 25)$

$8 \mid 3^m + 7^m - 2 \quad \forall m \geq 0$

$a_m = 3^m + 7^m$ $\qquad \lambda^2 = h \cdot \lambda + k$

Verificate che $a_{m+1} = h\, a_m + k\, a_{m-1}$

$\lambda^{m+1} = 10\lambda^m - 21\lambda^{m-1}$ $\qquad (x-3)(x-7) = x^2 - 10x + 21$

$\lambda^2 = 10\lambda - 21 \rightsquigarrow \lambda_1, \lambda_2$ $\qquad c_1 \lambda_1^m + c_2 \lambda_2^m = a_m$

Ora procediamo per induzione. Per $m=0, 1$ ho

$a_0 = 2$ e $a_1 = 10$ e effett. $8 \mid a_m - 2$

Ora supponiamo di sapere che $a_k = 8 b_k + 2$

per certi interi b_k, per ogni $k \leq m$.

$$a_{m+1} = 10 a_m - 21 a_{m-1} = 10 (8 \cdot b_m + 2)$$

$$- 21 (8 \cdot b_{m-1} + 2)$$

$$= 8 \cdot (10 b_m - 21 b_{m-1}) - 22$$

$$= 8 (10 b_m - 21 b_{m-1} - 3) + 2$$

□

$$7^m + 3^m - 2 \overset{?}{\equiv} 0 \pmod 8$$

Oss $3^1 \equiv 3 \mod 8$; $3^2 \equiv 1 \pmod 8$

$$3^{71} \equiv 3^{70} \cdot 3 \equiv (3^2)^{35} \cdot 3^1 \equiv 1^{35} \cdot 3 \pmod 8$$

$$3^{2n+1} \equiv 3 \cdot (3^2)^n \equiv 3 \cdot 1^n \equiv 3 \pmod 8$$

$$3^{2n} \equiv (3^2)^n \equiv 1^n \equiv 1 \pmod 8$$

$$7^2 \equiv 1 \pmod 8 \qquad 7^{2n} \equiv (-1)^{2n} \equiv 1^n \equiv 1 \pmod 8$$

$$7^{2n+1} \equiv 7^{2n} \cdot 7 \equiv 7 \pmod 8$$

$$3^m + 7^m - 2 \equiv \begin{cases} 1 + 1 - 2 \equiv 0 \pmod 8 \\ 3 + 7 - 2 \equiv 8 \equiv 0 \pmod 8 \end{cases}$$

CONGRUENZE

Titolo nota

Primo compitino: 8 novembre pomeriggio / 13 novembre mattina

Secondo compitino: 20 dicembre

Sottoins. di $\{1, \dots, 100\} = X$

Contare i sottoins. A di X t.c.

- $|A| = 3$, $\quad A = \{a, b, c\}$
- $a + b + c = 100$ $\qquad$ a, b, c interi > 0

Soluz. $\quad \# \{ (a, b, c) : \overbrace{a, b, c \in X,}^{} \; a + b + c = 100 \} =$

$$= \binom{100 - 1}{3 - 1} = \binom{99}{2} = 99 \cdot 49$$

$x_1 + \dots + x_k = n$

con $x_1, \dots, x_k$ int > 0

è $\quad \binom{n-1}{k-1}$

Vorrei dividere per 6, ma devo stare attento: in alcune

terne (a, b, c) ho un n° ripetuto!

$$3 + 3 + 94$$

Quante sono le terne ordinate con un numero ripetuto?

$$2a + b = 100 \rightsquigarrow b = 100 - 2a$$

$$100 - 2a > 0$$

$$1 \leq a < 50$$

Quante sono le sol. di $a + b + c = 100$ con 2 addendi uguali? $49 \cdot 3$ $\hookrightarrow$

$$\begin{cases} a = b \neq c \\ b = c \neq a \\ c = a \neq b \end{cases}$$

$$\binom{99}{2} - 3 \cdot 49 = \#\{\text{terne } (a,b,c) \text{ ord. con } a,b,c \in X,\ a+b+c=100, \text{ e } a,b,c \text{ tutti diversi}\}$$

$\{a,b,c\}$

$a+b+c=100$

$a+c+b$

$b+a+c$

$b+c+a$

$c+a+b$

$c+b+a$

$$\left\{ \begin{array}{l} \text{terne } (a,b,c) \text{ ord. con} \\ a,b,c \in X, \quad a+b+c = 100, \\ \text{e } a,b,c \text{ tutti diversi} \end{array} \right\} \xrightarrow{f} \left\{ \begin{array}{l} A \subseteq X, \quad |A| = 3 \\ A = \{a,b,c\} \\ a+b+c = 100 \end{array} \right\}$$

$$(a,b,c) \longmapsto \{a,b,c\}$$

La funzione f è $6 - a - 1$, e quindi la risposta al problema è

$$\frac{1}{6}\left[\binom{99}{2} - 49 \cdot 3 \right]$$

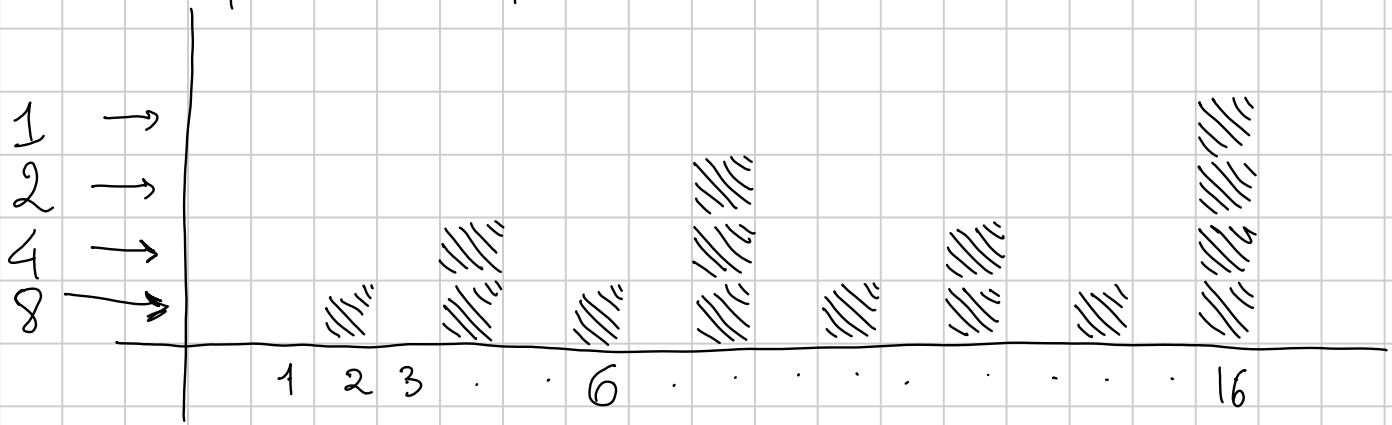
Fattorizzazione di $n!$

1) p primo $\mid n! \iff p \leq n$

$p \mid n \cdot (n-1) \cdot (n-2) \cdots 1 \implies p \mid n-i$ per qualche i

$p \leq n - i \leq n$

2) Con quale esponente compare un certo p?



16!

Potenza di 2 in $16!$ $= 2^{\#\text{ quadratini anneriti}}$

$$8 + 4 + 2 + 1 = \frac{16}{2} + \frac{16}{4} + \frac{16}{8} + \frac{16}{16}$$

Pot. di 2 in $18!$ ha esponente

$$\frac{18}{2} + \left\lfloor \frac{18}{4} \right\rfloor + \left\lfloor \frac{18}{8} \right\rfloor + \left\lfloor \frac{18}{16} \right\rfloor \qquad 4K + r$$

$$K = \left\lfloor \frac{4K + r}{4} \right\rfloor$$

Caso generale: l'esponente di p in $n!$ è

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots = \sum_{K=1}^{\infty} \left\lfloor \frac{n}{p^K} \right\rfloor$$

(il limite sup. della somma può essere sostituito da K_0

t.c. $p^{k_0} \leq n < p^{k_0+1}$)

Diofantee $x^2 - y^2 = n$

$x^2 - y^2 = 2022$ con x, y interi

$(x+y)\cdot(x-y) = 2022$

$$(*)\begin{cases} x+y = a \\ x-y = \dfrac{2022}{a} \end{cases} \qquad a \mid 2022$$

$a = 1$

$$\begin{cases} x+y = 1 \\ x-y = 2022 \end{cases} \rightsquigarrow \begin{cases} x = \dfrac{1+2022}{2} \\ y = \dfrac{1-2022}{2} \end{cases}$$

Risulta che x, y non sono <u>mai</u> interi! In effetti si ha

$$x = \frac{a + 2022/a}{2} \qquad y = \frac{a - 2022/a}{2}$$

Siccome 2022 ha ESATTAMENTE UN fattore 2, uno fra a e $2022/a$ è dispari e l'altro è pari:

$$a = 2^{e_1} \cdots \qquad 2022/a = 2^{e_2} \cdots$$

$$2^1 \cdots = 2022 = a \cdot \frac{2022}{a} = 2^{e_1+e_2} \cdots \Rightarrow e_1 + e_2 = 1$$

$$\Rightarrow \{e_1, e_2\} = \{0, 1\}$$

Conclusione: $x = \dfrac{\text{pari} + \text{dispari}}{2}$, che non è intero.

Oss. Sia n un intero. Allora $n^2 \equiv \begin{cases} 0 \\ 1 \end{cases} \pmod 4$

a seconda che n sia pari / dispari

$n = 2k \qquad n^2 = 4k^2 \equiv 0 \pmod 4$

$n = 2k+1 \qquad n^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$

(Si può anche controllare solo $0^2, 1^2, 2^2, 3^2$)

Supponiamo che x, y siano interi t.c. $x^2 - y^2 = 2022$

Allora $x^2 - y^2 \equiv 2022 \pmod 4$

$0 - 0 \qquad 2$

$0 - 1$

$1 - 0$

$1 - 1$

} non può succedere, quindi $x^2 - y^2 = 2022$ non ha soluz.

$x^2 - y^2 = n$ dove $n \equiv 2 \ (4)$ non ha soluz.

E $x^2 - y^2 = n$ con $n \not\equiv 2 \pmod 4$ ha soluz?

$(x-y)(x+y) = n$

$$\begin{cases} x - y = n/a \\ x + y = a \end{cases}$$

$$\Rightarrow \begin{cases} x = \dfrac{a + n/a}{2} \\ y = \dfrac{a - n/a}{2} \end{cases}$$

Se n è dispari: scegliendo $a = 1$ trovo $x = \dfrac{n+1}{2}$

$y = \dfrac{1-n}{2}$

$$\left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2 = \frac{n^2+2n+1-(n^2-2n+1)}{4} = \frac{4n}{4} = n$$

Se $n \equiv 0 \ (4)$, scelgo $a = 2$, $x = \frac{n/2+2}{2} = \frac{n}{4}+1$

$$y = \frac{n/2-2}{2} = \frac{n}{4}-1$$

$x^2 - y^2 = 3^{40}$: quante soluz. intere?

$3^{40} \equiv (-1)^{40} \equiv 1 \pmod 4$ automatica

$\#$ soluz $= \#\left\{ a \text{ divisore di } 3^{40} \text{ t.c. } \frac{a \pm 3^{40}/a}{2} \text{ interi} \right\}$

$= 2 \cdot 41$

Esempi di eqz. con congruenze

- $3X \equiv 6 \pmod{21} \rightsquigarrow X \equiv 2 \pmod{7}$

$\Downarrow$ $\qquad\qquad$ $\Uparrow$

$21 \mid 3X - 6 \iff 3 \cdot 7 \mid 3 \cdot (X-2)$

- $6X \equiv 7 \pmod{21} \rightsquigarrow$ impossibile

$\mcd(6, 21) \nmid 7$

$21 \mid 6X - 7 \implies 3 \mid 6X - 7 \implies 3 \mid 7$

$6X \equiv 7 \pmod{3} \implies 0 \equiv 7 \ (3)$

- $X^2 \equiv 0 \pmod 8 \iff 8 \mid X^2$ $\qquad X = 2^k \cdot d$

$\iff 2^3 \mid 2^{2k} \cdot d^2$ $\qquad d$ dispari

$\iff 2^3 \mid 2^{2k}$ $\qquad (2^3, d^2) = 1$

$\iff 3 \leq 2k$

$\iff k \geq 2 \iff X \equiv 0 \pmod 4$

$X \equiv 0, 4 \pmod 8$ $\qquad 8r$ $\qquad 8r+4$

- $X^2 \equiv 1 \pmod 8 \implies X^2 \equiv 1 \pmod 2 \Rightarrow X \equiv 1 \pmod 2$

$n \equiv 3 \pmod 8$ $\qquad n = 8h + 3$

Proviamo $x \equiv 1, \quad 3, \quad 5, \quad 7 \mod 8$

$1, \quad 9 \equiv 1, \quad (-3)^2 \equiv 9 \equiv 1, \quad 7^2 \equiv (-1)^2 \equiv 1 \pmod 8$

Conclusione: $x^2 \equiv 1 \pmod 8 \iff x$ dispari

$$x^2 - 1 \equiv 0 \pmod 8$$

$$\| $$

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

$x \equiv 1 \mod 4$

$x \equiv 3 \mod 4$

- $x^2 \equiv 1 \pmod{21} \iff \begin{cases} x^2 \equiv 1 \pmod 3 \\ x^2 \equiv 1 \pmod 7 \end{cases}$

$$21 \mid x^2 - 1 \iff \begin{cases} 3 \mid x^2 - 1 \\ 7 \mid x^2 - 1 \end{cases}$$

$$\begin{cases} x \equiv 1, 2 \pmod 3 \\ x \equiv 1, -1 \pmod 7 \end{cases}$$

$7 \mid x^2 - 1 = (x+1)(x-1) \iff 7 \mid x+1$ oppure $7 \mid x-1$

$\iff x \equiv -1 \ (7)$ " $x \equiv 1 \ (7)$

$x + 1 \equiv 0 \ (7)$

Le soluzioni sono gli x t.c. valga una fra

$$\begin{cases} x \equiv 1 \ (3) \\ x \equiv 1 \ (7) \end{cases} \qquad \begin{cases} x \equiv 1 \ (3) \\ x \equiv -1 \ (7) \end{cases} \qquad \begin{cases} x \equiv 2 \ (3) \\ x \equiv 1 \ (7) \end{cases} \qquad \begin{cases} x \equiv -1 \ (3) \\ x \equiv -1 \ (7) \end{cases}$$

$\updownarrow$ $\Updownarrow$ $\updownarrow$ $\updownarrow$

$x \equiv 1 \ (21)$ $\quad x \equiv 13 \ (21)$ $\quad x \equiv 8 \equiv B \ (21)$ $\quad x \equiv -1 \ (21)$

$\Rightarrow A$

Cerco A, che deve essere $\equiv -1 \ (7)$, $\equiv 1 \ (3)$

$-1 \equiv 6, \quad 13 \quad 20$

B $\quad 1, \quad 8, \quad 15$

$\hookrightarrow \equiv 2 \pmod 3$

$X^2 \equiv 1 \pmod{21} \iff X \equiv 1, 8, 13, 20 \pmod{21}$

- $5X \equiv 3 \pmod{48}$ ha soluz? Sì: $(5, 48) \mid 3$

$\Updownarrow$

$5X \equiv 3 - 48 \equiv -45 \pmod{48}$

$\iff X \equiv -9 \pmod{48}$

$\frac{48}{(5,48)}$

$5X = 3 \quad \rightarrow \quad X = 3/5$

Se io trovassi un K t.c. $5K \equiv 1 \pmod{48}$

$5X \equiv 3 \pmod{48}$

$X \equiv (5K)X \equiv 3K \quad (48)$

$\rightarrow 5K = 48h + 1 \quad \Leftrightarrow \quad 5K - 48h = 1 \quad (*)$

Strategia: risolvo $(*)$, e poi se voglio risolvere $5X \equiv ? \ (48)$

$\Leftrightarrow \quad X \equiv (5K)X \equiv K \cdot ? \ (48)$

Metodo di interpolaz. per sistemi di congruenze

(1) $\begin{cases} X \equiv 7 \quad (13) \\ X \equiv 11 \quad (27) \end{cases}$

$\begin{cases} X \equiv 1 \quad (13) \\ X \equiv 0 \quad (27) \end{cases}$

$\updownarrow$

$X \equiv A \quad (13 \cdot 27)$

$X = 7 \cdot A + 11 \cdot B \equiv \begin{cases} 7A \equiv 7 \quad (13) \\ 11B \equiv 11 \quad (27) \end{cases}$

$8 \cdot A + 12 B$

(2) $\begin{cases} X \equiv 8 \quad (13) \\ X \equiv 12 \quad (27) \end{cases}$

$\begin{cases} X \equiv 0 \quad (13) \\ X \equiv 1 \quad (27) \end{cases}$

$\updownarrow$

$X \equiv B \quad (13 \cdot 27)$

$A = 27$

$B = 13K = -26$

$13K = 27h + 1$

$27h - 13K = -1$

$-1, -2$

CONGRUENZE: ESEMPI

Titolo nota

TCR

7^3

(1) $\begin{cases} X \equiv 141 \pmod{343} \\ X \equiv 20 \pmod{70} \end{cases}$

(2) $\begin{cases} X \equiv 141 \pmod{343} \\ X \equiv 20 \pmod{71} \end{cases}$

(2) è risolubile (TCR) in quanto $(343, 71) = 1$

In particolare, (2) è equiv. a una singola congr.

$$X \equiv \bullet \pmod{343 \cdot 71}$$

(1) $(343, 70) = (343 - 4 \cdot 70, 70) = (63, 70)$

$= (63, 7) = 7$

$\parallel$

$(343 - 5 \cdot 70, 70) = (-7, 70)$

(1) $\overset{TCR}{\iff}$ $\begin{cases} X \equiv 141 \pmod{7^3} \\ X \equiv 20 \pmod{10} \\ X \equiv 20 \equiv 6 \pmod 7 \end{cases}$ $\Longrightarrow$ $X \equiv 141 \equiv 1 \pmod 7$

Siccome X non può essere simultan. $\equiv 1$, $\equiv 6 \mod 7$, il sistema non ha soluzioni

(3) $\begin{cases} X \equiv 141 \pmod{7^3} \\ X \equiv 22 \pmod{70} \end{cases}$ (TCR) $\iff$ $\begin{cases} X \equiv 141 \pmod{7^3} \\ X \equiv 22 \equiv 1 \pmod 7 \\ X \equiv 22 \pmod{10} \end{cases}$

implicata dalla precedente

$\begin{cases} X \cdot (X-2) = 0 \\ X = 0 \end{cases}$

$\downarrow$ TCR

la Soluzione esiste ed è unica mod $7^3 \cdot 10$

$$\begin{cases} x \equiv a_1 \ (p_1^{e_1}) \ , \quad x \equiv a_2 \ (p_1^{e_2}) \ , \ \dots \\ x \equiv b_1 \ (p_2^{f_1}) \ , \quad x \equiv b_2 \ (p_2^{f_2}) \ , \ \dots \\ \vdots \end{cases}$$

No soluz. $\rightarrow$ ~~$x \equiv 3 \mod 4$~~,

$x \equiv 23 \mod 32$ $\rightarrow$ $x \equiv 23 \equiv 3 \pmod 4$

$x \equiv 97 \ (128)$ $\rightarrow$ $x \equiv 97 \equiv 1 \ (32)$

$\rightarrow x \equiv 3 \ (4)$

$x \equiv 23 \ (32)$ $\rightarrow$ $x \equiv 3 \ (4)$

$x \equiv 151 \ (128)$ $\rightarrow$ $x \equiv 151 \equiv 23 \ (32)$

Le tre congr. sono equiv. alla singola $x \equiv 151 \ (128)$

TCR seconda versione

$$\{\text{classi di resto mod } (m\cdot n)\} \xrightarrow{\Phi} \{(\text{classi di resto mod } m, \text{ " " " } n)\}$$

$$a \bmod mn \longrightarrow (a \bmod m,\ a \bmod n)$$

è biiettiva $\iff (m,n)=1$

$$\begin{cases} x \equiv a_1 \bmod m \\ x \equiv a_2 \bmod n \end{cases}$$

Se Φ biiettiva: esiste $a \in \mathbb{Z}/mn\mathbb{Z}$ t.c. $a \equiv a_1 \bmod m$, $a \equiv a_2 \bmod n$

Applicazioni del TCR

1) Dim. che esistono 2021 interi consecutivi che NON sono primi.

$$\begin{cases} n \equiv 0 \pmod 2 \\ n+1 \equiv 0 \pmod 3 \\ n+2 \equiv 0 \pmod 5 \\ n+3 \equiv 0 \pmod 7 \\ \vdots \\ n+2020 \equiv 0 \pmod{p_{2021}} \end{cases}$$

TCR $\rightsquigarrow$ c'è una soluz. mod $(M := p_1 p_2 p_3 \cdots p_{2021})$, chiamiamola n_0

Posso scegliere $n_0 > M$

$$\begin{cases} n \equiv 0 \quad (2) \\ n \equiv -1 \quad (3) \\ n \equiv -2 \quad (5) \\ \quad \vdots \end{cases}$$

I numeri $n_0, n_0+1, \dots, n_0+2020$ sono composti:

per costruz., $n_0 + i$ è divisibile per il primo p_{i+1}.

Quindi: n_0+i può essere primo solo se è $= p_{i+1}$,

ma questo è impossibile perché $n_0+i > M > p_{i+1}$.

$$\begin{cases} n \equiv 0 \quad (2) \\ n+1 \equiv 0 \quad (3) \end{cases} \longleftrightarrow n \equiv 2 \pmod 6$$

$n_0 = 2$ non funziona

$n_0 = 8, \quad n_0 + 1 = 9$

2) Dim. che esistono 2021 interi consec. che NON SONO potenze perfetta (a^b , a intero >0 e b intero ≥ 2)

Oss. Se $n \equiv p \mod p^2$ con p primo $\Rightarrow$ n NON È pot. perfetta. $n \equiv p \ (p^2) \Rightarrow n \equiv p \equiv 0 \pmod p$

Supponiamo n pot. perfetta, $n = a^b$

$$p \mid a \cdot a \cdot a \cdots a \Rightarrow p \mid a$$

$$\Rightarrow p^b \mid n$$

$$\Rightarrow p^2 \mid n \Rightarrow n \equiv 0 \ (p^2)$$

Come prima considero

$$\begin{cases} n \equiv p_1 & (p_1^2) \\ n+1 \equiv p_2 & (p_2^2) \\ \vdots \\ n+2020 \equiv p_{2021} & (p_{2021}^2) \end{cases}$$

infinite soluz INTERE, una soluz. mod $(p_1 p_2 \cdots p_{2021})^2$

$\rightsquigarrow$ ogni soluz. di questo sistema (che ne ha ∞, per il TCR) risolve il problema.

Oss. Sia n intero positivo. Allora

$$n! + 2, \quad n! + 3, \quad \dots, \quad n! + n$$

Sono interi consec. compositi: infatti dato $k \le n$ si ha

$$k \mid n! + k$$

$n! = 1 \cdot 2 \cdot 3 \cdots \cdot k \cdot (k+1) \cdots n$

Un conteggio

$$\#\left\{ n \text{ interi} \;\middle|\; \begin{array}{l} 1 \le n \le 1000 \\ 2 \nmid n,\quad 3 \nmid n,\quad 5 \nmid n \end{array} \right\}$$

$$A_2 = \left\{ n \le 1000 \;\middle|\; 2 \mid n \right\} \qquad |A_2| = 500$$

$$A_3 = \left\{ n \le 1000 \;\middle|\; 3 \mid n \right\} \qquad |A_3| = \left\lfloor \frac{1000}{3} \right\rfloor$$

$$A_5 = \left\{ n \le 1000 \;\middle|\; 5 \mid n \right\} \qquad |A_5| = \left\lfloor \frac{1000}{5} \right\rfloor = 200$$

$$|A_2 \cup A_3 \cup A_5| = |A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_3 \cap A_5| - |A_2 \cap A_5| + |A_2 \cap A_3 \cap A_5| = 734$$

$$A_2 \cap A_3 = \left\{ n \le 1000 \;\middle|\; \begin{matrix} 2 \mid n \\ 3 \mid n \end{matrix} \right\} = \left\{ n \le 1000 \;\middle|\; 6 \mid n \right\}$$

$$|A_2 \cap A_3| = \left\lfloor \frac{1000}{6} \right\rfloor \qquad |A_3 \cap A_5| = \left\lfloor \frac{1000}{15} \right\rfloor \qquad |A_2 \cap A_5| = 100$$

$$|A_2 \cap A_3 \cap A_5| = \left\lfloor \frac{1000}{30} \right\rfloor$$

Per differenza: la risp. al probl. è 266

— o —

Secondo approccio: TCR. Conto i numeri fino a 990.

I numeri che mi interessano sono soluz. di 1 dei seguenti sistemi:

$$\begin{cases} X \equiv 1 \pmod 2 \\ X \equiv 1 \pmod 3 \\ X \equiv 1 \pmod 5 \end{cases} \qquad \begin{cases} X \equiv 1 \pmod 2 \\ X \equiv 2 \pmod 3 \\ X \equiv 1 \pmod 5 \end{cases}$$

$$\begin{cases} X \equiv 1 \pmod 2 \\ X \equiv 1 \pmod 3 \\ X \equiv 2 \pmod 5 \end{cases} \qquad \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5 \end{cases}$$

$$\begin{cases} X \equiv 1 \pmod 2 \\ X \equiv 1 \pmod 3 \\ X \equiv 3 \pmod 5 \end{cases} \qquad \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

$$\begin{cases} X \equiv 1 \pmod 2 \\ X \equiv 1 \pmod 3 \\ X \equiv 4 \pmod 5 \end{cases} \qquad \begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \end{cases}$$

Ogni sistema ha soluz unica $\pmod{30}$, cioè $\frac{990}{30} = 33$ soluz fra 1 e 990

Con 8 sistemi $\rightsquigarrow$ $33 \cdot 8$ soluzioni $= \frac{990}{30} \times 8$

Oss. Stiamo contando i numeri t.c. $(n, 30) = 1$.

La proprietà $(n, 30) = 1$ dipende solo da $n \bmod 30$, ed inoltre in $1 \le n \le 30$ ci sono $\varphi(30)$ classi coprime con 30. Ora $\varphi(30) = \varphi(2 \cdot 3 \cdot 5) =$

$$= \varphi(2) \cdot \varphi(3) \cdot \varphi(5) = 1 \times 2 \times 4 = 8$$

Oss. $(990 + i, 30) = (990 + i - 33 \cdot 30, 30) = (i, 30)$

Per controllare 991, ..., 1000 basta contr. 1, 2, ..., 10

Oss. $x^2 \equiv 4 \pmod{15} \iff \begin{cases} x^2 \equiv 4 \pmod 3 \\ x^2 \equiv 4 \pmod 5 \end{cases}$?

$15 \mid x^2 - 4 \iff 3 \mid x^2 - 4$ e $5 \mid x^2 - 4$

$y \equiv 4 \pmod{15} \iff \begin{cases} y \equiv 4 \pmod 3 \\ y \equiv 4 \pmod 5 \end{cases}$ $\forall y$ intero,

in partic. $y = x^2$

Sistemi con parametro

Al variare di $a \in \mathbb{Z}$ determinare le soluz. del sistema

$$\begin{cases} (6a-1)\,x \equiv 1 \pmod{21} \\ x \equiv a \pmod{35} \end{cases}$$

TCR ($\Leftarrow$)

$$\begin{cases} (6a-1)\,x \equiv 1 \quad (3) \\ (6a-1)\,x \equiv 1 \quad (7) \\ x \equiv a \quad (7) \\ x \equiv a \quad (5) \end{cases}$$

compatibili?

Se ho $\begin{cases} x \equiv a \ (7) \\ (6a-1)x \equiv 1 \ (7) \end{cases}$ allora $\begin{cases} x \equiv a \ (7) \\ (6a-1)\cdot a \equiv 1 \ (7) \end{cases}$

$$-a^2 - a - 1 \equiv 0 \ (7)$$

$$a^2 + a + 1 \equiv 0 \ (7) : \text{ vera solo per } a \equiv 2, 4 \ (7)$$

$$X \equiv a \quad (7)$$

$$6a-1 \equiv 6a-1 \quad (7)$$

$$X \cdot (6a-1) \equiv a \cdot (6a-1) \quad (\mathrm{mod}\ 7)$$

Logica: se $\begin{cases} X \equiv a \ (7) \\ (6a-1) \cdot X \equiv 1 \ (7) \end{cases}$ (II) $\Rightarrow a^2 + a + 1 \equiv 0 \ (7)$

$\Rightarrow a \equiv 2, 4 \ (7)$

Viceversa se a è uno di questi valori, la seconda congr (II) è equiv. a $\underbrace{a \cdot (6a-1)}_{\equiv 1 \ (7)} \cdot X \equiv a \ (7)$,

cioè a $X \equiv a \ (7)$

- $a \not\equiv 2, 4 \mod 7$: sist. non ha soluz
- $a \equiv 2, 4 \mod 7$

$$\begin{cases} (6a-1)x \equiv 1 & (3) \\ x \equiv a & (7) \\ x \equiv a & (5) \end{cases} \iff \begin{cases} x \equiv -1 & (3) \\ x \equiv a & (7) \\ x \equiv a & (5) \end{cases}$$

$$\iff \begin{cases} x \equiv -1 & (3) \\ x \equiv a & (35) \end{cases}$$

$$\iff x \equiv 70 \cdot (-1) + 36 \cdot a \quad (105)$$

$$\begin{cases} x \equiv 0 & (3) \\ x \equiv 1 & (35) \end{cases} \qquad \begin{cases} x \equiv 1 & (3) \\ x \equiv 0 & (35) \end{cases}$$

$$x \equiv 36 \quad (105) \qquad x \equiv 70 \quad (105)$$

Eqz. di secondo grado mod p

$$ax^2+bx+c=0 \qquad a\neq 0$$

$$\Updownarrow$$

$$x^2+b/a\,x+c/a=0 \iff \left(x+\frac{b}{2a}\right)^2-\frac{b^2}{4a^2}+\frac{c}{a}=0$$

$$\iff \left(x+b/2a\right)^2=\frac{b^2-4ac}{4a^2}$$

$$x+b/2a=\pm\frac{\sqrt{b^2-4ac}}{2a} \qquad x=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

Sia ora p un n° primo $\neq 2$. Allora

$a x^2 + b x + c \equiv 0 \pmod p$

$a \not\equiv 0 (p) \iff p \nmid a$

$(p, a) = 1$

$\rightsquigarrow$ esiste a^{-1} (classe di resto mod p) t.c. $a \cdot a^{-1} \equiv 1 (p)$

$x^2 + a^{-1} b x + a^{-1} c \equiv 0 \quad (p)$

Se $p \neq 2$: posso scrivere $x + \frac{b}{2a}$

$\hookrightarrow 2^{-1} \cdot a^{-1} \cdot b$

$$\left(x + b/2a\right)^2 + c/a - b^2/4a^2 \equiv 0 \quad (p)$$

$$\rightsquigarrow \quad x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

In particolare, vogliamo studiare $X^2 \equiv a \pmod p$

- $a \equiv 0 \ (p) \rightsquigarrow X^2 \equiv 0 \ (p) \rightsquigarrow X \equiv 0 \ (p)$
- se esiste una soluz., $s^2 \equiv a \pmod p$, allora

$$X^2 \equiv a \ (p) \iff X^2 \equiv s^2 \ (p)$$
$$\iff X^2 - s^2 \equiv 0 \ (p)$$
$$\iff (X+s)(X-s) \equiv 0 \ (p)$$
$$\iff p \mid X+s \quad \text{o} \quad p \mid X-s$$
$$\iff X \equiv -s \ (p) \quad \text{o} \quad X \equiv s \ (p)$$

$$X^2 \equiv 4 \ (5) \iff X \equiv \pm 2 \ (5)$$

$$A^2 + A + 1 \equiv 0 \quad (7)$$

$$A \equiv \frac{-1 \pm \sqrt{1-4}}{2} \equiv$$

$$\equiv \frac{-1 \pm \sqrt{4}}{2} \equiv (-1 \pm 2) \cdot 4$$

$$\equiv 4, 2 \quad (7)$$

CONGRUENZE IN TUTTO IL LORO SPLENDORE

Titolo nota 11/10/2021

Inversi $5X \equiv 3 \pmod{48}$

Idea: calcolare a classe in $\mathbb{Z}/48\mathbb{Z}$ t.c. $5a \equiv 1 \ (48)$

$5X \equiv b \pmod{48} \xrightarrow{\cdot a} 5aX \equiv ab \ (48)$

$5a - 1 = -48k \iff 5a + 48k = 1$

$48 = 9 \cdot 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1 \longrightarrow 1 = 3 - 2 = 3 - (5-3) = 2 \cdot 3 - 5$

$2 \cdot 48 - 19 \cdot 5$

$2 \cdot (48 - 5 \cdot 9) - 5$

$1 = 2 \cdot 48 + (-19) \cdot 5$

$$1 \equiv (-19) \cdot 5 \pmod{48} \rightsquigarrow a \equiv -19 \pmod{48}$$

$$5X \equiv 3 \ (48) \begin{cases} \rightarrow 5X \equiv -45 \ (48) \rightarrow X \equiv -9 \ (48) \\ \rightarrow (-19) \cdot 5 \cdot X \equiv 3 \cdot (-19) \ (48) \end{cases}$$

$$X \equiv -9 \pmod{48}$$

$$5X \equiv 4 \ (48) \rightarrow X \equiv 4 \cdot (-19) \pmod{48}$$

$$5 \cdot a \equiv 1 \ (48) \iff \begin{cases} 5a \equiv 1 \ (3) \\ 5a \equiv 1 \ (16) \end{cases} \iff \begin{cases} a \equiv 2 \ (3) \\ -a \equiv 3 \\ a \equiv -3 \ (16) \end{cases}$$

$$-19 \equiv a \equiv 29 \ (48)$$

Congruenze + succ. per ricorr.

$$\begin{cases} a_1 = 3 \\ a_{n+1} = a_n^2 - a_n + 1 \end{cases}$$

Tesi: per $m \neq n$ si ha $(a_m, a_n) = 1$

Soluz. Osserviamo che dobbiamo in partic. dim

$$(3, a_n) = (a_1, a_n) = 1 \qquad \forall n > 1$$

$a_2 = 7$ $\qquad a_2 \equiv 3^2 - 3 + 1 \equiv 1 \quad (3)$

Passo induttivo:

$$a_3 \equiv a_2^2 - a_2 + 1 \equiv 1^2 - 1 + 1 \equiv 1 \ (3)$$

Se $a_n \equiv 1 \ (3)$, allora $a_{n+1} \equiv a_n^2 - a_n + 1$

$$\equiv 1^2 - 1 + 1 \equiv 1 \quad (3)$$

Per simmetria mi basta trattare il caso $m < n$.

Dim. che $(a_m, a_n) = 1$ facendo vedere che $a_n \equiv 1 \ (a_m)$

($a_n - 1 = h \cdot a_m \iff a_n - h \cdot a_m = 1$,

e per Bézout $(a_m, a_n) = 1$)

Si ha $a_{m+1} = a_m^2 - a_m + 1 \equiv 1 \pmod{a_m}$

e poi per induzione esattamente come prima

(se $a_n \equiv 1 \ (a_m) \implies a_{n+1} \equiv 1 \ (a_m)$)

Una congr. espon.

$$\#\{\, d \text{ divisori positivi di } 3^{40}\cdot 5^{25} \text{ t.c. } d \equiv 1 \ (7)\}$$

Ogni tale d è della forma $\boxed{3^a \cdot 5^b}$ con $0 \le a \le 40$, $0 \le b \le 25$

$$2^a \cdot 4^b = 2^a \cdot 2^{2b} = 2^{a+2b}$$

$3^0 = 1$, $3^1 = 3$, $3^2 = 9 \equiv 2$, $3^3 \equiv 6 \equiv -1 \pmod 7$

$$\operatorname{ord}_7(3) = 6$$

$$\operatorname{ord}_7(3) \mid \varphi(7) = 6.$$

$3^4 \equiv -3 \equiv 4 \ (7)$ $\qquad$ $3^5 \equiv 12 \equiv 5 \ (7)$

Quindi: $3^a \cdot 5^b \equiv 3^a \cdot 3^{5b} \equiv 1 \pmod 7$

$\iff 3^{a+5b} \equiv 1 \pmod 7$ $\qquad$ (*)

Fatto $a^x \equiv 1 \pmod p \iff \mathrm{ord}_p(a) \mid x$

(*) $\iff a + 5b \equiv 0 \ (6) \iff a - b \equiv 0 \ (6)$

$\iff a \equiv b \ (6)$

NO!

$2^{a+5b} \equiv 1 \pmod 7 \iff a + 5b \equiv 0 \ (7-1)$

Oss Siccome so che $\text{ord}_p(a) \mid p-1$, allora se $p-1 \mid x$ in particolare $\text{ord}_p(a) \mid x$, e quindi $a^x \equiv 1 \pmod p$

$$\#\left\{ d \mid 3^{40} \cdot 5^{25},\ d \equiv 1 \ (7) \right\} = \#\left\{ (a,b) \;\middle|\; \begin{array}{l} a \equiv b \ (6) \\ 0 \le a \le 40 \\ 0 \le b \le 25 \end{array} \right\}$$

	0	1	2	3	4	5
a	7	7	7	7	7	6
b	5	5	4	4	4	4

$$35 + 35 + 28 + 28 + 28 + 24$$

Congr. polinomiale

$X^{27} \equiv X^{15} \pmod{77}$: contare le soluz. mod 77

TCR $\Leftrightarrow$ $\begin{cases} X^{27} \equiv X^{15} \pmod 7 \\ X^{27} \equiv X^{15} \pmod{11} \end{cases}$ $\Leftrightarrow$ $\begin{cases} X^{27} - X^{15} \equiv 0 \ (7) \\ X^{27} - X^{15} \equiv 0 \ (11) \end{cases}$

($Y = X^{27} - X^{15}$ $\quad Y \equiv 0 \ (77) \Leftrightarrow \begin{cases} Y \equiv 0 \ (7) \\ Y \equiv 0 \ (11) \end{cases}$)

Oss $X^7 \equiv X \pmod 7$

$X^{7+K} \equiv X^7 \cdot X^K \equiv X \cdot X^K \equiv X^{1+K}$

E' vero che $X^{27} \equiv X^3 \ (7) \quad \forall x \in \mathbb{Z}/7\mathbb{Z}$,

ma NON È VERO che $X^{24} \equiv 1$

$X^{27} - X^{15} = X^{15}(X^{12} - 1) \equiv 0 \ (7) \iff$ $7 \mid X$ oppure

$\begin{cases} 7 \mid X^{12} - 1 \\ 7 \nmid X \end{cases}$

Quindi: se $7 \mid X$ la congr. è vera;

se $7 \nmid X$, " " " " se e solo se

$X^{12} - 1 \equiv 0 \ (7)$

Siccome $7 \nmid X$, so che $X^6 \equiv 1 \ (7)$

$\Rightarrow X^{12} \equiv 1 \ (7)$

Cioè ogni $x \in \mathbb{Z}/7\mathbb{Z}$ rispetta $X^{27} - X^{15} \equiv 0 \ (7)$

$$X^{27} - X^{15} \equiv X^{15}\left(X^{12} - 1\right) \equiv 0 \quad (11)$$

- Se $X \equiv 0 \ (11)$ OK
- Se $X \not\equiv 0 \ (11)$, è soluz. $\iff X^{12} \equiv 1 \ (11)$

$\iff X^{10} \cdot X^2 \equiv 1 \ (11)$

$\iff X^2 \equiv 1 \ (11)$

$\iff X \equiv \pm 1 \ (11)$

$$X^{27} - X^{15} \equiv 0 \ (77) \iff \begin{cases} X \equiv \text{qualsiasi cosa} \pmod 7 \\ X \equiv -1, 0, 1 \pmod{11} \end{cases}$$

$\updownarrow$

21 soluzioni mod 77

Sistema

Determinare, al variare di $a \in \mathbb{Z}$, le soluz. di

$$\begin{cases} 3^x \equiv 7^a \pmod{11} \\ (a+3)x \equiv 2 \pmod{5} \end{cases}$$

$7^4 \equiv 3 \pmod{11}$

$$3^x \equiv 7^a \pmod{11} \iff (7^4)^x \equiv 7^a \pmod{11}$$

$$\left(\iff 7^{4x-a} \equiv 1 \pmod{11}\right)$$

$$\iff 4x - a \equiv 0 \pmod{\mathrm{ord}_{11} 7}$$

Gatto ++ $\quad a^x \equiv a^y \pmod p \iff x \equiv y \pmod{ord_p(a)}$

(se $p \nmid a$)

$ord_{11}(7) \mid 10$, quindi è ~~1~~, ~~2~~, ~~5~~, 10

$7^5 \equiv -1 \ (11)$: l'ordine non è 5

$$\begin{cases} 4x \equiv a \ (10) \\ (a+3)x \equiv 2 \ (5) \end{cases} \qquad \left[\begin{cases} 4x \equiv a \ (2) \\ 4x \equiv a \ (5) \\ (a+3)x \equiv 2 \ (5) \end{cases} \right]$$

$$\begin{cases} a \equiv 0 \ (2) \\ -x \equiv a \ (5) \iff x \equiv -a \ (5) \\ -a(a+3) \equiv 2 \ (5) \end{cases}$$

$\longrightarrow$ condizione sul parametro: se non è rispettata non ci sono soluzioni

$$a^2 + 3a + 2 \equiv 0 \ (5) \iff a \equiv -1, -2 \ (5)$$
$$\equiv 4, 3$$

$$(a+1)(a+2)$$

Conclusione: • se a è dispari oppure $a \equiv 0, 1, 2 \ (5)$
il sistema non ha soluz.

• se invece a è pari e $\equiv 3$ o $4 \ (5)$:
il sistema ha la soluz. $X \equiv -a \ (5)$

(Ha soluz $\iff a \equiv 4, 8 \pmod{10}$)

φ di Eulero

Trovare gli n interi >0 t.c. $\varphi(n) = \frac{2}{5} n$.

Scriviamo $n = p_1^{e_1} \cdots p_k^{e_k}$,

$$\varphi(n) = (p_1-1) \cdot p_1^{e_1-1} \cdot (p_2-1) \cdot p_2^{e_2-1} \cdots (p_k-1) \cdot p_k^{e_k-1}$$

$$\varphi(p^k) = (p-1) \cdot p^{k-1}$$

$$\frac{2}{5} n = \frac{2}{5} \frac{p_1^{e_1}}{p_1^{e_1-1}} \cdots \frac{p_k^{e_k}}{p_k^{e_k-1}}$$

$5 \cdot (p_1 - 1)(p_2 - 1) \dots (p_k - 1) = 2 \cdot p_1 \cdot p_2 \dots p_k$ (*)

$p_1 < p_2 < \dots < p_k$: $p_k \mid 5 \underbrace{(p_1 - 1)}_{< p_k} \dots \underbrace{(p_k - 1)}_{< p_k}$

$\Rightarrow p_k = 5$

$\Rightarrow n = 2^a \cdot 3^b \cdot 5^c$, con $c \geq 1$ e $a, b \geq 0$

Se $b \geq 1$: $3 \mid 2 \cdot p_1 \dots p_k = 5 \cdot (p_1 - 1) \dots (p_k - 1)$

Fattori possibili: 5, $(2-1)$, $(3-1)$, $(5-1)$

assurdo

Caso 1: $n = 5^k$ $\quad \varphi(n) = 4 \cdot 5^{k-1} \neq \frac{2}{5} n$

Caso 2: $n = 2^a \cdot 5^b$ $\quad \varphi(2^a \cdot 5^b) = 2^{a-1} \cdot 4 \cdot 5^{b-1}$

$= \frac{2}{5} \cdot 2^a \cdot 5^b = \frac{2}{5} n$

Risposta: tutti e soli gli $n = 2^a \cdot 5^b$ con $a, b \geq 1$

Divisori e $\varphi(n)$

Sia $d(n) =$ n° divisori > 0 di n

(i) Dim. che $d(n) + \varphi(n) \leq n + 1 \quad \forall n$

(ii) Caratt. n t.c. $d(n) + \varphi(n) = n$

1	2	3	4	...	n

$d \mid n, \quad (d, n) = 1 \Rightarrow d = 1$

$D_n = \{ \text{divisori di } n \}$ $\qquad C_n = \{ 1 \le k \le n, \quad (k, n) = 1 \}$

$$|D_n \cup C_n| \le n$$

$$\| \qquad \overbrace{\qquad\qquad}^{n}$$

$$|D_n| + |C_n| - |D_n \cap C_n| = d(n) + \varphi(n) - 1$$

(ii) $\boxed{d(n) + \varphi(n) = n}$: vuol dire che c'è ESATTAMENTE 1 NUMERO in $\{1, \dots, n\}$ che non è né div.

né coprimo con n.

$n - d_1$ e $n - d_2$

Oss Se $d \mid n$, $d \mid (n-d, n) \neq 1$ (se $d \neq 1$)

$n - d \mid n \Rightarrow n - d \mid n - (n-d) = d$

$n - d \leq d \quad n \leq 2d$

Prendo $d = p$, il più piccolo fattore primo di n.

- $(n-p, n) = p$
- $n - p \mid n \iff n - p \mid p \iff$

$$\begin{cases} n - p = 1 \iff n = p + 1 \text{ NO} \\ n - p = p \iff n = 2p \end{cases}$$

$p = 2$

$n = 4$

Similmente: si prende $n-2p \mid n \iff n-2p \mid 2p$

Concl: se $n \neq 6, 8, 9$, allora $n-p$ e $n-2p$ non sono né div. di n, né coprimi con n

Le soluz. di $d(n) + \varphi(n) = n$ sono $n = 6, 8, 9$

ANCORA CONGRUENZE

Titolo nota 04/11/2021

Es 75

$$\begin{cases} x^{660} \equiv 1 \quad (847) \\ x \equiv 11 \quad (13) \end{cases}$$

$(847, 13) = 1$

- Se x è soluzione, $(x, 847) = 1$

$x^{660} = 1 + 847k \Rightarrow$ se $p \mid x$ e $p \mid 847$, per diff. $p \mid 1$, assurdo

- $x^{\varphi(847)} \equiv 1 \quad (847)$
- Ci interessa fattorizzare $847 = 7 \cdot 121 = 7 \cdot 11^2$

Oss. Se n non è primo, allora $\exists\, d$ divisore di n, $d \neq 1$, con $d \leq \sqrt{n}$.

$n = a \cdot b$: se sia a sia b sono $> \sqrt{n}$,

allora $n = ab > \sqrt{n} \cdot \sqrt{n} = n$, assurdo.

- $\varphi(7 \cdot 11^2) = \varphi(7)\,\varphi(11^2) = 6 \cdot 11 \cdot (11-1) = 660$
- Per Eulero-Fermat, $(x, 847) = 1 \Rightarrow x^{660} \equiv 1 \ (847)$

$\Rightarrow$ Soluz. prima congr: sono gli interi X coprimi con 847

" " " " " " 77

$\Leftrightarrow$

$$\begin{cases} X^{660} \equiv 1 \ (847) \\ X \equiv 11 \ (13) \end{cases} \Leftrightarrow \begin{cases} X \not\equiv 0 \ (7) \\ X \not\equiv 0 \ (11) \\ X \equiv 11 \ (13) \end{cases}$$

6 possibilità

10 "

Il fatto che x risolva il sistema dipende solo da $x \bmod 7 \cdot 11 \cdot 13$ $\qquad$ 1001 $\qquad$ 11

Ci sono 60 classi di resto mod $7 \cdot 11 \cdot 13$ che risolvono

Congr. modulo potenze di primi

$$(1)\begin{cases} ax \equiv 2 \pmod{12} \\ (2)\ gx \equiv a^2 + 2a - 3 \pmod{3^4} \end{cases} \longrightarrow ax \equiv 2 \pmod{3}$$

Studiamo (2):

- Mod 3: $0 \equiv a^2 + 2a \pmod 3 \iff 0 \equiv a(a+2) \pmod 3$

  Guardando (1) scartiamo $a \equiv 0$, quindi $a \equiv 1 \pmod 3$

- Mod 9: $0 \equiv a^2 + 2a - 3 \pmod 9$

$0 \equiv \underbrace{(a+3)}(a-1) \pmod 9$

Non ci sono fattori 3, quindi invertibile mod 9

$\Rightarrow \quad 0 \equiv a - 1 \pmod 9$

$\Rightarrow \quad a \equiv 1 \ (9)$

$a = 3K+1 \rightsquigarrow \quad 0 \equiv 9K^2 + 6K + 1 + 6K + 2 - 3 \ (9)$

$0 \equiv 3K \ (9) \qquad 9 \mid 3K$

$0 \equiv K \ (3) \qquad 3 \mid K$

$a = 3(3h) + 1 = 9h + 1$

- Mod 81:

$$9X \equiv (9h+1)^2 + 2\cdot(9h+1) - 3 \quad (81)$$
$$\equiv 81h^2 + 18h + 1 + 18h + 2 - 3 \quad (81)$$
$$\equiv 36h \quad (81)$$

$\Leftrightarrow$ $X \equiv 4h \pmod 9$

- Abbiamo trovato che una condizione NECESSARIA affinché il sistema abbia soluz. è $a \equiv 1 \pmod 9$

Se questa condiz. è verificata, $a = 1 + 9h$, il sist. è equiv. a

$$\begin{cases} (1+9h)X \equiv 2 \quad (12) \\ X \equiv 4h \pmod 9 \end{cases}$$

$$\begin{cases} (1+9h)\,x \equiv 2 & (4) \\ (1+9h)\,x \equiv 2 & (3) \\ x \equiv 4h & (9) \end{cases}$$

$$\begin{cases} (1+h)\,x \equiv 2 & (4) \quad \circledast \\ x \equiv 2 & (3) \\ x \equiv 4h & (9) \end{cases}$$

$$\Downarrow$$

$$\begin{cases} x \equiv 4h & (3) \\ x \equiv 2 & (3) \end{cases}$$

sono compatibili $\iff h \equiv 2\ (3)$

$\circledast$ Ha soluz $\iff (1+h, 4) \mid 2$

$\iff h+1 \not\equiv 0\ (4)$

$\iff h \not\equiv 3\ (4)$

Le sue soluz. sono: $(1+h)x \equiv 2 \quad (4)$

- se $1+h$ è dispari: $x \equiv 2(1+h) \quad (4)$

  $1^2 \equiv 3^2 \equiv 1 \quad (4)$ $\qquad x \equiv 2 \quad (4)$

- se $1+h$ è pari: allora $1+h \equiv 2 \, (4)$

  $2x \equiv 2 \quad (4)$

  $x \equiv 1 \quad (2)$

Il sistema ha soluz. solo se a è della forma

$$a = 9h+1 = 9(3l+2)+1$$

e $\quad h \not\equiv 3(4) \iff 3l+2 \not\equiv 3 \, (4)$

$\iff 3l \not\equiv 1 \quad (4) \iff l \not\equiv 3 \, (4)$

Es Dim. che $x^2 \equiv 14 \pmod{5^k}$ ha soluz $\forall k \geq 1$

- $k=1$: c'è la soluz. $x_1 \equiv 2 \ (5^1)$
- per induzione: supponiamo di avere x_k t.c. $x_k^2 \equiv 14 \ (5^k)$

Calcolo $x_k^2 = 14 + a \cdot 5^k$

Se $x_{k+1}^2 \equiv 14 \ (5^{k+1}) \Rightarrow x_{k+1}^2 \equiv 14 \ (5^k)$

Cerco x_{k+1} della forma $x_k + b \cdot 5^k$

$$14 \overset{?}{\equiv} (x_k + b \cdot 5^k)^2 \equiv x_k^2 + 2b x_k \cdot 5^k + b^2 \cdot 5^{2k} \ (5^{k+1})$$

$$\equiv 14 + a \cdot 5^k + 2b \cdot x_k \cdot 5^k \ (5^{k+1})$$

$$\Leftrightarrow \quad 0 \equiv 5^k (a + 2b \cdot x_k) \ (5^{k+1})$$

$$\Leftrightarrow \quad 0 \equiv a + 2b x_k \ (5)$$

$\Rightarrow \quad b \equiv -\frac{a}{2x_k} \quad (5)$: 2 è invertibile

e $(x_k, 5) = 1$ perché

per induz. $x_k \equiv 2 \ (5)$

Quindi ho costruito x_{k+1} e finisco per induzione.

Es veloce

Sia $p > 3$ un n° primo. Allora

$$p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$$

$$6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) \overset{?}{\equiv} 0 \quad (p)$$

$$3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \overset{?}{\equiv} 0 \quad (p)$$

$$\downarrow$$

Per Fermat, $\downarrow \equiv 3 \cdot 1 + 2 \cdot 1 + 1 - 6 \equiv 0 \ (p)$

Oss $a^{p-1} \equiv 1 \ (p) \iff a^{p-2} \equiv 1/a \ (p)$

$$2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv 1/2 + 1/3 + 1/6 - 1 \equiv 0 \ (p)$$

Cubi mod p

$p = 32003$. Voglio sapere quante soluz. ha

- $\begin{cases} x^3 \equiv 1754 \ (p) \\ x^{p-1} \equiv 1 \ (p) \end{cases}$

$x^{32001+1} \equiv 1 \ (p)$ $\qquad (x^3)^{\frac{32001}{3}} \cdot x \equiv 1 \ (p)$

$$\Rightarrow \quad 1754^{10667} \cdot X \equiv 1 \quad (p)$$

$$\Rightarrow \quad X \equiv \left(1754^{10667}\right)^{-1} \pmod p$$

$$\qquad\qquad\qquad\qquad \parallel$$

$$1754^{-10667}$$

Sia ora $y := 1754^{-10667} \pmod p$. Osserviamo che $(y,p)=1$

$$y^3 \equiv 1754^{-32001} \cdot 1754^{p-1} \equiv 1754 \quad (p)$$

$$p-1 \equiv 0, 1 \quad (3)$$

Es $p=7$, $\quad X^3 \equiv 1 \quad (7)$ ha 3 soluz., $1, 2, 4$

Teo (Wilson) p primo $\Rightarrow$ $(p-1)! \equiv -1 \pmod p$

Dim

$1 \cdot \underbrace{2 \cdot 3 \cdot 4}_{\equiv 1 \,(7)} \cdot 5 \cdot 6 \equiv -1 \quad (7)$

$8 \equiv 1 \quad (7)$

Ogni classe di resto fra 1 e $p-1$ ha un inverso $\pmod p$. Una classe X coincide con X^{-1}

$\Leftrightarrow X \equiv X^{-1} \quad (p) \quad \Leftrightarrow X^2 \equiv 1 \quad (p)$

$\Leftrightarrow X \equiv \pm 1 \quad (p)$

Metto le classi di resto a coppie di inversi, resta fuori solo $p-1 \equiv -1 \pmod p$

Esponenziale + lineare

Trovare gli n t.c. $3^n \equiv n+4 \pmod{10}$

n	0	1	2	3	4	5	6	7	8	9	10	
$3^n \bmod 10$	1	3	-1	(-3)	1	3	-1	-3	1			}
$n+4 \bmod 10$	4	5	6	(7)	8	9	0	1	2	3	4	

Oss cruciale Se $n \equiv n' \pmod{20}$ ho <u>SIA</u>

$n \equiv n' \ (4) \Rightarrow 3^n \equiv 3^{n'} \pmod{10}$, <u>SIA</u>

$n \equiv n' \ (10) \Rightarrow n+4 \equiv n'+4 \pmod{10}$

In particolare: n è soluz. $\Leftrightarrow$ n' è soluzione, cioè la proprietà di essere soluz. dipende solo da $n \bmod 20 = \text{m.c.m.}(4, 10)$

Sia ora p un n° primo. Determinare il n° di soluz. di $3^n \equiv n + 4 \ (p)$ con $1 \leq n \leq p(p-1)$

$$n \equiv 3^n - 4 \ (p)$$

Se n è $0 \pmod{p-1}$, allora $3^n - 4 \equiv -3 \ (p)$

e quindi è soluz $\Leftrightarrow$ $\begin{cases} n \equiv -3 \ (p) \\ n \equiv 0 \ (p-1) \end{cases}$

$n = i + k(p-1) \quad \Rightarrow \quad 3^n \equiv 3^i \, 3^{k(p-1)}$

$\equiv 3^i \left(3^{p-1}\right)^k \pmod p$

$\equiv 3^i \pmod p$

C'è una e una sola soluz. per ogni classe di resto

mod $p-1$ mod $p\cdot(p-1)$

$\Rightarrow$ $p-1$ soluzioni.

$p \equiv 3 \ (4) \Rightarrow x^2 + 1 \equiv 0 \ (p)$ non ha soluzioni

Supponiamo che x sia una soluzione.

① $x^2 \equiv -1 \ (p) \Rightarrow \boxed{x^4 \equiv 1 \ (p)}$ ②

$(x, p) = 1 \qquad \text{ord}_p(x)$

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

Da ② segue che $\operatorname{ord}_p(x) \mid 4$

Se $\operatorname{ord}_p(x) = 1$ o 2, $\quad X^2 \equiv 1 \quad (p)$

$\|\|$

-1

$\iff 2 \equiv 0 \quad (p)$, impossibile per $p > 2$

Se $\operatorname{ord}_p(x) = 4 \implies 4 \mid p-1 \implies p \equiv 1 \quad (4)$

Oss $\quad X^8 \equiv -1 \quad (p) \implies \operatorname{ord}_p(x) = 16 \implies 16 \mid p-1$

$X^{16} \equiv 1 \quad (p)$ $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\Downarrow$

$p \equiv 1 \quad (16)$

Oss. Sia $p > 2$ primo. Soluz. di $X^2 \equiv 1 \ (p^k)$?

$$(X+1)(X-1) \equiv 0 \ (p^k)$$

$$(X+1, X-1) = (X+1, (X+1)-(X-1)) = (X+1, 2)$$

$$\text{o} \quad X+1 \equiv 0 \ (p^k) \quad \text{o} \quad X-1 \equiv 0 \ (p^k)$$

$$\Rightarrow \quad X \equiv \pm 1 \ (p^k)$$

$$p \mid X+1 \qquad p \mid X-1$$

RESIDUI K-ESIMI MOD p

Titolo nota

Criterio di Eulero

p primo, n intero, poniamo

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{se } p \nmid n \text{ e } X^2 \equiv n \pmod p \text{ si risolve} \\ -1 & \text{se } p \nmid n \text{ e } X^2 \equiv n \pmod p \text{ NON si risolve} \\ 0 & p \mid n \end{cases}$$

Dim. che $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod p$ (per $p > 2$)

Oss 1: $\left(n^{\frac{p-1}{2}}\right)^2 \equiv n^{p-1} \equiv \begin{cases} 0 & \text{se } p \mid n \\ 1 & \text{se } p \nmid n \text{ per Fermat} \end{cases}$

Se $p \nmid n$: $n^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

Oss 2 Se $n \equiv a^2 \pmod{p}$, allora

$$n^{\frac{p-1}{2}} \equiv a^{2 \cdot \frac{p-1}{2}} \equiv a^{p-1} \equiv 1 \pmod{p}$$

Oss 3 Sia $f(x)$ un polinomio a coefficienti in $\mathbb{Z}/p\mathbb{Z}$.

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

con $a_n, a_{n-1}, \ldots, a_0 \in \mathbb{Z}/p\mathbb{Z}$

Quante soluzioni ha $f(x) \equiv 0 \pmod{p}$? Non più di n.

Teo (Ruffini) Se $f(x)$ è un polinomio a coefficienti ...

↳ e se $f(x_0) \equiv 0$, allora $f(x) \equiv (x - x_0)\, g(x)$

Se $f(x) \equiv 0 \ (p)$ ha una soluzione x_1, posso scrivere

$f(x) \equiv (x - x_1) \cdot g(x)$ $\quad$ $g(x)$ = polinomio di grado $n-1$

Ora: $f(x) \equiv 0 \ (p) \iff (x - x_1) \cdot g(x) \equiv 0 \ (p)$

$\iff x - x_1 \equiv 0 \ (p)$ o $g(x) \equiv 0 \ (p)$

Dimostriamo allora che

n° soluz. di $f(x) \equiv 0 \mod p \leq$ grado $f(x)$

- Se grado $f(x) = 1$: $f(x) = ax + b$, $a \not\equiv 0 \ (p)$

$ax + b \equiv 0 \ (p) \iff x \equiv -b/a \ (p)$

e $f(x)$ ha 1 soluzione

- Se grado $f(x) \geq 2$:

  * se non ci sono soluzioni: Ok!

  * se invece esiste una soluz. x_1 $\quad f(x_1) \equiv 0 \ (p)$

  Scrivo $f(x) = (x - x_1)\, g(x)$ e

  $$\{\text{soluz. di } f(x) \equiv 0 \ (p)\} = \{x_1\} \cup \{\text{soluz. } g(x) \equiv 0 \ (p)\}$$

  dove grado $g(x)$ = grado $f(x) - 1$.

  Per ip. induttiva $g(x) \equiv 0 \ (p)$ ha $\leq$ grado $g(x)$ soluz.

  $$\Rightarrow \#\{\text{sol. } f(x) \equiv 0 \ (p)\} \leq 1 + \underbrace{\deg}_{\text{grado}}\, g(x)$$

  $$= 1 + (\deg f(x) - 1) = \deg f(x)$$

  □

⚠ $f(x) = x^2 - 1$ $\quad f(x) \equiv 0 \pmod 8$ ha 4 soluzioni

(più di $2 = \deg f(x)$)

Oss 4 $\quad n^{\frac{p-1}{2}} \equiv 1 \pmod p$: per quali n?

Consideriamo $f(x) = x^{\frac{p-1}{2}} - 1$. Sappiamo che se $a \not\equiv 0 (p)$ è quadr. mod p, allora $f(a) \equiv 0 \ (p)$

Ma quanti sono i quadrati mod p?

$$h : \left(\mathbb{Z}/p\mathbb{Z}\right)^* \longrightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^*$$
$$x \longmapsto x^2$$

$\{$quadrati mod $p\}$ $=$ imm h

Si ha $h(a) = h(b) \iff a^2 \equiv b^2 \pmod p$

$$\Leftrightarrow \quad (a-b)(a+b) \equiv 0 \quad (p)$$

$$\Leftrightarrow \quad a-b \equiv 0 \ (p) \quad \text{oppure} \quad a+b \equiv 0 \ (p)$$

$$\Leftrightarrow \quad a \equiv b \ (p) \quad \text{o} \quad a \equiv -b \ (p)$$

In particolare, $h\left|_{\left\{1, 2, \dots, \frac{p-1}{2}\right\}}\right.$ è iniettiva

$$h(-i) = h(i) \qquad h\left(\frac{p+1}{2}\right) = h\left(p - \frac{p+1}{2}\right) = h\left(\frac{p-1}{2}\right)$$

$$h\left(\frac{p+3}{2}\right) = h\left(\frac{p-3}{2}\right)$$

Quindi: $\left|\operatorname{imm} h\right| = \left|\operatorname{imm} h\left|_{\left\{1, 2, \dots, \frac{p-1}{2}\right\}}\right.\right| = \frac{p-1}{2}$.

Combinando tutto sappiamo che:

- $\{\text{radici di } f(x) = x^{\frac{p-1}{2}} - 1\} \geq \{\text{quadrati mod } p\}_{\neq 0}$
- $|\{\text{radici di } f(x)\}| \leq \frac{p-1}{2}$
- $|\{\text{quadr} \neq 0 \ (p)\}| = \frac{p-1}{2}$

$\Rightarrow \{\text{radici di } f(x)\} = \{\text{quadrati} \neq 0 \text{ mod } p\}$

Se $b \in \mathbb{Z}/p\mathbb{Z}$, $b \neq 0$, non è un quadrato,

$$f(b) \neq 0 \iff b^{\frac{p-1}{2}} - 1 \neq 0 \ (p)$$

$$\iff b^{\frac{p-1}{2}} \neq 1 \ (p)$$

Siccome $b^{\frac{p-1}{2}} \in \{1, -1\} \mod p$, si deve avere

$$b^{\frac{p-1}{2}} \equiv -1 \pmod p$$ □

Conseguenza $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \in \{-1, 0, 1\}$

Dim: Se uno fra a e b è $\equiv 0 \ (p)$ entrambi i lati dell'uguagl. sono 0. Altrimenti osserviamo che

$$\underbrace{\left(\frac{ab}{p}\right)} \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \underbrace{\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)} \pmod p$$

Siccome $p \geq 3$, la congruenza può essere verificata solo se c'è uguagl $\Rightarrow \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Conseg. 2 $x^2 + 1 \equiv 0 \ (p)$: per $p \equiv 3 \ (4)$ non ha soluz.

$$x^2 \equiv -1 \ (p)$$

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

$$\equiv \begin{cases} 1 & \text{se } \frac{p-1}{2} \text{ pari} \\ -1 & \text{se } \frac{p-1}{2} \text{ disp} \end{cases} \pmod p$$

$\frac{p-1}{2} = 2k \quad p = 4k+1$

$\frac{p-1}{2} = (2k+1) \quad p = 4k+3$

$$\Rightarrow \left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{se } p \equiv 1 \ (4) \\ -1 & \text{se } p \equiv 3 \ (4) \end{cases}$$

Conseg. 3 $(x^2 - 2)(x^2 - 3)(x^2 - 6) \equiv 0 \pmod p$: ha soluz.

per ogni p. Per $p = 2, 3$ OK.

Per gli altri p: vorrei che almeno una fra

$$x^2 \equiv 2 \ (p), \quad x^2 \equiv 3 \ (p), \quad x^2 \equiv 6 \ (p)$$

avesse soluz., cioè che almeno uno fra

$$\left(\frac{2}{p}\right), \left(\frac{3}{p}\right), \left(\frac{6}{p}\right) \quad \text{fosse } +1$$

Non possono essere tutti e 3 uguali a -1 perché

$$\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$$

Riassunto

- $\#\{\text{quadr. mod } p\} = \underbrace{1}_{\text{zero}} + \underbrace{\frac{p-1}{2}}_{\text{quadr. non nulli}}$

- $a \not\equiv 0$ è quadr. mod p $\iff$ $a^{\frac{p-1}{2}} \equiv 1 \ (p)$

Due commenti

1) $h : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ è un omom. di grp.

$x \longmapsto x^2$

$h(xy) = h(x)\,h(y)$ $\qquad (xy)^2 \equiv x^2 y^2 \pmod p$

2) $(\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow \{\pm 1\}$ è un omom. di grp.

$n \longmapsto \left(\frac{n}{p}\right)$

Residui k-esimi: $(k, p-1) = 1$

$$X^k \equiv n \pmod p, \qquad n \not\equiv 0 \ (p)$$

Sia $h : (\mathbb{Z}/p\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$

$$x \longmapsto x^k$$

Mostriamo che h è bigettiva $\iff$ $X^k \equiv n \ (p)$ ha una ed una soluz. mod p

Basta vedere che h è iniettiva

h è un omom. di grp: $h(xy) = h(x) \cdot h(y)$ ✓

$$(xy)^k \equiv x^k y^k \pmod p$$

Basta allora controllare che $\ker h = \{1\}$

$$\ker h = \{ x \in (\mathbb{Z}/p\mathbb{Z})^\times \mid h(x) = 1 \} = \{ 1 \}$$

$$x^k \equiv 1 \ (p) \iff \begin{cases} ord_p(x) \mid k \\ ord_p(x) \mid p-1 \end{cases}$$

$$\iff ord_p(x) \mid mcd(k, p-1) = 1$$

$$\iff x^1 \equiv 1 \ (p)$$

$\Rightarrow h$ iniettiva $\Rightarrow h$ bigettiva.

Secondo approccio $(p-1, k) = 1 \overset{\text{Bézout}}{\Longrightarrow}$ esistono $m, b \in \mathbb{Z}$

t.c. $m \cdot (p-1) + b \cdot k = 1$

$$X \equiv X^1 \equiv X^{m(p-1)+b\cdot k} \equiv \left(X^{p-1}\right)^m \cdot \left(X^k\right)^b \pmod p$$

$$\equiv 1^m \cdot \left(X^k\right)^b \pmod p$$

Se $X^k \equiv n \ (p) \Rightarrow X \equiv n^b \pmod p$

Viceversa, $\left(n^b\right)^k \equiv n^{bk} \cdot \underbrace{n^{m\cdot(p-1)}}_{1} \equiv n^{\overbrace{bk+m(p-1)}^{1}} \equiv n \ (p)$

Un caso con $(k, p-1) \neq 1$

$p = 7, \quad k = 3$

	1	2	3	4	5	6
0	1	2	3	4	5	6
0	1	1	-1	1	-1	-1

$\varphi: (\mathbb{Z}/7\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/7\mathbb{Z})^3$ ha nucleo di cardin. 3

$x \longmapsto x^3$

$h(1) = h(2) = h(4) = 1 \longleftarrow$

$h(3)$ $\qquad h(2 \cdot 3) = h(2) \cdot h(3) = h(3)$

$h(4 \cdot 3) = h(4) \cdot h(3) = h(3)$

$p = 13 \qquad x^3 \equiv 1 \quad (13) : \qquad x \equiv 1, 3, 9$

$(-4)^3 \equiv -64 \equiv 1 \quad (13)$

$2^3 \equiv 8 \quad (13) \qquad 6^3 \equiv 8 \quad (13) \qquad 18^3 \equiv 5^3 \equiv 8 \quad (13)$

$(2 \cdot 3)^3 \equiv 2^3 \cdot 3^3 \equiv 2^3$

$4^3 \equiv -1 \qquad 4 \cdot 3 \equiv 12 \equiv -1 \qquad 4 \cdot 9 \equiv 10$

$10^3 \equiv -1 \quad (13)$

Applicazione $x^3 + 13 \equiv 0 \quad (7 \cdot 8 \cdot 11)$

$$\Leftrightarrow \begin{cases} x^3 \equiv -13 & (7) \\ x^3 \equiv -13 & (8) \\ x^3 \equiv -13 & (11) \end{cases} \qquad \begin{cases} x^3 \equiv 1 & (7) \\ x^3 \equiv 3 & (8) \\ x^3 \equiv 9 & (11) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1, 2, 4 \ (7) \\ x \equiv 3 \ (8) \\ x \equiv 4 \ (11) \end{cases}$$

$$10 - 3 \cdot 3 = \underline{1}$$

$$x \equiv x^1 \equiv x^{10} \cdot (x^3)^{-3} \equiv (x^3)^{-3} \equiv \left((-2)^3\right)^{-1} \equiv 3^{-1}$$

$$\equiv 4 \quad (11).$$

Quanti sono i residui sesti mod 23?

$$\#\{ x^6 \mid x \in \mathbb{Z}/23\mathbb{Z} \} = \frac{p-1}{2} + 1$$

$$\left(\mathbb{Z}/23\mathbb{Z}\right)^{\times} \xrightarrow[\sim]{h_3} \left(\mathbb{Z}/23\mathbb{Z}\right)^{\times} \xrightarrow{h_2} \left(\mathbb{Z}/23\mathbb{Z}\right)^{\times}$$

$$x \longmapsto x^3$$

$$y \longmapsto y^2$$

Cifre

Trovare le ultime 2 cifre di $13^{39^5} = 13^{(39^5)}$

$$\left(13^{39}\right)^5 = 13^{39 \cdot 5}$$

Cioè: $13^{(39^5)} \mod 100$, ovvero mod 25 e mod 4

$$13 \equiv 1 \ (4) \quad \Rightarrow \quad 13^{39^5} \equiv 1 \ (4)$$

$$13^{39^5} \equiv 13^{(39^5 \bmod \varphi(25))} \pmod{25}$$

$39^5 = h \cdot \varphi(25) + r$, dove $r \equiv 39^5 \pmod{20}$

$$13^{39^5} \equiv \left(13^{\varphi(25)}\right)^h \cdot 13^r \equiv 13^r \pmod{25}$$

Per noi: $13^{39^5} \equiv 13^{19} \equiv 13^{-1} \equiv 2 \pmod{25}$.

TCR $\Rightarrow$ $13^{39^5} \equiv 77 \pmod{100}$

$n = \ldots + 10^2 a_2 + 10 a_1 + a_0 \equiv 10 a_1 + a_0 \pmod{100}$

$$13^{39^5} \equiv 13^{(39^5 \bmod 40)} \equiv 13^{-1} \pmod{100}$$

$1+p \mod p^n$

$p > 2$ primo. Calcolare $\operatorname{ord}_{(\mathbb{Z}/p^n\mathbb{Z})^\times}(1+p)$. $n \geq 2$

$n = 2$ $\quad (1+p)^k \equiv 1 \pmod{p^2}$

$$(1+p)^k = 1 + \binom{k}{1} p + \binom{k}{2} p^2 + \cdots + \binom{k}{k} p^k \equiv 1 + kp:$$

vale se (e solo se) $\quad 1 \equiv 1 + kp \pmod{p^2}$

$$0 \equiv kp \pmod{p^2}$$

$$0 \equiv k \pmod{p}$$

L'ordine mod p^2 è p.

$\boxed{n=3}$ $\quad (1+p)^k \equiv 1 \quad (p^3) \implies (1+p)^k \equiv 1 \quad (p^2)$

$$(1+p)^k \equiv 1 + \binom{k}{1} p + \binom{k}{2} p^2 + \dots$$

$$\Downarrow$$

$$k \equiv 0 \quad (p)$$

$k = ph$ $\qquad 1 \equiv 1 + (ph) \cdot p + \frac{(ph)(ph-1)}{2} p^2 \quad (p^3)$

$$0 \equiv h + \underbrace{\frac{(ph)(ph-1)}{2}}_{\equiv 0 \ (p) \text{ perché } p \neq 2} \pmod p$$

$\Rightarrow \quad k \equiv 0 \quad (p^2), \quad \mathrm{ord}_{(\mathbb{Z}/p^3\mathbb{Z})^\times}(1+p) = p^2$

In generale: $\mathrm{ord}_{(\mathbb{Z}/p^n\mathbb{Z})^\times}(1+p) = p^{n-1}$.

Dimostriamo che $(1+p)^{p^a} = 1 + p^{a+1} \cdot b$ con $(b,p)=1$

Caso base $(1+p) = 1 + p \cdot b$ $\quad b = 1$

$$(1+p)^{p^{a+1}} = \left((1+p)^{p^a}\right)^p = \left(1 + p^{a+1} \cdot b\right)^p$$

$$= 1 + p \cdot p^{a+1} \cdot b + \sum_{k \geq 2} \binom{p}{k} \left(p^{a+1} \cdot b\right)^k$$

$$= 1 + p^{a+2} \cdot \left(b + \sum_{k \geq 2} \underbrace{\binom{p}{k}}_{\equiv 0 \,(p)} b^k \cdot p^{\overbrace{k(a+1)-a-2}^{\geq 1^*}}\right)$$

* salvo $k=2$, $a=0$

$$\equiv b \not\equiv 0 \pmod{p}$$

$$(1+p)^k \equiv 1 \pmod{p^n} \qquad k = p^{n-1}$$

$$(1+p)^{p^{n-1}} \equiv 1 + p^{(n-1)+1} \cdot b \equiv 1 \pmod{p^n}$$

$$\Rightarrow \operatorname{ord}_{(\mathbb{Z}/p^n\mathbb{Z})^\times}(1+p) \mid p^{n-1}$$

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \cdot b \pmod{p^n}$$

$$\not\equiv 1 \pmod{p^n}$$

$$\Rightarrow \operatorname{ord}_{(\mathbb{Z}/p^n\mathbb{Z})^\times}(1+p) \nmid p^{n-2}$$

$$\Rightarrow \operatorname{ord} = p^{n-1}.$$

Titolo nota

$\varphi(m) = 12$

$12 = 2^2 \cdot 3, \qquad m = p_1^{e_1} \cdots p_k^{e_k} \qquad p_1 < p_2 < \dots < p_k$

$2^2 \cdot 3 = 12 = \varphi(m) = \varphi(p_1^{e_1}) \cdots \varphi(p_k^{e_k})$

$= (p_1 - 1) \cdot p_1^{e_1 - 1} \cdot \dots \cdot (p_k - 1) \cdot p_k^{e_k - 1}$

1) Non ci possono essere più di 2 primi dispari

2) $\max\{p_i\} \leq 13$

3) $p_k - 1 \mid 12 \Rightarrow p_k - 1 \in \{1, 2, 3, 4, 6, 12\}$

$p_k \in \{2, 3, 5, 7, 13\}$

4) $\max\{e_i\} \leq 3$; un esponente 3 può corrisp. solo a $p=2$

2 " " " " $p=2,3$

- Se $p_k = 13 \Rightarrow m = 13 \cdot h$ con $(h, 13) = 1$

$$12 = \varphi(m) = \varphi(13) \cdot \varphi(h) = 12 \cdot \varphi(h)$$

$$\Leftrightarrow \varphi(h) = 1 \Leftrightarrow h = 1, 2$$

$$m = 13, 26$$

- Se $p_k = 7 \Rightarrow m = 7 \cdot h$ con $(h, 7) = 1$

$$12 = \varphi(m) = \varphi(7)\,\varphi(h) = 6\,\varphi(h)$$

$$\varphi(h) = 2 \Leftrightarrow h = 3, 4, 6$$

- Se $p_k = 5$ $\quad n = 5h \quad \varphi(h) = 3$: no

Oss $\varphi(n)$ è pari $\forall n \geq 3$.

* se p dispari $| n \Rightarrow \underbrace{(p-1)}_{\text{pari}} | \varphi(n) \Rightarrow \varphi(n)$ pari

* se n non ha fattori disp., $n = 2^k$ e $\varphi(n) = 2^{k-1}$

è pari per $k \geq 2$

- Casi con $p_k \leq 3$: per voi.

$G = ((\mathbb{Z}/19\mathbb{Z})^\times, \cdot)$

G è ciclico, ovvero $G \simeq \mathbb{Z}/18\mathbb{Z}$.

$g = 2$ $\qquad |\langle g \rangle| = \text{ord}(g)$

Basta controllare se $2^6 \not\equiv 1 \ (19)$ e $2^9 \not\equiv 1 \ (19)$

$64 \not\equiv 1 \ (19)$ $\qquad 2^4 \cdot 2^4 \cdot 2 \equiv$

$(-3)\cdot(-3)\cdot 2 \equiv -1 \ (19)$

a lezione avevo erroneamente scritto "2". Il punto è che ogni divisore PROPRIO di 18 divide almeno uno fra 6 e 9

1) -2 è un gener?

2) Quanti e quali sono tutti i generatori?

1) $(-2)^9 \equiv (-1)^9 2^9 \equiv (-1)\cdot(-1) \equiv 1 \ (19)$:

$\text{ord}_{19}(-2) = 9$, e -2 non è un gen.

* 2 non è un $\square$ mod 19: $\left(\frac{2}{19}\right) = -1$

$* -1$ " " " " " "

$$\left(\frac{-1}{19}\right) = -1$$

$$\left(\frac{-2}{19}\right) = 1$$

2) Ogni classe di resto mod 19 si scrive come 2^k per un opportuno k

$$2^0, 2^1, 2^2, \ldots, 2^{17}$$

$\operatorname{ord}_{(\mathbb{Z}/19\mathbb{Z})^*}(2^k) = 18$: quando? Se e solo se $(18,k)=1$

$$\text{"}\min\{h>0 \mid (2^k)^h \equiv 1 \ (19)\}\text{"} = \frac{18}{(18,k)}$$

$2^{kh} \equiv 1 \quad (19) \quad \Leftrightarrow \quad 18 \mid k \cdot h$

$\Leftrightarrow \quad \frac{18}{(18,k)} \mid h$

$kh \equiv 0 \ (18)$

$\Updownarrow$

$h \equiv 0 \left(\frac{18}{(18,k)} \right)$

N° dei generatori: $\varphi(18) = 6$

Quali sono? $2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$

Gruppi: $f: \left(\mathbb{Z}/18\mathbb{Z}, + \right) \longrightarrow \left((\mathbb{Z}/19\mathbb{Z})^\times, \cdot \right)$

$1 \longmapsto 2$

$f(1+1) = f(1) \cdot f(1) \qquad f(2) = 2^2$

$f(1+1+1) = f(1) f(1) f(1) = 2^3$

$$\overline{k} \longmapsto 2^k$$

Se ho due rappr. k_1, k_2 della classe $\overline{k}$, allora

$k_2 = k_1 + 18h$ e

$$2^{k_2} \equiv 2^{k_1} \cdot 2^{18h} \equiv 2^{k_1} \cdot (2^{18})^h$$

$$\equiv 2^{k_1} \quad (19)$$

$$f(k_1 + k_2) = 2^{k_1 + k_2} = 2^{k_1} 2^{k_2} = f(k_1)\, f(k_2)$$

Sia $g: (\mathbb{Z}/19\mathbb{Z})^\times \longrightarrow \mathbb{Z}/18\mathbb{Z}$ la funzione inversa.

$x \in (\mathbb{Z}/19\mathbb{Z})^\times$ è un generatore $\Leftrightarrow$ $g(x)$ è un gen. di $(\mathbb{Z}/19\mathbb{Z})^\times$ $\Leftrightarrow$ gen. di $\mathbb{Z}/18\mathbb{Z}$

$\Downarrow$

$(g(x), 18) = 1$

Al contrario: i generatori di $(\mathbb{Z}/19\mathbb{Z})^\times$ sono $f(y) = 2^y$ dove y è un gen. di $\mathbb{Z}/18\mathbb{Z}$, cioè i generatori sono le potenze di 2 in cui l'espon. è primo con 18.

Oss $\#\{ (\mathbb{Z}/19\mathbb{Z})^\times \longleftarrow \mathbb{Z}/18\mathbb{Z} : f \text{ isom.} \} = \#\text{gen. di } (\mathbb{Z}/19\mathbb{Z})^\times$

$f : \mathbb{Z}/18\mathbb{Z} \longrightarrow (\mathbb{Z}/19\mathbb{Z})^\times$ isom

$1 \longmapsto f(1)$ di ordine 18: ho 6 scelte

Una volta fissato $f(1)$, f è complet. determinata

$$k \longmapsto f(1)^k$$

* f omom: $f(k_1 + k_2) \overset{?}{=} f(k_1)\, f(k_2)$

$$f(1)^{k_1+k_2} = f(1)^{k_1} \cdot f(1)^{k_2}$$

* f bigettivo: basta vedere che è iniettivo, e

$$\ker f = \{ n \in \mathbb{Z}/18\mathbb{Z} : f(1)^n \equiv 1 \quad (19) \}$$

$$= \{ n \in \mathbb{Z}/18\mathbb{Z} : n \equiv 0 \quad (18) \} = \{0\}$$

TCR con i gruppi Se $(m,n)=1$, la funzione

$$\varphi : \mathbb{Z}/_{mn\mathbb{Z}} \longrightarrow \mathbb{Z}/_{m\mathbb{Z}} \times \mathbb{Z}/_{n\mathbb{Z}}$$

$$[a]_{mn} \longmapsto \left([a]_m , [a]_n\right)$$

è un isom. di gruppi

Risolvere $\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$ $\longleftrightarrow$ calcolare $\varphi^{-1}\left([a],[b]\right)$

In particolare, risolvere $\begin{cases} x \equiv 1 \pmod m \\ x \equiv 0 \pmod n \end{cases}$ $\longleftrightarrow$ $\varphi^{-1}\left((1,0)\right)$

e $\begin{cases} x \equiv 0 \pmod m \\ x \equiv 1 \pmod n \end{cases}$ $\longleftrightarrow$ $\varphi^{-1}\left((0,1)\right)$

$$\varphi^{-1}\big((a,b)\big) = \varphi^{-1}\big((a,0)+(0,b)\big)$$

φ^{-1} è un omom. $\Longrightarrow$

$$= \varphi^{-1}\big((a,0)\big) + \varphi^{-1}\big((0,b)\big)$$

$$= \varphi^{-1}\Big(\underbrace{(1,0)+(1,0)+\dots+(1,0)}_{a \text{ volte}}\Big) + \varphi^{-1}\Big(\underbrace{(0,1)+\dots+(0,1)}_{b \text{ volte}}\Big)$$

$$= a\cdot\varphi^{-1}\big((1,0)\big) + b\,\varphi^{-1}\big((0,1)\big)$$

$x \longmapsto x^2$

G un gruppo, $f: G \longrightarrow G$, $x \longmapsto x^2$

Dimostrare che f è un omom. di grp $\Leftrightarrow$ G abeliano

Dim f omo $\iff$ $\forall a, b \in G$ si ha $f(a \cdot b) = f(a) \cdot f(b)$

$\iff$ $(a \cdot b)^2 = a^2 \cdot b^2$ $\quad \forall a, b$

$ba = ab$ $\iff$ $abab = a^2 b^2$ $\quad$ "

$\iff$ $a^{-1} \cdot (abab) \cdot b^{-1} = a^{-1} \cdot a^2 \cdot b^2 \cdot b^{-1}$

$\iff$ $\underbrace{(a^{-1} \cdot a)}_{e_G} \cdot ba \cdot \underbrace{(b \cdot b^{-1})}_{e_G} = \underbrace{(a^{-1} \cdot a)}_{e_G} \cdot ab \underbrace{(bb^{-1})}_{e_G}$

$\iff$ $ba = ab$ $\quad \forall a, b$ $\quad \square$

Cor Se G è un gup. t.c. $g^2 = e_G$ $\quad \forall g \in G$

$\left(\text{es.} \quad G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq (\mathbb{Z}/8\mathbb{Z})^\times \right)$,

allora G è abeliano

Dim $f: G \longrightarrow G$ è sempre un omomorf., e per ipotesi coincide con $g \longmapsto g^2$ $\square$

$$g \longmapsto e_G$$

$$\varphi(n) \geq \frac{n}{1+\omega(n)}$$

Sia $\omega(n) = n^\circ$ dei fattori primi distinti di n.

$$\omega(2^4 \cdot 3^2 \cdot 5^7) = 3$$

Tesi: $\varphi(n) \geq \dfrac{n}{1+\omega(n)}$

Per induzione su $\omega(n)$.

- Se $\omega(n) = 0$, $n = 1$ e $\varphi(1) \geq \frac{1}{1+0}$ ✓

- Supponiamo nota la tesi per $\omega(n) \leq k$ e dimostriamo per $\omega(n) = k+1$.

Sia $n = p_1^{e_1} p_2^{e_2} \dots p_{k+1}^{e_{k+1}}$ $\quad p_1 < \dots < p_{k+1}$

$$\varphi(n) = \varphi\left(p_1^{e_1} \dots p_{k+1}^{e_{k+1}}\right) = \varphi\left(p_1^{e_1} \dots p_k^{e_k}\right) \varphi\left(p_{k+1}^{e_{k+1}}\right)$$

$$\overset{\text{ip. ind.}}{\geq} \frac{p_1^{e_1} \dots p_k^{e_k}}{1+k} \cdot p_{k+1}^{e_{k+1}-1} \cdot (p_{k+1} - 1) \overset{?}{\geq} \frac{p_1^{e_1} \dots p_{k+1}^{e_{k+1}}}{\underbrace{k+2}_{1+\omega(n)}}$$

$$\iff \frac{p_{k+1} - 1}{1+k} \geq \frac{p_{k+1}}{2+k}$$

$$\Leftrightarrow \quad \cancel{1} - \frac{1}{p_{k+1}} \geq \frac{k+1}{k+2} = \cancel{1} - \frac{1}{k+2}$$

$$\Leftrightarrow \quad \frac{1}{p_{k+1}} \leq \frac{1}{k+2} \qquad \Leftrightarrow \quad k+2 \leq p_{k+1}$$

Se $q_1 = 2 < q_2 = 3 < q_3 = 5 < \dots$ la seq di tutti i n$^{\text{ri}}$ primi. Allora $p_{k+1} \geq q_{k+1} \geq 2(k+1) - 1$

$$= 2k+1 \overset{?}{\geq} k+2$$

$$\Leftrightarrow \quad k \geq 1$$

Dobbiamo solo verificare che $p_{0+1} \geq 0+2$

$$2 \geq 2$$

39. f una permutaz. di $\{1, \dots, n\}$.

$$x \mid y \iff f(x) \mid f(y)$$

(i) È vero che f manda il prodotto di k primi distinti nel prodotto di k primi distinti?

① y e $f(y)$ hanno lo stesso n° di divisori.

② $f(1) = 1$, $f(p)$ è primo $\forall p$

③ $n = p_1 \cdots p_k$ $\quad p_i \mid n \Rightarrow f(p_i) \mid f(n)$

$\Rightarrow f(n)$ ha almeno k divisori primi distinti

④ $f(n) = q_1^{e_1} \cdots q_k^{e_k} \cdot q_{k+1}^{e_{k+1}} \cdots q_t^{e_t}$

$q_i = f(p_i)$ per $i \le k$

$$d(n) = 2^k \quad \Longrightarrow \quad d(f(n)) = (e_1+1)\cdots(e_k+1)(e_{k+1}+1)\cdots(e_t+1)$$

$$\geq 2^k \cdot (e_{k+1}+1)\cdots(e_t+1)$$

$$\Rightarrow e_{k+1} = \ldots = e_t = 0$$

e $e_i = 1$ per $i = 1, \ldots, k$. **VERO**

ii) E' vero che f manda pot. di primi in pot. primi?

$$d(f(p^2)) = d(p^2) = 3 \quad \Rightarrow \quad f(p^2) = q^2$$

$$n = p_1^{e_1} \cdots p_k^{e_k} \qquad d(n) = \underbrace{(e_1+1)}_{2+1} \cdot \ldots \cdot (e_k+1) = 3$$

$d(f(p^3)) = d(p^3) = 4$: proviamo $f(p^3) = q_1 \cdot q_2$

$p^2 \mid p^3 \iff f(p^2) \mid f(p^3) = q_1 q_2$

$\|$

q^2

Se $f(p^3)$ ha almeno 2 div. primi, q_1, q_2

$q_1 \mid f(p^3)$

$f|_{\{\text{primi} \le n\}}$: è una permutaz di $\{\text{primi} \le n\}$

$q_1 = f(x_1)$ con x_1 primo

$f(x_1) \mid f(p^3)$

$\Updownarrow$

$x_1 \mid p^3$

$\Updownarrow$

$x_1 = p$

Abbiamo dim: l'unico divisore primo di $f(p^n)$ è $f(p)$

$\Rightarrow \quad f(p^n) = f(p)^k \qquad$ (e $\quad k+1 = d(f(p^n)) =$

$= d(p^n) = n+1$)

$$f(p^n) = f(p)^n$$

$\{1, 2, 3\} \longrightarrow \{1, 2, 3\}$

$1 \longmapsto 1$

$2 \longmapsto 3$

$3 \longmapsto 2$

iii) $n=10$. $f(2^n) = f(2)^n$ $f(2^3) = f(2)^3 \leq 10$

$\Rightarrow f(2) = 2$

$f(3^2) = f(3)^2 \leq 10 \Rightarrow f(3) \leq 3 \Rightarrow f(3) = 3$

$5 \mid 5, 10$ $f(5) \mid f(5), f(10)$

$\{\overset{\cap}{5}, 7\}$

Se $f(5) = 7$ dovrei avere 2 mult. di 7 in $\{1, \dots, 10\}$

$\Rightarrow f(5) = 5 \Rightarrow \dots \Rightarrow f = id$

GRUPPI

Titolo nota

Gruppi di ordine ≤ 6

$|G| = 1 \qquad G = \{e\} \qquad e \cdot e = e$

$|G| = 2, 3, 5 \Rightarrow G$ ciclico, $G \simeq \mathbb{Z}/p\mathbb{Z}$

$|G| = 4 \qquad G = \{e, a, b, c\}$

	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

$$a \cdot b = \begin{cases} e \\ \cancel{a} \\ \cancel{b} \\ c \end{cases}$$

$a \cdot b = a \longrightarrow b = e$

Oss · L'ordine di ogni elemento deve dividere 4

· Se c'è un elemento g di ordine 4, allora $\langle g \rangle = G$.

$\Rightarrow$ G ciclico $\Rightarrow$ $G \simeq \mathbb{Z}/4\mathbb{Z}$

Se $\text{ord}(a) = 4$

$f_a : G \longrightarrow G$

$x \longmapsto a \cdot x$

$f_{a^{-1}} : G \longrightarrow G$

$x \longmapsto a^{-1} x$

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

No: $a^2 = e \Rightarrow \text{ord}(a) = 2$

$a \cdot b = a^3 \neq e$

$c = a \cdot b = a \cdot a^2 = a^3$

$a \cdot c = a^4 = e$

$b \cdot c \overset{?}{=} a$

$a^2 \cdot a^3 = a^4 \cdot a = e \cdot a = a$

• Viceversa: se NESSUN elemento di G ha ordine 4,

$\Rightarrow \quad a^2 = b^2 = c^2 = e \xRightarrow[\text{altra volta}]{\text{es.}} G$ abeliano

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

$= \{ \underset{e}{(0,0)}, \underset{a}{(0,1)}, \underset{b}{(1,0)}, \underset{c}{(1,1)} \}$

$a + b = c, \quad a + c = (1,0) = b$

$b + c = a$

• $|G| = 6$

$\mathbb{Z}/6\mathbb{Z} \longleftrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad S_3$

$(1,1)$ (written above $\times$ with $\cap$)

$(g_1, g_2) \in G_1 \times G_2 \qquad \text{ord}(g_1, g_2) = \text{mcm}\left(o_{G_1}(g_1), o_{G_2}(g_2)\right)$

Sia $g \in G$ di ordine massimo

- $\text{ord}(g) = 6 \Rightarrow \langle g \rangle = G \simeq \mathbb{Z}/6\mathbb{Z}$
- $\text{ord}(g) = 3 \qquad G \supseteq \{e, g, g^2\}$

  Sia $h \in G \setminus \{e, g, g^2\}$

  $e \quad g \quad g^2 \quad h \quad hg \quad hg^2$

$h \cdot g^i \neq g^j$: se $h \cdot g^i = g^j \Rightarrow h \cdot g^i \cdot (g^{-1})^i = g^j \cdot g^{-i}$

$\Rightarrow h = g^{j-i}$, ma

$h \notin \{1, g, g^2\}$

$h \cdot g^i \neq h \cdot g^j$ $\qquad$ $h^{-1} h \cdot g^i = h^{-1} h \cdot g^j \iff g^i = g^j$

Es $(hg) \cdot (g^2) = h \cdot g^3 = h$

$g \cdot h \neq g, h, g^2, e = g^3$ $\qquad$ $gh = g^3$

$h = g^2$

Quindi $g \cdot h = \begin{cases} h \cdot g \\ h \cdot g^2 \end{cases}$

Oss $\operatorname{ord}(h) = 2$. Certamente si ha $h^2 \in \{1, g, g^2\}$.

Se $h^2 = g$, qual è l'ordine di h?

$h^6 = (h^2)^3 = g^3 = e$ $\qquad$ $h^2 = g \neq e$

$h^3 = h \cdot h^2 = h \cdot g \neq e$

Avrei allora che h ha ord. 6, ma non ci sono elem. di ord. 6. Similmente $h^2 \neq g^2$, e quindi $h^2 = e$.

CASO 1: $gh = hg$

Considero $g \cdot h$. Allora:

$$(g \cdot h)^2 = g \cdot (h \cdot g) \cdot h$$
$$= g \cdot (g \cdot h) \cdot h$$
$$= g^2 \cdot h^2 = g^2$$

$$(g \cdot h)^3 = g(hg)h\,gh = g(gh)h\,gh$$
$$= g \cdot g \cdot (h \cdot h) \cdot (g \cdot h)$$

$$= g \cdot g \cdot e \cdot g \cdot h = g^3 h = h$$

$\text{ord}_G(g \cdot h) \mid \#G = 6$, e l'ordine è $\neq 2, 3$

$\Rightarrow$ $g \cdot h$ ha ordine 6 $\Rightarrow$ assurdo

CASO 2 $\quad g \cdot h = h \cdot g^2$

$$hg \cdot h = h(gh)$$
$$= h(hg^2) = h^2 g^2 = g^2$$
$$(hg)^2 = \underbrace{hghg}_{hg^2} = h^2 g^3 = e$$

	e	g	g^2	h	hg	hg^2
e	e	g	g^2	h	hg	hg^2
g	g	g^2	e			
g^2	g^2	e	g			
h	h	hg	hg^2	e	g	g^2
hg	hg	hg^2	h	g^2	e	
hg^2	hg^2	h	hg			

Troviamo un isom fra questo G ed S_3

$$f: G \xrightarrow{\sim} S_3$$

$$g \longmapsto (1,2,3)$$

$$h \longmapsto (1,2)$$

$$g^2 \longmapsto (1,2,3)\circ(1,2,3) = (1,3,2)$$

$$hg \longmapsto (1,2)\circ(1,2,3) = (2,3)$$

$$hg^2 \longmapsto (1,3)$$

$$e \longmapsto id$$

$f(hg) = f(h)\circ f(g)$

- $|G| = 6$, l'ordine max. e' $2 \Longrightarrow \forall g \in G,\ g^2 = e$

  $\Rightarrow G$ abeliano. Siano a, b due elem. distinti in

$G \setminus \{e\}$ e consideriamo $H = \{e, a, b, ab\}$

$$a \cdot (ab) = a^2 b = b \qquad a^2 = b^2 = (ab)^2 = e$$

$$b \cdot (ab) = (ab) \cdot b = ab^2 = a$$

$\Rightarrow$ H è un sottogruppo! $\qquad H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

Ma per Lagrange si dovrebbe avere che $\#H \mid \#G$, cioè $4 \mid 6$, assurdo.

Classi laterali dx e sx

Dato G gruppo e H sottogruppo avete definito

$$\varphi : \{gH : g \in G\} \xrightarrow{?} \{Hg : g \in G\}$$

$$gH \overset{?}{\longmapsto} H(g)$$

⚠ Non è ben definita!

$$g_1 H = g_2 H \iff g_2^{-1} g_1 H = H \iff g_2^{-1} \cdot g_1 \in H$$

$$gH = H \iff g \in H$$

$$(g_2^{-1} g_1)^{-1} = g_1^{-1} \cdot g_2$$

male!

$$g_1 H = g_2 H \longrightarrow Hg_1 \overset{?}{=} Hg_2 \iff g_2 \cdot g_1^{-1} \in H$$

$$\Rightarrow H = H \cdot g_2 g_1^{-1}$$

$$\varphi : \{gH\} \longrightarrow \{Hg\}$$

$$gH \longmapsto Hg^{-1}$$

$g_1 H = g_2 H \rightsquigarrow H g_1^{-1} \overset{?}{=} H g_2^{-1}$ ✓

$\Downarrow \qquad\qquad \Uparrow$

$g_2^{-1} \cdot g_1 \in H \Rightarrow H \cdot g_2^{-1} \cdot g_1 = H$

ok, abbiamo la buona def!

L'inversa di φ è $\{Hg\} \longrightarrow \{gH\}$

$Hg \longmapsto g^{-1}H$

Es $G = S_3$, $H = \langle (1,2) \rangle$. Quante sono le classi lat?

Classi lat sx: $H = \{e, (1,2)\}$

$(1,3)H = \{(1,3), (1,2,3)\} = (1,2,3) \cdot H$

$(2,3)H = \{(2,3), (1,3,2)\} = (1,3,2)H$

Class. lat dx: H °

$$H(1,3) = \{(1,3),\ (1,3,2)\}$$

$$H(1,2,3) = H(2,3) = \{(2,3),\ (1,2,3)\}$$

$(1,3)H \longmapsto H\cdot(1,3)$

$\|$

$(1,2,3)H \longmapsto H\cdot(1,2,3)$

non funziona

$(1,3)H \longmapsto H(1,3)$

$\|$

$(1,2,3)H \longmapsto H(1,2,3)^{-1}$

$\|$

$H(1,3,2)$

$H\cdot(2,3) = \{(2,3),$ $(1,2)(2,3) = (3,1,2)$

Sgp. di indice 2 sono normali

$H < G$ di indice 2: $G = H \sqcup gH$ (unione disgiunta $\sqcup$)

$= H \sqcup H \cdot g'$

La classe laterale gH è $G \setminus H$

" " " Hg " $G \setminus H$

Il sgp H è normale: le sue classi lat dx e sx coincidono.

Ordini

$G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (a, b, c) $\quad |G| = 96$

$\{ \text{ord}(g) : g \in G \} = \{1, 2, 4, 8; 3, 6, 12, 24\}$

$$\text{ord}_G((a,b,c)) = \text{mcm}\left(\text{ord}(a), \text{ord}(b), \text{ord}(c)\right)$$

$$\text{ord}(a) \in \{1,2,4,8\} \qquad \text{ord}(b) \in \{1,2,4\} \qquad \text{ord}(c) \in \{1,3\}$$

Quanti elementi hanno ord 12?

$\text{ord}(a,b,c) = 12 \implies \text{ord}(c) = 3$, due scelte per c

Si tratta di contare le coppie (a,b) di ordine 4.

Contiamo $\#\{(a,b) : \underbrace{4\cdot(a,b) = (0,0)}\}$

$(a,b)+(a,b)+(a,b)+(a,b)$

$$- \#\{(a,b) : 2(a,b) = (0,0)\}$$

$$= \#\{a \in \mathbb{Z}/8\mathbb{Z} : 4a \equiv 0 \ (8)\} \times \#\{b \in \mathbb{Z}/4\mathbb{Z} : 4b \equiv 0 \ (4)\}$$

$$- \#\{a \in \mathbb{Z}/8\mathbb{Z} : 2a \equiv 0 \ (8)\} \times \#\{b \in \mathbb{Z}/4\mathbb{Z} : 2b \equiv 0 \ (4)\}$$

$$= 4 \times 4 - 2 \times 2 = 12$$

$$\#\text{ el. di ord. } 12 = \varphi(12) \cdot \varphi(2) = 24$$

$$\#\{x \in \mathbb{Z}/300\mathbb{Z} : 15x \equiv 0 \ (300)\} = 15$$

$$x \equiv 0 \ \left(\tfrac{300}{15}\right)$$

$$\frac{300}{300/15} = 15$$

Fatto $\#\{g \in \mathbb{Z}/n\mathbb{Z} : \mathrm{ord}(g) \mid d\} = d \quad (d \mid n)$

$$\#\{g \in \mathbb{Z}/n\mathbb{Z} : \mathrm{ord}(g) \mid d\} = \#\{x \in \mathbb{Z}/n\mathbb{Z} : dx \equiv 0 \ (n)\}$$

$$= \sum_{e \mid d} \#\{g \in \mathbb{Z}/n\mathbb{Z} : \mathrm{ord}(g) = e\} =$$

$$= \sum_{e \mid d} \varphi(e) = d$$

Caso $p=2$ del teo di Cauchy

G finito, $|G|$ pari. Allora esiste $g \in G$ di ordine 2

$g^2 = id \qquad g = g^{-1} \qquad (e \quad g \neq id)$

Partizioniamo G tramite la relaz. di equiv.

$$g \sim h \iff g = h \circ g = h^{-1}$$

$$\begin{array}{ccc} g & \sim & h & \sim & k \\ & = & & = & \\ & \text{inv} & & \text{inv} & \end{array}$$

$G =$ $\bigcup$ classi di equiv.

$= \{e\} \cup \underbrace{\{g_1, g_1^{-1}\}}_{\text{distinti}} \cup \dots \cup \underbrace{\{g_k, g_k^{-1}\}}_{\text{distinti}} \cup \{h_1\} \cup \dots \cup \{h_s\}$

$$|G| = 1 + 2 \cdot K + s$$

$$\Rightarrow \underset{\text{ipotesi}}{0 \equiv |G| \equiv 1 + s} \quad (2)$$

$\Rightarrow s$ dispari

$\Rightarrow s \neq 0$

$\Rightarrow$ esistono elementi di ordine 2

□

GRUPPI II

Note Title

Sottogruppi dei grup. finiti

G FINITO, $H \subseteq G$ "chiuso per l'operazione",

ovvero t.c. $\forall\, h_1, h_2 \in H \qquad h_1 \overset{\cdot}{G} h_2 \in H.$

Allora H è un sottogrup. di G

Dim. Basta vedere che $\forall\, h \in H, \quad h^{-1} \in H.$

$H \ni h, \quad h \cdot h, \quad h \cdot h \cdot h, \ \ldots$

$$\langle h \rangle \subseteq G \Rightarrow |\langle h \rangle| < +\infty \Rightarrow \operatorname{ord}(h) = n < \infty.$$

$$e, h, h^2, h^3, \ldots, h^{\operatorname{ord}(h)-1}$$

$$h^n = e \Rightarrow h \cdot h^{n-1} = e \Rightarrow h^{n-1} = h^{-1}$$

Allora $H \ni h^{n-1} = h^{-1}$ □

Oss Per $G = \mathbb{Z}$ e $H = N$ abbiamo un controes.

per G infinito.

Omomorfismi

$G_1 = \mathbb{Z}/m\mathbb{Z}$, $G_2 = \mathbb{Z}/n\mathbb{Z}$

$\mathrm{Hom}(G_1, G_2) = \{ f : G_1 \longrightarrow G_2 \text{ omomorfismo} \}$

Oss $\varphi : G_1 \longrightarrow H$ omomorfismo.

$\varphi(\bar{1}) = h$ $\varphi(\bar{2}) = \varphi(\bar{1}+\bar{1}) = \varphi(\bar{1}) \cdot \varphi(\bar{1}) = h^2$

$\varphi(\bar{3}) = h^3, \ldots, \varphi(\bar{k}) = h^k$

↳ $k > 0$

φ è determinato da $\varphi(\overline{1})$

$$\varphi(\overline{-1}) = \varphi(\overline{1})^{-1} = h^{-1}$$

$$\varphi(\overline{-2}) = \varphi\left((\overline{-1}) + \overline{(-1)}\right) = \varphi(-1)\cdot\varphi(-1) = h^{-2}$$

Caso $m=3$, $n=2$ $\qquad \varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$

$$\varphi(\overline{1}) = \overline{0} \rightsquigarrow \varphi : \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

$$x \longmapsto 0$$

Oss G, H gruppi. La funzione $\varphi : G \longrightarrow H$ è un
$g \longmapsto e_H$

omomorfismo: $\varphi(a\cdot b) = \varphi(a)\,\varphi(b)$

$e = e\cdot e$

Se invece cerco di costruire $\varphi : \mathbb{Z}/_{3}\mathbb{Z} \longrightarrow \mathbb{Z}/_{2}\mathbb{Z}$ ho

$\bar{1} \longmapsto \bar{1}$

un problema: $\underset{2}{\underset{\shortparallel}{\text{ord}}}(\varphi(1)) \mid \text{ord}\, \underset{3}{\underset{\shortparallel}{1}}$

A mano: $\varphi(1) = 1 \implies \varphi(1+1+1) = \varphi(1)+\varphi(1)+\varphi(1)$

$$\varphi(1+1+1) = 0 = \varphi(0) \qquad \varphi(1)+\varphi(1)+\varphi(1) = 1+1+1 = 1$$

$\varphi : \mathbb{Z}/_{m}\mathbb{Z} \longrightarrow \mathbb{Z}/_{n}\mathbb{Z}$

$1 \longmapsto h$

$\text{ord}(h) \mid \text{ord}(1) = m$

Lagrange: $\text{ord}(h) \mid \# \mathbb{Z}/_{n}\mathbb{Z} = n$

$\implies \text{ord}(h) \mid \text{MCD}(m, n)$

Siccome $\mathbb{Z}/n\mathbb{Z}$ contiene (m,n) elementi il cui ordine divide (m,n), abbiamo <u>al massimo</u> (m,n) omom.

Viceversa: sia $\bar{h} \in \mathbb{Z}/n\mathbb{Z}$ con $\text{ord} \mid (m,n) =: d$.

Allora affermo che $f: \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ è ben definita

$$\overline{k} \longmapsto \overline{k \cdot h}$$

ed un omomorfismo.

Oss La condiz $\text{ord}(h) \mid d$ vuol dire $d \cdot h \equiv 0 \ (n)$

$\Leftrightarrow h \equiv 0 \ \left(\frac{n}{d}\right)$

<u>Buona definizione</u>: se k_1, k_2 sono due rappr. della stessa classe $\bar{k}$ in $\mathbb{Z}/m\mathbb{Z}$, voglio verificare che

$$k_1 \cdot h \overset{?}{\equiv} k_2 \cdot h \pmod{n}$$

$$\iff (k_1 - k_2) \cdot h \equiv 0 \pmod{n}$$

$(k_1 - k_2)$: divisibile per m; h: divisibile per $\frac{n}{(n,m)}$

$(k_1 - k_2) \cdot h$: divisibile per $\frac{mn}{(m,n)} = \frac{m}{(m,n)} \cdot n$

Omomorfismo: $f(\overline{k_1} + \overline{k_2}) = f(\overline{k_1}) + f(\overline{k_2})$ in $\mathbb{Z}/n\mathbb{Z}$

$$\iff \overline{h \cdot (k_1 + k_2)} \overset{?}{=} \overline{k_1 \cdot h} + \overline{k_2 h} \quad \text{in } \mathbb{Z}/n\mathbb{Z}$$

Vero per proprietà delle congruenze.

Conclusione: $|\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})| = (m, n)$

* $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) = \{ f \text{ che manda tutto in } 0 \}$

(f è det. da $f(\bar{1})$, che deve avere ordine finito)

* $\mathrm{Hom}(\mathbb{Z}, H)$ con H gruppo qualsiasi

Per ogni $h \in H$ fissato,

$$f_h : \mathbb{Z} \longrightarrow H$$
$$n \longmapsto h^n$$

è un omom:

$$h^{m+n} = f_h(m+n) \overset{?}{=} f_h(m) \cdot f_h(n) = h^m \cdot h^n$$

ok!

Automorfismi

G gruppo. $\quad \mathrm{Aut}(G) = \{ f : G \to G \mid f \text{ isom. di gruppi} \}$

Fatto: $(\mathrm{Aut}\, G, \text{composizione})$ è un gruppo

* $e = id_G$
* composiz. associativa
* $f : G \to G$ isom. $\Rightarrow$ esiste una FUNZIONE $f^{-1} : G \to G$

f^{-1} è un omom. di gup? Cioè: è vero che $f^{-1}(a \cdot b) \stackrel{?}{=} f^{-1}(a) \cdot f^{-1}(b)$?

$$\Leftrightarrow \quad f\left(f^{-1}(a\cdot b)\right) \overset{?}{=} f\left(f^{-1}(a)\cdot f^{-1}(b)\right)$$

$$\Leftrightarrow \quad a\cdot b = f\left(f^{-1}(a)\right)\cdot f\left(f^{-1}(b)\right)$$

$$\Leftrightarrow \quad a\cdot b = a\cdot b$$

Chi sono $\mathrm{Aut}(\mathbb{Z})$ e $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$?

$$\mathrm{Aut}(\mathbb{Z}) = \left\{ \varphi_n : \begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \\ 1 & \longmapsto & n \end{array} \quad \text{invertibili} \right\}$$

immagine $\varphi_n = \varphi_n(\mathbb{Z}) = \{\varphi_n(h) \mid h \in \mathbb{Z}\}$

$$= \{h\cdot n \mid h\in\mathbb{Z}\} = n\mathbb{Z}$$

Se $n\mathbb{Z} = \mathbb{Z} \Rightarrow 1$ è multiplo di n

$\Rightarrow n = \pm 1$

$\Rightarrow \mathrm{Aut}(\mathbb{Z}) = \{\pm id\} \cong \mathbb{Z}/2\mathbb{Z}$

$$\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) = \left\{ \varphi_a : \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \longmapsto & \overline{ax} \end{array} \;\middle|\; \varphi_a \text{ invertib} \right\}$$

$$= \left\{ \varphi_a \dots \;\middle|\; \varphi_a \text{ iniettiva} \right\} = \left\{ \varphi_a \;\middle|\; \ker \varphi_a = \{0\} \right\}$$

Cioè: dobbiamo cercare le soluzioni di $a \cdot x \equiv 0 \ (n)$

$\Leftrightarrow x \equiv 0 \ \left(\frac{n}{(n,a)}\right)$: ci sono (n,a) soluz.

φ_a iniettivo $\Leftrightarrow$ $(n, a) = 1$

Oss $(a, n) = 1 \Rightarrow \exists b$ t.c. $ab \equiv 1 \ (n)$ e

$\varphi_a^{-1} = \varphi_b$: $\varphi_b \circ \varphi_a (x) = \varphi_b (ax) =$

$= b \cdot a \cdot x \equiv x \ (n)$

$Aut(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^*$: Ψ

$\varphi_a \longmapsto a$

Ψ è un isom. di grp: Ψ è bigettiva per quanto sopra.

Verifichiamo che è un omom:

$$\psi(a \cdot b) \overset{?}{=} \psi(a) \circ \psi(b)$$

$\Leftrightarrow \quad \forall x \in \mathbb{Z}/n\mathbb{Z}$ vale $\quad \psi(ab)(x) = (\psi(a) \circ \psi(b))(x)$

$$\varphi_{ab}(x) = (\varphi_a \circ \varphi_b)(x)$$

$$\overline{ab \cdot x} = \overline{a \cdot (bx)}$$

ok!

Prop $\left(\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}), \circ\right) \simeq \left((\mathbb{Z}/n\mathbb{Z})^*, \cdot\right)$

Sottogruppi ciclici di G

$s_d(G)$ = n° sottogp. di G ciclici di ordine d

= " " " " " isom. a $\mathbb{Z}/d\mathbb{Z}$

$e_d(G)$ = n° elementi di G di ordine d

$$s_d(G) = \frac{e_d(G)}{\varphi(d)}$$

F_d: $\{$ elementi di ord $= d\}$ $\longrightarrow$ $\{$ sottogp. ciclici $\simeq \mathbb{Z}/d\mathbb{Z}\}$

g $\longmapsto$ $\langle g \rangle$

1) F_d è suriettiva: un sgp. $H \overset{\psi}{\simeq} \mathbb{Z}/d\mathbb{Z}$ è della

forma $F_d(h)$ dove $h = \varphi^{-1}(1)$ è un gen. di H

2) Fissato H, quanti sono i g t.c. $F_d(g) = H$?

Ovvero: quanti sono i generatori di H? Tanti quanti quelli di $\mathbb{Z}/d\mathbb{Z}$, ovvero $\varphi(d)$

$$\Rightarrow \#\{\text{sottogp} \simeq \mathbb{Z}/d\mathbb{Z}\} = \#\{\text{elem. di ord } d\} / \varphi(d).$$

Es Quanti sono i sottogp $\simeq \mathbb{Z}/8\mathbb{Z}$ di $\mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/32\mathbb{Z}$?

Basta contare gli elem. di ordine 8.

Un elem. (a,b) ha ordine 8 se

$$8(a,b) = (0,0)$$

ma $\quad 4(a,b) \neq (0,0)$

$$\#\{\text{el. ord. } 8\} = \#\left\{\text{soluz. di } \begin{cases} 8a \equiv 0 \ (16) \\ 8b \equiv 0 \ (32) \end{cases}\right\}$$

$$- \#\left\{\text{soluz. di } \begin{cases} 4a \equiv 0 \ (16) \\ 4b \equiv 0 \ (32) \end{cases}\right\}$$

$$= 8 \cdot 8 - 4 \cdot 4 = 48$$

$$\#\{\text{sgp} \simeq \mathbb{Z}/8\mathbb{Z}\} = \frac{1}{\varphi(8)} \cdot (\text{n° elem. ord } 8) = 12.$$

Ordini di elementi in gruppi ABELIANI

G grup. abeliano finito, $\mathcal{O} = \{ \text{ord}(g) \mid g \in G \}$

1) Se $n \in \mathcal{O}$ e $d \mid n$, $d > 0$, allora $d \in \mathcal{O}$

Ho $g \in G$ di ordine n. Preso $h = g^{n/d}$ si ha

$$h^d = \left(g^{n/d}\right)^d = g^n = 1$$

e d'altro canto $h^k = 1 \iff g^{kn/d} = 1$

$\iff \text{ord}(g) \mid \frac{kn}{d} \iff n \mid \frac{kn}{d} \iff d \mid k$

e perciò $\text{ord}(h) = d$

2) g_1, g_2 di ordini n_1 ed n_2 E $(n_1, n_2) = 1$

$\Rightarrow$ $\text{ord}(g_1 \cdot g_2) = n_1 \cdot n_2$ [G abeliano!]

Oss $\underbrace{\langle g_1 \rangle}_{\text{sottogp. di ordine } n_1} \cap \underbrace{\langle g_2 \rangle}_{\text{sottogp. di ord } n_2} = K = \{1\}$

$K < \langle g_1 \rangle$, $K < \langle g_2 \rangle$

Per Lagrange,

$$\left.\begin{array}{l} \#K \mid \#\langle g_1 \rangle = n_1 \\ \#K \mid \#\langle g_2 \rangle = n_2 \end{array}\right\} \Rightarrow \#K \mid (n_1, n_2) = 1$$

$\text{ord}(g_1 \cdot g_2)$: voglio gli esponenti h t.c. $(g_1 \cdot g_2)^h = 1$

$$\underbrace{g_1 g_2 \; g_1 g_2 \; g_1 g_2 \cdots g_1 g_2}_{h \text{ volte}} = g_1^h \cdot g_2^h$$

$$g_1^h \cdot g_2^h = 1 \iff g_1^h = g_2^{-h}$$

$$\iff \begin{cases} g_1^h = 1 \\ \text{e} \\ g_2^{-h} = 1 \iff g_2^h = 1 \end{cases}$$

$$\iff \begin{cases} n_1 \mid h \\ n_2 \mid h \end{cases} \iff n_1 n_2 \mid h$$

e cioè $\text{ord}(g_1 g_2) = n_1 n_2$

Non è vero che $\text{ord}(g_1 \cdot g_2) = \text{mcm}\left(\text{ord}(g_1), \text{ord}(g_2)\right)$

Esempio: $G = \left(\mathbb{Z}/3\mathbb{Z}\right)^*$, $g_1 = g_2 = -1$

$\operatorname{ord}(g_1) = \operatorname{ord}(g_2) = 2$

$\operatorname{ord}(g_1 \cdot g_2) = 1$

3) $n_1, n_2 \in \mathcal{O} \Rightarrow \operatorname{mcm}(n_1, n_2) \in \mathcal{O}$

g_1 g_2

Es $\operatorname{mcm}(n_1, n_2) = d_1 \cdot d_2$ con $(d_1, d_2) = 1$, $d_1 \mid n_1$, $d_2 \mid n_2$

(per voi)

Dal punto 1: $g_1^{n_1/d_1}$ ha ord d_1

$g_2^{n_2/d_2}$ " " d_2

Dal pto 2: $g_1^{n_1/d_1} \cdot g_2^{n_2/d_2}$ ha ord $= d_1 \cdot d_2 = \text{mcm}(n_1, n_2)$

4) $\max \mathcal{O} = \text{mcm}\{\text{ord}(g) : g \in G\}$

$M := \max \mathcal{O}$. $\max \mathcal{O} \leq \text{mcm}(\text{ord}(g) : g \in G)$

Viceversa: se $n \in \mathcal{O}$, allora $\text{mcm}(n, M) \in \mathcal{O}$

$\geq M$ $\quad$ $= M$

$\Rightarrow n \mid M \Rightarrow M$ è multiplo di tutti gli altri ordini

Teo Sia p un n° primo. Il gruppo $(\mathbb{Z}/p\mathbb{Z})^\times$ è ciclico

Dim. $\mathcal{O} = \{\text{ord}(x) : x \in (\mathbb{Z}/p\mathbb{Z})^\times\}$, $M := \max \mathcal{O}$

Tesi: $M = p-1$ (ogni $\text{ord}(x) \mid p-1$)

Dall'es prima: $\forall x \in (\mathbb{Z}/p\mathbb{Z})^\times$, $\text{ord}(x) \mid M$

cioè $x^M \equiv 1 \ (p) \quad \forall x \in (\mathbb{Z}/p\mathbb{Z})^\times$

Sia $f(x) = x^M - 1$: vale $f(x) \equiv 0 \ (p) \quad \forall x \in (\mathbb{Z}/p\mathbb{Z})^\times$

$\Rightarrow$ $f(x)$ ha almeno $p-1$ radici

Ma $\#$ radici $\leq$ grado $f(x) = M$

$\#$ radici $= p-1$

$\square$

Un gruppo infinito con elem. di ordine finito

$$\mu_n = \{ \zeta \in \mathbb{C} \mid \zeta^n = 1 \} \simeq \mathbb{Z}/n\mathbb{Z}$$

$$\exp\left(\frac{2\pi i}{n} k\right) \longleftarrow k$$

$\mu_\infty = \bigcup_{n \geq 1} \mu_n$ è un gruppo con il prodotto.

$\mu_\infty \subseteq \mathbb{C}^\times$ è un sgp

- se $\zeta \in \mu_\infty \Rightarrow \exists\, n$ t.c. $\zeta \in \mu_n \Rightarrow \zeta^{-1} \in \mu_n \Rightarrow \zeta^{-1} \in \mu_\infty$
- se $\zeta_1, \zeta_2 \in \mu_\infty \to \exists\, n_1, n_2$ t.c. $\zeta_1 \in \mu_{n_1}$, $\zeta_2 \in \mu_{n_2}$

$$(\zeta_1 \zeta_2)^{n_1 n_2} = \zeta_1^{n_1 n_2} \cdot \zeta_2^{n_1 n_2} = 1 \cdot 1 = 1$$

$$\Rightarrow \zeta_1 \cdot \zeta_2 \in \mu_{n_1 \cdot n_2} \Rightarrow \zeta_1 \cdot \zeta_2 \in \mu_\infty$$

- Se $\zeta \in \mu_\infty \Rightarrow \exists n \quad \zeta \in \mu_n \Rightarrow \zeta^n = 1$

$\Rightarrow \operatorname{ord}(\zeta) \mid n$ es finito

GRUPPI III

Titolo nota

H ciclico, G/H ciclico

G gruppo ab., $H < G$ ciclico. Supponiamo:

i) G/H ciclico

ii) $\left(|G/H|, |H| \right) = 1$

$\Rightarrow$ G è ciclico

Soluz. Sia $m = |H|$ e $n = |G/H|$. $H \simeq \mathbb{Z}/m\mathbb{Z}$ e $G/H \simeq \mathbb{Z}/n\mathbb{Z}$.

$$\pi : G \longrightarrow G/H \simeq \mathbb{Z}/m\mathbb{Z}$$

$$g \longmapsto gH$$

π surgettiva, omom. di gruppi

$|G| = n \cdot m$. Vorrei trovare:

- $g_1 \in G$ di ordine m : basta prendere un generatore di $H \subseteq G$
- $g_2 \in G$ " " $n = |G/H|$

e poi usare $\text{ord}(g_1 g_2) = \text{ord}(g_1)\,\text{ord}(g_2)$ che vale siccome $(m, n) = 1$

Il quoz. G/H contiene un elem. xH di ordine n.

Cosa sappiamo su $\text{ord}_G(x)$?

$\pi : G \longrightarrow G/H$

$\pi(x) = xH$

$n = \text{ord}(\pi(x)) \mid \text{ord}(x)$

$\text{mcm}(\text{ord}(g_1), \text{ord}(x)) = \text{mcm}(m, n \cdot K)$ e~

divisib. per $m \cdot n$

$\operatorname{ord}(g_1) \mid \#G = m \cdot n$

$\operatorname{ord}(x) \mid \#G = m \cdot n$

$\Rightarrow \operatorname{mcm}(\operatorname{ord}(g_1), \operatorname{ord}(x)) = m \cdot n$

Dai fatti dell'eserc. scorsa $\Rightarrow$ esiste $g \in G$ di ordine $\operatorname{mcm}(\operatorname{ord}(g_1), \operatorname{ord}(x)) = mn \Rightarrow G$ ciclico.

Controesempi

- G non abeliano: $G = S_3$, $H = \langle (1,2,3) \rangle$

  $G/H \simeq \mathbb{Z}/2\mathbb{Z}$

- H non ciclico: $G = \mathbb{Z}/2\mathbb{Z} \times \overbrace{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}}^{\text{TCR}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

  $H = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \{0\}$

$$G/H \simeq \mathbb{Z}/3\mathbb{Z}$$

- $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $\quad H = \mathbb{Z}/2\mathbb{Z} \times \{0\}$ $\quad G/H \simeq \mathbb{Z}/2\mathbb{Z}$

Altro es $\quad G = \mathbb{Z} \quad H = 2\mathbb{Z} \quad G/H \simeq \mathbb{Z}/2\mathbb{Z}$

$$2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Cor $G = \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times$ è ciclico $\forall p$ dispari, $\forall n \geq 1$

Dim • ord mod p^n di $(1+p)$ è p^{n-1}

$\rightsquigarrow$ il sottogp $\langle 1+p \rangle =: H$ è ciclico di ordine p^{n-1}

- $\tilde{H} = \{ x \in (\mathbb{Z}/p^n\mathbb{Z})^\times : x \equiv 1 \ (p) \}$

$= \{ x \in \mathbb{Z}/p^n\mathbb{Z} : x \equiv 1 \ (p) \}$

$|\tilde{H}| = p^{n-1}$ = una classe ogni p, su un totale di p^n classi

- ogni el. di H è $\equiv 1 \ (p) \Rightarrow H \subseteq \tilde{H}$
- per cardinalità: $H = \tilde{H}$.
- $\varphi : (\mathbb{Z}/p^n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ $\quad [xy]_p = [x]_p \cdot [y]_p$

$[x]_{p^n} \longmapsto [x]_p$

φ è surgettivo; dato $[A]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$ si ha

$$[A]_p = f\left([A]_{p^n}\right)$$

$$\ker f = \left\{ x \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times : \quad f(x) \equiv 1 \pmod p \right\}.$$

$$= \left\{ x \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times : \quad x \equiv 1 \pmod p \right\} = H$$

1° teo di isomorfismo: $\operatorname{im} f \simeq G/\ker f$.

$$\Rightarrow \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \simeq G/H$$

$\uparrow$ ciclico di ordine $p-1$

H ciclico p^{n-1}, G/H ciclico di ord $p-1$ $\Longrightarrow$ G ciclico

□

Es $\#\left\{ x^k : x \in \left(\mathbb{Z}/p^n\mathbb{Z}\right)^\times \right\} = \dfrac{\varphi(p^n)}{(k, \varphi(p^n))}$ p dispari

$\#\left\{ x^k : x \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \right\} = \dfrac{p-1}{(k, p-1)}$ p qualsiasi

Dim L'insieme in questione è l'img. di $f : \left(\mathbb{Z}/p\mathbb{Z}\right)^\times \to \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$

$x \longmapsto x^k$

1° teo isom: $\dfrac{\overbrace{\left|\left(\mathbb{Z}/p\mathbb{Z}\right)^\times\right|}^{p-1}}{|\ker f|} = |\mathrm{Imm}|$

Si tratta di calcolare $\#\ker f$

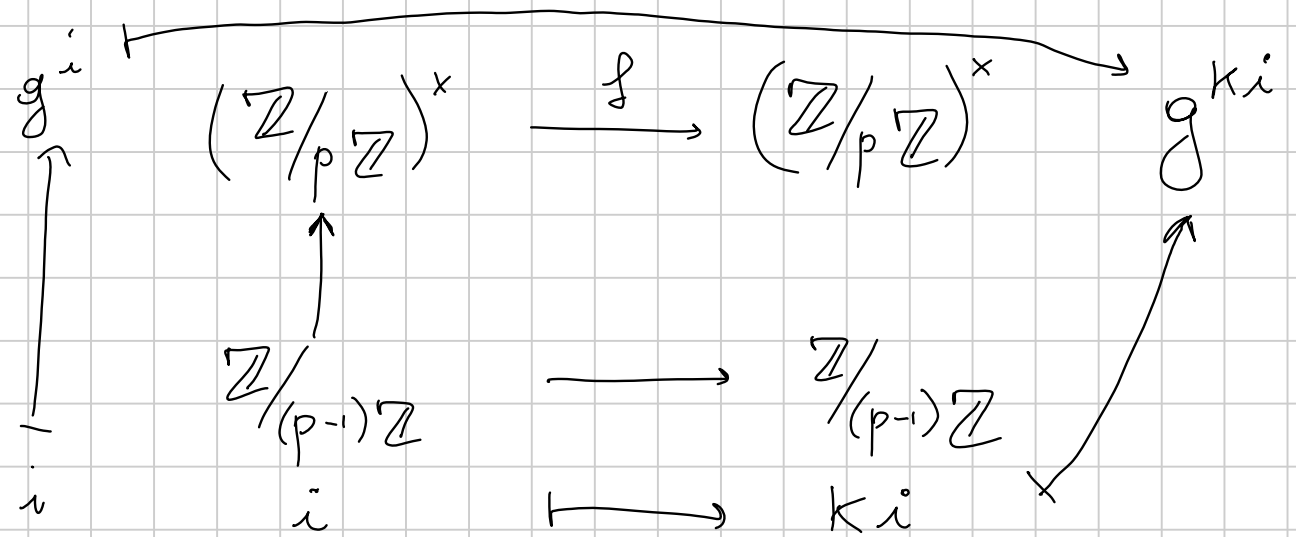
Siccome $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ ciclico, generato da g, gli elementi di $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ sono $\{ g^1, \dots, g^{p-1} \}$

$$g^i \in \ker f \iff g^{ki} \equiv 1 \quad (p)$$

$$\iff p-1 \mid ki$$

$$\iff ki \equiv 0 \quad (p-1)$$

Γ



$$ki \equiv 0 \quad (p-1) \iff i \equiv 0 \quad \left(\frac{p-1}{(k,p-1)} \right) : \text{la congr.}$$

d $\quad$ 1

ha $\frac{p-1}{d} = \frac{p-1}{(p-1)/(k,p-1)} = (k, p-1)$ soluzioni

Quindi: $\#\ker f = (k, p-1) \Rightarrow \#\,\mathrm{Imm}\, f = \frac{p-1}{(k,p-1)}$ □

Omom. e sgp. normali

$f: G_1 \longrightarrow G_2$ omomorfismo.

1) Se $H_1 < G_1$ è un sgp, $f(H_1) < G_2$? Sì
2) " $H_1 \triangleleft G_1$ " " " normale, $f(H_1) \triangleleft G_2$? NO
3) $H_2 < G_2$, è vero che $f^{-1}(H_2)$ è sgp di G_1? Sì
4) $H_2 \triangleleft G_2$, " " " " " norm. di G_1?

2) $\langle (1,2) \rangle < S_3$ non è normale.

$f(H_1) = \langle (1,2) \rangle$?

Se prendo $f: \langle (1,2) \rangle \longrightarrow S_3$ l'immersione, questa mi dà un controesempio!

Oss $H < G$ è normale $\iff$ $gHg^{-1} = H \quad \forall g \in G$

$gH = Hg$

$g h_1 g^{-1} \cdot g h_2 g^{-1} = g(h_1 h_2) g^{-1}$

4) Vediamo se $f: S_3 \longrightarrow G_2$ può avere $f^{-1}(H_2) = \langle (1,2) \rangle$

$\triangledown$

H_2

$f^{-1}(H_2) \supseteq \ker f$

$\ker f \triangleleft S_3$

$\downarrow$

può essere $\{e\}$, $\langle (1,2,3) \rangle$, S_3

$\rightsquigarrow$ $\ker f$ banale!

$S_3 \hookrightarrow G_2$

$\triangleright$

H_2

$g H_2 g^{-1} = H_2 \quad \forall g \in G_2$

$\Rightarrow g H_2 g^{-1} = H_2 \quad \forall g \in S_3$

Sarà vero? Sì!

$G_1 \xrightarrow{f} G_2 \xrightarrow{\pi} G_2/H_2$

$\ker(\pi \circ f) = \{ g \in G_1 : \pi(f(g)) = e H_2 \}$

$$= \{ g \in G_1 : \quad f(g)\, H_2 = e\, H_2 \}$$

$$= \{ g \in G_1 : \quad f(g) \in H_2 \} = f^{-1}(H_2),$$

cioè $f^{-1}(H_2)$ è un nucleo, e quindi un sgp. normale.

Altra possib: verificare che $\forall g \in G_1 \quad g\, f^{-1}(H_2)\, g^{-1} = f^{-1}(H_2)$

$\subseteq$ Prendiamo $g \times g^{-1}$ con $x \in f^{-1}(H_2)$.

Voglio $g x g^{-1} \in f^{-1}(H_2) \iff f(g x g^{-1}) \in H_2$

$\iff f(g)\, \underbrace{f(x)}_{\in H_2}\, f(g)^{-1} \overset{?}{\in} H_2$

• è vera perché

$f(g) \cdot H_2 \cdot (f(g))^{-1} = H_2$

$\square$ per voi!

in quanto $H_2 \trianglelefteq G_2$

Es 176 G grp, $\Delta := \{ (g,g) \mid g \in G \} \subseteq G \times G$

1. Δ è sgp ed è $\simeq G$

$$f: G \longrightarrow \Delta \qquad g \longmapsto (g,g)$$

$$h: \Delta \longrightarrow G \qquad (g,g) \longmapsto g$$

$$\tilde{f}: G \longrightarrow G \times G \qquad g \longmapsto (g,g)$$

è un omom. di grp.

$$\tilde{f}(g_1 \cdot g_2) \stackrel{?}{=} \tilde{f}(g_1) \cdot \tilde{f}(g_2)$$

$$(g_1 g_2, g_1 g_2) \stackrel{?}{=} (g_1, g_1) \cdot (g_2, g_2)$$ che sono uguali, ok

$\tilde{f}$ omom $\Rightarrow$ $\mathrm{Im}\,\tilde{f} = \Delta$ è un sottogp

$\Rightarrow$ f omom $\Rightarrow$ f è un isom (perché omom. bigettivo)

2. Δ è normale in $G \times G \iff G$ abeliano

$\Leftarrow$ G ab $\Rightarrow$ $G \times G$ ab $\Rightarrow$ ogni sgp è normale

$\Rightarrow$ $(g_1, g_2)\,\Delta\,(g_1, g_2)^{-1} = \Delta \quad \forall\, (g_1, g_2) \in G \times G$

Δ = $(g_1, g_2) \cdot (g_1^{-1}, g_2^{-1}) = (e, e)$

$$\{ (g_1, g_2)(g, g)(g_1^{-1}, g_2^{-1}) \mid g \in G \}$$

$$\{ (g_1 g g_1^{-1},\ g_2 g g_2^{-1}) \mid g \in G \}$$

Questo è $= \Delta \Rightarrow$ $g_1 g g_1^{-1} = g_2 g g_2^{-1}$ $\forall g \in G$

$\forall g_1, g_2 \in G$

$$\boxed{g_1 g g_1^{-1} g_2} = \boxed{g_2 g} \overset{?}{=} g g_2$$

In particolare: per $g_1 = id$, si ottiene

$$g g_2 = g_2 g \qquad \forall g \quad \forall g_2$$

cioè G abeliano.

3. G abeliano $\Rightarrow$ $\dfrac{G \times G}{\Delta} \simeq G$

IDEA FREQUENTE Cercare di renderlo un caso particolare del 1° teo. isomorfismo.

$G \times G$ = grp. partenza di un omom. f

Δ = $\ker f$

G = immagine f

$$f : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a + (-b) \\ & & a \cdot b^{-1} \end{array}$$

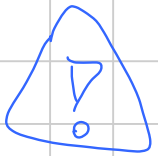
$$\ker f = \{ (a,b) : f(a,b) = 0 \} = \{ (a,b) : a + (-b) = 0 \}$$

$$\Delta = \{ (a,b) : a + (-b) + b = b \}$$

f omomorfismo:

$$f((a_1, b_1) + (a_2, b_2)) = f(a_1, b_1) + f(a_2, b_2)$$

$$(a_1 + a_2) - (b_1 + b_2) = (a_1 - b_1) + (a_2 - b_2) \quad \text{ok}$$



Notazione da non usare: $a \cdot (-b)$. Se l'operaz. è denotata $+$, l'opposto si scrive $-b$; se l'operaz. è "$\cdot$", l'inverso "" b^{-1}

Precisazione aggiunta dopo la lezione

In classe ho dimenticato di verificare che $\mathrm{Imm}\, f = G$, cioè che f è suriettiva:

$$f(G \times G) \supseteq f(G \times \{0\}) = \{ f((a,0)) \mid a \in G \}$$

$$= \{ a - 0 \mid a \in G \} = G$$

$$\Rightarrow \mathrm{Imm}\, f \supseteq G \Rightarrow \mathrm{Imm}\, f = G$$

Es 183

$$f: \mathbb{Z}/12\mathbb{Z} \longrightarrow \overbrace{\mathbb{Z}/4\mathbb{Z} \times S_3}^{H}$$: contare gli hom e gli hom. iniettivi

- f è determinato da $f(1)$
- Dato $h \in \mathbb{Z}/4\mathbb{Z} \times S_3$, esiste un omomorfismo $f: \mathbb{Z}/12\mathbb{Z} \to H$ t.c. $f(1) = h \iff \text{ord}(h) \mid 12$

Oss Vale in generale: dato G grp e $g \in G$, esiste un omom $f: \mathbb{Z}/n\mathbb{Z} \longrightarrow G$ t.c. $f(1) = g \iff \text{ord}(g) \mid n$

$h = (a, b)$ $\qquad h^{12} = (12\,a,\ b^{12}) = (0, id)$

$\Rightarrow$ tutti gli $h \in H$ hanno ordine che divide 12

$\Rightarrow$ gli omom. sono $|H| = 4 \cdot 6 = 24$

Poi: f iniettivo $\iff$ $f(1)$ ha ord 12

$\iff$ $h'' = (a, b)$ con $\operatorname{ord}(b) = 3$, $\operatorname{ord}(a) = 4$

$2 \cdot 2 = 4$ scelte.

GRUPPI IV

Titolo nota

TEOREMA DI CAUCHY PER GRUPPI ABELIANI

Sia G un grup. finito ABELIANO e p primo che divide $|G|$.

Allora $\exists\, g \in G$ di ordine p

Dim Scriviamo $|G| = p \cdot n$ e andiamo per induz. su n.

$n = 1$ $|G| = p \Rightarrow G \simeq \mathbb{Z}/p\mathbb{Z}$ contiene elem. ord p.

Passo induttivo Sia $h \in G \setminus \{e\}$ qualsiasi.

- se $\text{ord}(h)$ è multiplo di $p \Rightarrow$

  ① $\langle h \rangle$ è ciclico di ordine $\equiv 0 \ (p)$, e in un grup. ciclico ci sono elem. di ogni ordine che divide

$|\langle h \rangle|$, quindi in partic. elem. ord $= p$

② se l'insieme $\{ \text{ord}(g) : g \in G \}$ contiene un elemento $(\text{ord } h)$, contiene anche tutti i suoi divisori

③ se $\text{ord}(h) = p \cdot t$, $\text{ord}(h^t) = p$

– se $\text{ord}(h) \neq 0$ sia $H = \langle h \rangle$. Osservo che $H \triangleleft G$.

Considero G/H : e' un grup. ab., di cardinalita'

$< |G|$ $\left(= |G|/|H| \right)$, e $p \mid \#(G/H)$

$p \mid \dfrac{|G|}{|H|}$ ← divis. per p

← non e' divis. per p : $|H| = \text{ord}(h) \not\equiv 0 \ (p)$

Per ip. induttiva esiste $x \in G/H$ di ordine $= p$.

$\pi : G \longrightarrow G/H$ omom. di grp. surgettivo.

In particolare $\exists\, y \in G$ t.c. $\pi(y) = x$

$p = \text{ord}(x) = \text{ord}\,(\pi(y)) \mid \text{ord}\,(y)$

e si conclude come sopra (prendendo $h = y$) $\square$

$H < G, \quad K < G \rightsquigarrow HK \overset{?}{<} G$

Dati $H < G$, $K < G$ definiamo $HK = \{ h \cdot k \mid h \in H, k \in K \}$

$KH = \{ k \cdot h \mid h \in H, k \in K \}$

HK è un sottogp $\Leftrightarrow$ $HK = KH$

Oss Se almeno uno fra H e K è $\triangleleft G$, allora

(se $H \triangleleft G$) $\quad HK = \bigcup_{k \in K} H \cdot k = \bigcup_{k \in K} k \cdot H = K \cdot H$

Dim $\boxed{\Leftarrow}$ $*$ è $\in H \cdot K$, perché $e = \underset{\in H}{e} \cdot \underset{\in K}{e}$

$$* \quad (h_1 k_1) \cdot (h_2 k_2) = h_1 \, (k_1 \cdot h_2) \cdot k_2 = \overbrace{h_1 \cdot (h_3}^{\in H} \cdot \overbrace{k_3)}^{\in K} \cdot k_2$$

$k_1 \cdot h_2 \in K \cdot H \overset{\text{ipotesi}}{=} H \cdot K$, cioè $\exists \, h_3 \in H, k_3 \in K$ t.c. $k_1 \cdot h_2 = h_3 \cdot k_3$

$\| \quad (h_1 \cdot h_3) \cdot (k_3 \cdot k_2)$

* Sia $h \cdot k$ un elemento di $H \cdot K$. È vero che

$$\underbrace{k^{-1} \cdot h^{-1}}_{\in K \cdot H = H \cdot K} \stackrel{?}{\in} HK$$

$\boxed{\Rightarrow}$ HK sottogp. Vogliamo $HK = KH$

Doppia inclusione:

$\boxed{\supseteq}$ $k \cdot h \in H \cdot K \quad \forall k \in K, \forall h \in H$

$k = e \cdot k \in H \cdot K$
$h = h \cdot e \in H \cdot K$
} siccome HK sottogp $\Rightarrow k \cdot h \in HK$

$\boxed{\subseteq}$ Voglio mostrare che $h \cdot k \in K \cdot H \quad \forall h \in H, \forall k \in K$

Consideriamo $\underbrace{k^{-1}}_{(ek^{-1})} \cdot \underbrace{h^{-1}}_{(h^{-1}e)} \in HK$

$(ek^{-1}) \in HK \quad (h^{-1}e) \in H \cdot K$

Quindi: $k^{-1}h^{-1} \in HK$ dice che $\exists\, h_2 \in H$ $\exists\, k_2 \in K$

t.c. $k^{-1}h^{-1} = h_2 \cdot k_2$

inverso $\Longrightarrow$ $h \cdot k = k_2^{-1} \cdot h_2^{-1} \in KH$ □

Cardinalità di $H \cdot K$

$H < G$ e $K < G$; non richiediamo HK sia un sottogruppo

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Dim. $\varphi : H \times K \longrightarrow HK$

$$(h, k) \longmapsto hk$$

Es $G = \mathbb{Z}/12\mathbb{Z}$ $\quad H = \frac{2\mathbb{Z}}{12\mathbb{Z}}$ $\quad K = \frac{6\mathbb{Z}}{12\mathbb{Z}}$

$$H = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}, \bar{8}, \bar{10}\} \qquad K = \{\bar{0}, \bar{6}\}$$

$$H + K = \{\underset{0}{0+0}, \underset{6}{0+6}, \underset{10}{4+0}, \underset{8}{4+6}, \underset{2}{8+0}, \underset{}{8+6},$$
$$\underset{2}{2+0}, \underset{8}{2+6}, \underset{6}{6+0}, \underset{0}{6+6}, \underset{10}{10+0}, \underset{4}{10+6}\}$$

- φ è surgettiva (per definizione)
- Dato $hK \in \operatorname{imm} \varphi$, qual è la cardinalità di $\varphi^{-1}(hK)$?

$$(h_1, K_1) \xmapsto{\varphi} h_1 K_1 = hK$$

$$\Updownarrow$$

$$H \ni h^{-1} h_1 = K K_1^{-1} \in K$$

$$\Downarrow$$

$$h^{-1} h_1 \in H \cap K$$

Troviamo allora che è una bigezione!

$$\varphi^{-1}(hK) \longrightarrow H \cap K$$

$$(h_1, K_1) \longmapsto h^{-1} h_1 = K K_1^{-1}$$

$$(hx, x^{-1}K) \longmapsto x$$

$$(h_1, k_1) \longmapsto \underbrace{h^{-1} \cdot h_1}_{x} = \underbrace{k \cdot k_1^{-1}}_{x} \longmapsto (h \cdot (h^{-1} h_1), (k_1 \cdot k^{-1}) k)$$

$$\uparrow \qquad\qquad = \qquad\qquad (h_1, k_1)$$

$$x \in H \cap K \longmapsto (h \cdot x,\ x^{-1} k) \longmapsto h^{-1}(hx) = x$$

Abbiamo $H \times K \longrightarrow HK$ e $|H \cap K| = a - 1$

$$\Rightarrow |HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Centro

$$Z(G) = \{ h \in G \mid gh = hg \quad \forall g \in G \}$$

$Z(G) \trianglelefteq G$ $\qquad$ $g \cdot Z(G) = Z(G) \cdot g$

Dim. che se $G/Z(G)$ è ciclico, allora è banale (cioè G era abeliano, $Z(G) = G$)

Dim. $G/Z(G)$ è ciclico, cioè generato da un elemento che chiamiamo $g\,Z(G)$

Prendiamo $g_1, g_2 \in G$.

$$g_1 Z(G) = g^{k_1} Z(G)$$
$$g_2 Z(G) = g^{k_2} Z(G)$$

Vale perciò:

$$g^{-k_1} g_1 Z(G) = Z(G)$$

cioè $\exists\, z_1 \in Z(G)$ t.c. $g^{-k_1} g_1 = z_1$

$\Leftrightarrow$ $g_1 = g^{k_1} \cdot z_1$

Allo stesso modo $g_2 = g^{k_2} \cdot z_2$

$$g_1 g_2 = g^{k_1} z_1 \, g^{k_2} z_2 = g^{k_1} \cdot g^{k_2} \cdot z_1 \cdot z_2 = g^{k_1+k_2} z_1 z_2$$

$$g_2 g_1 = g^{k_2} z_2 \, g^{k_1} z_1 = g^{k_2} \cdot g^{k_1} \cdot z_1 \cdot z_2 = g^{k_1+k_2} z_1 z_2$$

$$g^{k_2} g^{k_1} z_2 z_1$$

Teo di corrispondenza

$G = \mathbb{Z} \times \mathbb{Z}$. Trovare i sgp. H di G t.c. $[G : H] = 5$.

$$\{\text{sgp. di } G/K\} \longleftrightarrow \{\text{sgp. di } G \text{ che } \supseteq K\}$$

Se H è come nel testo, $G/H \simeq \mathbb{Z}/5\mathbb{Z}$

gH — $H \iff g \in H \implies 5g \in H$

$(5g)H = H \iff 5g \in H$

Conclusione: se H è del tipo voluto, $H \supseteq \{5g \mid g \in \mathbb{Z} \times \mathbb{Z}\}$ (a,b)

$5\mathbb{Z} \times 5\mathbb{Z} = \{(5a, 5b) \mid a, b \in \mathbb{Z}\}$ $''$

$K := 5\mathbb{Z} \times 5\mathbb{Z}$. Per corrisp. $G = \mathbb{Z} \times \mathbb{Z}$

$$\left\{ \text{Sgp } H < G : \; H \supseteq K, \; [G:H] = 5 \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{sottogp di } G/K \\ \text{di indice } 5 \end{array} \right\}$$

$$\|$$

$$\left\{ \begin{array}{l} \text{sottogp di } (\mathbb{Z}/5\mathbb{Z})^2 \\ \text{di CARDIN. } 5 \end{array} \right\} = \left\{ \begin{array}{l} \text{sottogp di } \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \\ \text{di indice } 5 \end{array} \right\}$$

Es Dim che $\dfrac{A \times B}{C \times D} \simeq \dfrac{A}{C} \times \dfrac{B}{D}$

I sgp. di $(\mathbb{Z}/5\mathbb{Z})^2$ di card 5 sono ciclici; il loro numero è $\#\{\text{elementi di ord } 5\} / \varphi(5) = \dfrac{25-1}{4} = 6$

$$5(a,b) = (5a, 5b) = (0,0)$$

Concretamente sono:

- $\langle (1,0) \rangle$
- $\langle (1,1) \rangle$
- $\langle (1,2) \rangle$
- $\langle (1,3) \rangle$
- $\langle (1,4) \rangle$

l'unico elem. della forma $(1,x)$ è il generatore dato

$\langle (0,1) \rangle$

Non contiene elem. della forma $(1,x)$

Oss $\langle (1,2) \rangle = \{ (x,y) \in \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \mid y \equiv 2x \ (5) \}$

$\langle (1,2) \rangle = \langle (x, 2x) \rangle$

Chi sono i sgp di $\mathbb{Z}\times\mathbb{Z}$ corrispondenti?

$$\pi: \mathbb{Z}\times\mathbb{Z} \longrightarrow \frac{\mathbb{Z}\times\mathbb{Z}}{5\mathbb{Z}\times 5\mathbb{Z}}$$

$$C \longmapsto \pi(C)$$

$$\pi^{-1}(D) \longmapsto D$$

$$\pi^{-1}\left(\langle (1,3)\rangle\right) = \left\{ (x,y)\in\mathbb{Z}\times\mathbb{Z} \,:\, \pi((x,y))\in\langle(1,3)\rangle \right\}$$

$$= \left\{ (x,y)\in\mathbb{Z}\times\mathbb{Z} \,:\, y\equiv 3x \ (5) \right\}$$

$\exists$ 6 sgp sono: $\left\{ (x,y) \mid x\equiv 0\ (5) \right\} \longleftrightarrow \langle(0,1)\rangle$

$$\{(x,y) \mid y \equiv 0 \ (5)\} \longleftrightarrow \langle (1,0) \rangle$$

$k = 1, 2, 3, 4$

$$\{(x,y) \mid y \equiv kx \ (5)\} \longleftrightarrow \langle (1,k) \rangle$$

Oss $5\mathbb{Z} \times \mathbb{Z} < \mathbb{Z} \times \mathbb{Z}$

$\mathbb{Z} \times 5\mathbb{Z}$

$$\frac{\mathbb{Z} \times \mathbb{Z}}{5\mathbb{Z} \times \mathbb{Z}} \simeq \frac{\mathbb{Z}}{5\mathbb{Z}} \times \{0\}$$

Es 173 libro

G gyp, p primo, $H, K \trianglelefteq G$ di indice p con $H \cap K = \{e\}$. (H, K distinti)

1. Dim che $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

Per ipotesi, $G/H \simeq G/K \simeq \mathbb{Z}/p\mathbb{Z}$

$$f: G \longrightarrow G/H \times G/K \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

$$x \longmapsto (xH, xK)$$

È un omom? Sì:

$$f(xy) \overset{?}{=} f(x)\, f(y)$$

$$\| \qquad\qquad \| \text{ per def. di prodotto e di quoziente}$$

$$(xyH, xyK) = (xH, xK)\cdot(yH, yK)$$

$$\ker f = \{x \in G \mid f(x) = (H,K)\} = \{x \in G \mid (xH, xK) = (H,K)\}$$

$$= \{ x \in G \mid xH = H \quad e \quad xK = K \} = \{ x \in G \mid \begin{matrix} x \in H \\ x \in K \end{matrix} \}$$

$$= H \cap K = \{e\}$$

Dal 1° teo di isom: $\frac{G}{\ker f} \simeq \operatorname{imm} f \iff G \simeq \operatorname{imm} f$

Basta mostrare che f è surgettiva.

$G \simeq \operatorname{imm} f$ è isom. ad un sottogp. di $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

$$B < \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \quad : \quad \text{Lagrange} \Rightarrow |B| \mid p^2$$

$|B| = 1 \rightsquigarrow B$ banale; $|B| = p \rightsquigarrow B \simeq \mathbb{Z}/p\mathbb{Z}$; $|B| = p^2 \rightsquigarrow B \simeq (\mathbb{Z}/p\mathbb{Z})^2$

$|G| = 1$ no $\left(|G|/|H| = p \right)$; $|G| = p$; $|G| = p^2$

$H' = K = \{e\}$

ma H, K sono DISTINTI!

Quindi $|\mathrm{Im}\, f| = |G| = p^2 \Rightarrow f$ suriettiva

$\Rightarrow$ è l'isom. voluto

$$f : G \xrightarrow{\sim} G/H \times G/K \xrightarrow{\sim} \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$$

Due sgp normali

$H, K \trianglelefteq G$ con $H \cap K = \{e\}$

Allora $h \cdot k = k \cdot h \quad \forall h \in H \quad \forall k \in K$

$$gHg^{-1} = H \iff h \cdot k \cdot h^{-1} = k$$

$$\Updownarrow$$

$$H, K \ni (\underbrace{h \cdot k \cdot h^{-1}}) \cdot k^{-1} = e$$

$$\in K$$

$$hKh^{-1} = K$$

$$h \cdot \underbrace{(k \cdot h^{-1} \cdot k^{-1})} \in H$$

$$k \cdot H \cdot k^{-1} = H$$

$$\Rightarrow \quad hkh^{-1}k^{-1} \in H \cap K = \{e\}$$

$$\Rightarrow hkh^{-1}k^{-1} = e \quad \text{come voluto}$$

Titolo nota

$$G = \bigcup_{n \geq 1} \bigcup_{k} \{ \zeta_n^k \}, \qquad \zeta_n^k = e^{i 2\pi k/n}$$

Dim. che $G \simeq \mathbb{Q}/\mathbb{Z}$ $\qquad (\mathbb{Q}, +)$

$(\mathbb{Z}, +)$

Vorrei: un omom. da $\mathbb{Q}$ in G, surgettivo, con nucleo $\mathbb{Z}$

Consideriamo $f: \mathbb{Q} \longrightarrow G$, che è una funz.

$q \longmapsto e^{2\pi i q}$

surgettiva. È omom? $\qquad f(q_1 + q_2) = f(q_1) \cdot f(q_2)$

$$e^{2\pi i (q_1 + q_2)} = e^{2\pi i q_1} \cdot e^{2\pi i q_2}$$

Chi è il $\ker$? $\ker f = \{ q \in \mathbb{Q} : e^{2\pi i q} = 1 \}$

$e^{2\pi i q} = \cos(2\pi q) + i \sin(2\pi q)$

$\sin(2\pi q) = 0 \iff 2\pi q \in \mathbb{Z} \cdot \pi \qquad 2\pi q = n\pi$

$\iff q$ è $n/2$ per qualche $n \in \mathbb{Z}$

$\cos(2\pi q) = 1 \iff q \in \mathbb{Z}$

$\rightsquigarrow \ker f = \mathbb{Z}$, e dal 1° teo di isom:

$$G = \operatorname{Imm} f \simeq \mathbb{Q}/\mathbb{Z}$$

Oss $G = \bigcup \mu_n$ dove $\mu_n = \{ x \in \mathbb{C} \mid x^n = 1 \} \simeq \mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Q} \supseteq \left\{ \frac{k}{n} \;\middle|\; k \in \mathbb{Z} \right\} = \frac{1}{n}\mathbb{Z} \supseteq \mathbb{Z}$$

$$\left\{ \text{Sottogp di } \mathbb{Q}/\mathbb{Z} \right\} \longleftrightarrow \left\{ \text{sottogp di } \mathbb{Q} \text{ che contengono } \mathbb{Z} \right\}$$

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}} \longleftarrow \frac{1}{n}\mathbb{Z}$$

le classi laterali $\frac{k}{n} + \mathbb{Z}$

In effetti: la classe laterale $\frac{1}{n} + \mathbb{Z} \in \frac{\frac{1}{n}\mathbb{Z}}{\mathbb{Z}}$

genera: $\underbrace{\left(\frac{1}{n} + \mathbb{Z}\right) + \dots + \left(\frac{1}{n} + \mathbb{Z}\right)}_{k \text{ volte}} = \frac{k}{n} + \mathbb{Z}$

ed è di ordine n: $\left(\frac{1}{n} + \mathbb{Z}\right) + \dots + \left(\frac{1}{n} + \mathbb{Z}\right) = 0 + \mathbb{Z}$

$$\frac{k}{n} + \mathbb{Z} = 0 + \mathbb{Z}$$

se e solo se $k/n \in \mathbb{Z} \iff n \mid k$

Oss Sia $H < \mathbb{Q}/\mathbb{Z}$ FINITAMENTE GENERATO, cioè

$$H = \langle h_1, \dots, h_k \rangle$$

Tesi: H ciclico! Scriviamo $h_i = \frac{a_i}{b_i} + \mathbb{Z}$.

Posto $N = mcm(b_1, b_2, \dots, b_k)$, sia anche $\frac{a_i}{b_i} = \frac{c_i}{N}$

$$H = \left\langle \frac{c_1}{N} + \mathbb{Z}, \frac{c_2}{N} + \mathbb{Z}, \dots, \frac{c_k}{N} + \mathbb{Z} \right\rangle \subseteq \frac{\frac{1}{N}\mathbb{Z}}{\mathbb{Z}} \cong \mathbb{Z}/N\mathbb{Z}$$

Quindi H è sgp di un gp ciclico $\Rightarrow$ H ciclico.

Oss $H_2 = \left\{ q + \mathbb{Z} \;\middle|\; q = \frac{a}{2^k} \quad a \in \mathbb{Z},\ k \geq 1 \right\}$ non è ciclico.

($|H_2| = +\infty$: le classi di $\frac{1}{2^k} + \mathbb{Z}$ sono tutte distinti; se H_2 ciclico, H_2 sarebbe $\simeq \mathbb{Z}$, ma ogni elem. di H_2 ha ord. finito).

$\mathrm{Hom}(A \times B,\ C \times D)$

152: n° di omom. $G \to G$, dove $G = \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

Più generalmente: descrivere

$$\{ f : A \times B \to C \times D \quad \text{omomorfismi} \}$$

quando A, B, C, D sono grp. abeliani. Dimostreremo:

1. $\mathrm{Hom}(A, C\times D) \longleftrightarrow \mathrm{Hom}(A,C) \times \mathrm{Hom}(A,D)$

2. $\mathrm{Hom}(A\times B, C) \longleftrightarrow \mathrm{Hom}(A,C) \times \mathrm{Hom}(B,C)$

$$\Rightarrow \mathrm{Hom}(A\times B, C\times D) \overset{(2)}{\longleftrightarrow} \mathrm{Hom}(A, C\times D) \times \mathrm{Hom}(B, C\times D)$$

$$\longleftrightarrow \mathrm{Hom}(A,C) \times \mathrm{Hom}(A,D) \times \mathrm{Hom}(B,C) \times \mathrm{Hom}(B,D)$$

(152): $\#\mathrm{Hom}(\mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}) =$

$= \#\mathrm{Hom}(\mathbb{Z}/20, \mathbb{Z}/20\mathbb{Z}) \times \#\mathrm{Hom}(\mathbb{Z}/20\mathbb{Z}, \mathbb{Z}/8\mathbb{Z})$

$\times \#\mathrm{Hom}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/20\mathbb{Z}) \times \#\mathrm{Hom}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/8\mathbb{Z})$

$$= (20,20) \times (20,8) \times (20,8) \times (8,8)$$

$$= 20 \cdot 4 \cdot 4 \cdot 8.$$

$$\mathrm{Hom}(A, C \times D) \longleftrightarrow \mathrm{Hom}(A,C) \times \mathrm{Hom}(A,D)$$

$$\varphi \longmapsto (\varphi_1, \varphi_2)$$

$$\varphi(a) = (\varphi_1(a), \varphi_2(a))$$

$$\left(\begin{array}{c} A \longrightarrow C \times D \\ a \longmapsto (\varphi_1(a), \varphi_2(a)) \end{array} \right) \longleftarrow\!\shortmid (\varphi_1, \varphi_2)$$

Vediamo che φ omom implica φ_1 e φ_2 omom.

$$\varphi(a+b) = (\varphi_1(a+b),\ \varphi_2(a+b))$$

φ è un omomorfismo

$$\varphi(a)+\varphi(b) = (\varphi_1(a), \varphi_2(a)) + (\varphi_1(b), \varphi_2(b))$$

$$= (\varphi_1(a)+\varphi_1(b),\ \varphi_2(a)+\varphi_2(b))$$

Invece, per $\mathrm{Hom}(A\times B, C) \longleftrightarrow \mathrm{Hom}(A,C)\times\mathrm{Hom}(B,C)$

$$\varphi \qquad (a\mapsto \varphi(a,e);\ b\mapsto \varphi(e,b))$$

$$\left(\begin{array}{ccc} A\times B & \longrightarrow & C \\ (a,b) & \longmapsto & \varphi_1(a)+\varphi_2(b) \end{array}\right) \longleftarrow\!\shortmid \qquad (\varphi_1, \varphi_2)$$

p-gruppi abeliani elementari: $G = \underbrace{\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \times \dots \times \mathbb{Z}/p\mathbb{Z}}_{k}$

Oss Ogni tale gruppo è automaticamente uno s.v. su $\mathbb{F}_p$,

con $g_1 = (x_1, \dots, x_k)$

$g_2 = (y_1, \dots, y_k)$

$\lambda \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$g_1 + g_2 = (x_1 + y_1, x_2 + y_2, \dots, x_k + y_k)$

$\lambda \cdot g_1 = (\lambda x_1, \lambda x_2, \dots, \lambda x_k)$

Oss • Ogni sgp è un sottosp. vettoriale

• $\#\{H < G \mid \#H = p^{k-1}\} = \#\{$luoghi di zeri di 1 eqz. lineare$\}$

$= \#\{H : H = \{a_1 x_1 + \dots + a_k x_k = 0\}\}$

$$= \frac{p^k - 1}{p - 1}$$

$x_1 + 2x_2 - x_3 = 0$

$\lambda x_1 + 2\lambda x_2 - \lambda x_3 = 0$

di eqz lineari in k variabili a coeff. in $\mathbb{F}_p$, non $0 = 0$

↖ n° dei fattori di proporzionalità non nulli

Es $k = 2$: i sgp di ord. p in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ sono $\frac{p^2-1}{p-1}$

Oss Sottogp di ordine p^2 in $\left(\mathbb{Z}/p\mathbb{Z}\right)^k = \{\text{sottosp. di dim } 2\}$

Per generare uno sotto spazio di dim 2 mi servono 2 elementi lin. indip. v_1, v_2

$\underbrace{(p^k - 1)}_{\text{scelte per } v_1} \cdot \underbrace{(p^k - p)}_{\text{scelte per } v_2}$ ← multipli di v_1

Però, viceversa: fissato un sottosp. di dim 2, questo quante basi ha? $(p^2-1)(p^2-p)$

$$\#\text{ sottosp. di dim } 2 = \#\text{ sottogp. di ord } p^2 = \frac{(p^k-1)(p^k-p)}{(p^2-1)(p^2-p)}$$

Es 166

$$G = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$$

- $H < G$ di ordine 4

  $H \simeq \mathbb{Z}/4\mathbb{Z}$: sono $\dfrac{\#\text{ elementi di ordine } 4}{\varphi(4)}$

  $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$: chi sono gli elem. di ordine 2 in G?

$\longrightarrow (4,6)\ ;\quad (4,12)\ ;\quad (8,6)$

$2(a,b) = (0,0)$

$\begin{cases} 2a \equiv 0\ (8) \\ 2b \equiv 0\ (12) \end{cases}$ $\qquad$ $a \equiv 0\ (4)$ $\qquad$ $b \equiv 0\ (6)$

L'unico sgp $\simeq (\mathbb{Z}/2\mathbb{Z})^2$ è $\dfrac{4\mathbb{Z}}{8\mathbb{Z}} \times \dfrac{6\mathbb{Z}}{12\mathbb{Z}}$

$\{\bar{0}, \bar{4}\} \times \{\bar{0}, \bar{6}\}$

- Contare gli $H < G$ con $|H| = 48$ $\Leftrightarrow$ indice 2

Se $[G:H] = 2 \Rightarrow \forall g \in G,\ g + H \in G/H$

$G/H \simeq \mathbb{Z}/2\mathbb{Z}$

$2g + H = H$

$\Rightarrow 2g \in H$

Conclusione: $K := \{ 2g \mid g \in G \} \subseteq H$

$$\left\{ \begin{array}{l} \text{sottogp di } G \text{ di indice } 2 \\ (\text{che contengono } K) \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{l} \text{sottogp di } G/K \\ \text{di indice } 2 \end{array} \right\}$$

$$K = \left\{ (2a, 2b) \mid (a,b) \in \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \right\} = \frac{2\mathbb{Z}}{8\mathbb{Z}} \times \frac{2\mathbb{Z}}{12\mathbb{Z}}$$

$$G/K = \frac{\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}}{2\mathbb{Z}/8\mathbb{Z} \times 2\mathbb{Z}/12\mathbb{Z}} \simeq \frac{\mathbb{Z}/8\mathbb{Z}}{2\mathbb{Z}/8\mathbb{Z}} \times \frac{\mathbb{Z}/12\mathbb{Z}}{2\mathbb{Z}/12\mathbb{Z}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Conclusione: $\#\{ H \text{ con } \#H = 48 \} = \#\{ \text{sgp di } (\mathbb{Z}/2\mathbb{Z})^2 \text{ di indice } 2 \}$

$= 3$

Anelli

Elencare pol. irriid. in $\mathbb{F}_2[x]$ di grado ≤ 4

Grado 1: x, $x+1$ $\qquad a_1 x + a_0$

$x = x \cdot 1$

Grado 2: $x^2 = x \cdot x$ $\qquad x^2+1 = (x+1)^2$ $\qquad a_2 x^2 + a_1 x + a_0$ ($a_2 = 1$)

$x \cdot (x+1) = x^2 + x$ $\qquad x^2 + x + 1$

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

irriducibile, perché non ha radici ED E' DI GRADO ≤ 3

Grado 3: $x^3 + 1$ $\qquad \boxed{x^3 + x + 1}$ $\qquad \boxed{x^3 + x^2 + 1}$

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

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

Grado 4: $X^4 + X^2 + 1 = (x^2 + x + 1)^2$

$1 + 3$ $\qquad$ $2 + 2$

$X^4 + X^2 + 1 = (\underbrace{f(x)}_{\text{grado } 1})\, g(x)$ $\qquad$ $X_0^4 + X_0^2 + 1 = \overset{\circ}{\widetilde{f(x_0)}}\, g(x_0)$

$X^4 + X + 1$ è irriducibile: non ha radici; non può essere (grado 2 irr) × (grado 2 irrid)

$(x^2 + x + 1)(x^2 + x + 1)$

In generale: in $\mathbb{F}_2[x]$ un pol. di grado 4 è irrid.

se e solo se non ha radici E non è X^4+X^2+1

Criterio della derivata

$f(x) \in K[x]$. Allora le seguenti sono equivalenti:

1) $(f(x), f'(x)) \neq (1)$

2) $\exists\, \alpha \in \overline{K}$ t.c. $f(x) = (x-\alpha)^2 \cdot g(x)$ in $\overline{K}[x]$

Supponiamo che $(f(x), f'(x)) = 1$

$\xrightarrow{\text{Bézout}}$ $f(x)\, a(x) + f'(x)\, b(x) = 1$ (*)

Se per assurdo $f(x) = (x-\alpha)^2 g(x)$ $\quad f(\alpha) = 0$

$f'(\alpha) = 0$ $\qquad$ $f'(x) = 2(x-\alpha)\,g(x) + (x-\alpha)^2 g'(x)$

Oss/Def. • La derivata di $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

è $\qquad f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$

• Vale $\qquad (f(x)\,g(x))' = f(x)'\,g(x) + f(x)\,g'(x)$

Sostituendo $x = \alpha$ in (A) trovo $0 \cdot a(\alpha) + 0 \cdot b(\alpha) = 1$,

assurdo. Abbiamo dim che (non 1) $\Rightarrow$ (non 2)

$(f, f') = 1 \Rightarrow f$ non ha radici multiple

Viceversa: supponiamo che f non abbia radici multiple.

Se per assurdo $(f(x), f'(x)) \neq 1$, diciamo che

$(f(x), f'(x)) = a(x)$ di grado ≥ 1.

Allora su $\overline{K}$ abbiamo che:

- $f(x) = a(x)\, g(x)$ in $\overline{K}[x]$
- $f'(x) = a(x)\, h(x)$ in $\overline{K}[x]$
- $\exists\, \beta \in \overline{K}$ t.c. $a(\beta) = 0 \Rightarrow x-\beta \mid a(x) \mid f(x)$

$$\underbrace{x-\beta \mid a(x) \mid f'(x)}_{f'(x) = (x-\beta)\cdot q(x)}$$

$\Rightarrow f(x) = (x-\beta)\cdot j(x)$

$f'(x) = j(x) + (x-\beta)\cdot j'(x)$

Valuto in β: $0 = j(\beta) + 0 \cdot j'(\beta) \Rightarrow x-\beta \mid j(x)$

$\Rightarrow j(x) = (x-\beta)\, l(x)$

$f(x) = (x-\beta)^2 \ell(x)$ ha una rad. doppia

Es $X^4 + X^2 + 1 = f(x) \in \mathbb{F}_2[x]$; $f'(x) = 4X^3 + 2X^2 = 0$

Es (campo di spezz. di $X^3 - 2$ su $\mathbb{Q}$)

Radici: $\sqrt[3]{2}$, $\sqrt[3]{2} \cdot \zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$

C. d. s. $K = \mathbb{Q}\left(\sqrt[3]{2}, \sqrt[3]{2}\,\zeta_3, \sqrt[3]{2}\cdot\zeta_3^2\right)$ — K_1

$= \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$ — K_2

⊂ Se in un campo ho $\sqrt[3]{2}$ e ζ_3 ho anche $\sqrt[3]{2}\cdot\zeta_3$ e $\sqrt[3]{2}\cdot\zeta_3\cdot\zeta_3$

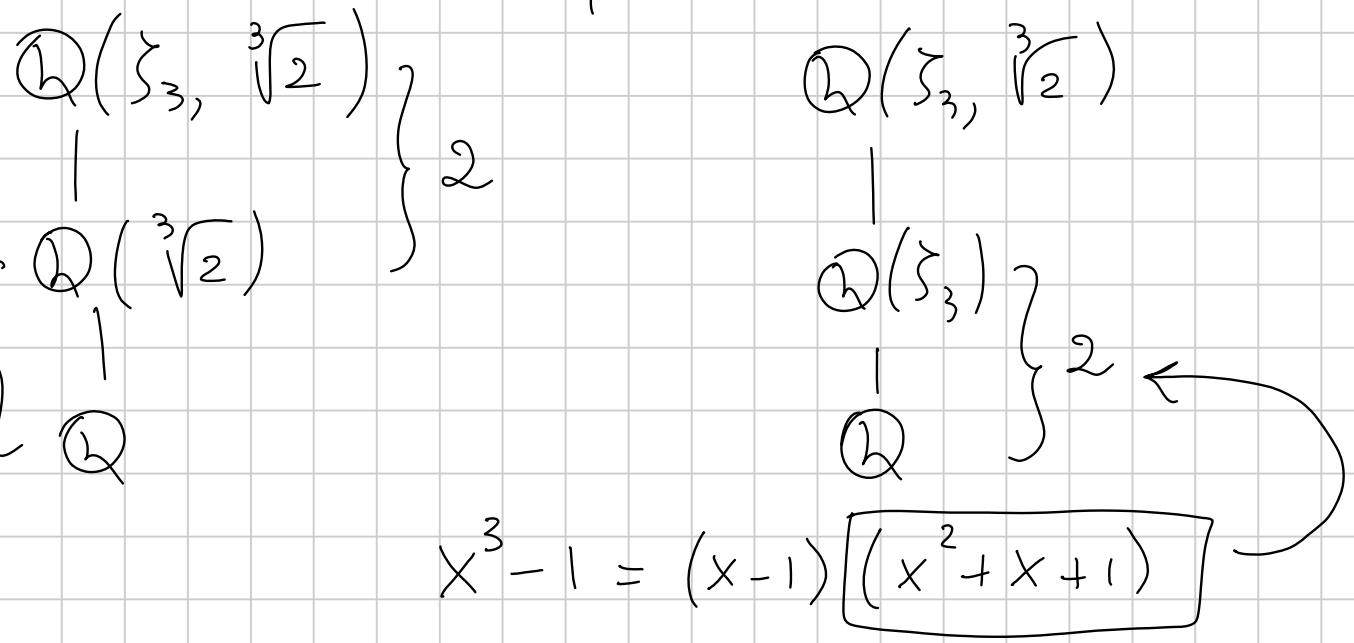
K_2 è un campo e contiene $\sqrt[3]{2}$, $\sqrt[3]{2}\,\zeta_3$, $\sqrt[3]{2}\,\zeta_3^2$

$\Rightarrow$ K_2 contiene il più piccolo campo con questi 3 elem., cioè K_1

3 $K_1 \supseteq K_2$: $K_1 \ni \sqrt[3]{2}$ per def.

$$K_1 \ni \zeta_3 = \left(\sqrt[3]{2}\cdot\zeta_3\right) / \left(\sqrt[3]{2}\right)$$

($\sqrt[3]{2}\cdot\zeta_3 \in K_1$, $\sqrt[3]{2} \in K_1$) □



$[\mathbb{Q}(\zeta_3, \sqrt[3]{2}) : \mathbb{Q}]$ è divisibile per 6

$\Rightarrow$ è uguale a 6.

ANELLI & CAMPI

Titolo nota

Fattorizzazione Radici raz.: a/b con $a \mid 1$ e $b \mid 1$

$f(x) = \boxed{x^4 + 3x^3 - x^2 + 1}$: fattorizz. in $\mathbb{F}_2[x]$, $\mathbb{F}_3[x]$, $\mathbb{Q}[x]$

- $\mathbb{F}_2$: $f(x) \equiv x^4 + x^3 + x^2 + 1$

  $x^4 + x^3 = x^3 \cdot (x+1)$

  $\equiv (x+1)\underbrace{(x^3 + x + 1)}_{\text{irriducibile}}$

  $x^2 + 1 = (x+1)^2$

- $\mathbb{F}_3$: $f(x) \equiv x^4 - x^2 + 1 \equiv x^4 + 2x^2 + 1$

  $= (x^2 + 1)^2$

  $x^2 \equiv -1 \quad (3)$

Oss. $f'(x) = 4x^3 - 2x = x^3 + x = x \cdot (x^2 + 1)$.

- Q: equivalentemente voglio fattorizzare in $\mathbb{Z}[x]$

  * Se $f(x)$ avesse una radice, $f(b)=0$, allora riducendo mod 3 avrei $\overline{f}(\overline{b}) \equiv 0\ (3)$, e $f(x)$ mod 3 avrebbe una radice, NO

  In alternativa: criterio radici raz. dice che basta verificare $f(\pm 1) \neq 0$

  * $f(x) = g(x) \cdot h(x)$ con $\deg g = \deg h = 2$

    $\downarrow$ mod 2

    $\overline{f(x)} \equiv \overline{g(x)} \cdot \overline{h(x)}$ in $\mathbb{F}_2[x]$.

    $\|$

    $(x+1)(x^3+x+1)$ dove x^3+x+1 è IRRIDUCIBILE in $\mathbb{F}_2[x]$,

assurdo perché $3 = \deg(x^3+x+1) > \deg g(x), \deg h(x)$.

$\Rightarrow$ $f(x)$ irrid. in $\mathbb{Z}[x]$ $\Rightarrow$ $f(x)$ irrid in $\mathbb{Q}[x]$

Quozienti di $K[x]$

$f(x) = x^3 - 5x^2 + 7x - 3$ e $A := \mathbb{F}_5[x] / (f(x))$.

Calcolare $\#A$, il n° di divisori di zero, di invertibili, di nilpotenti.

$f(x) \equiv x^3 + 2x + 2 = (x-1)^2(x+a)$ $\quad (x-1)^2(x+2)$

$f'(x) = 3x^2 + 2 = 3 \cdot (x^2+4) = 3(x^2-1)$ $\quad 2 = a$

* $\#A = \#\{$ resti nella divisione per $f(x)\}$

$$= \# \left\{ a_0 + a_1 x + a_2 x^2 : \quad a_0, a_1, a_2 \in \mathbb{F}_5 \right\}$$

$$= 5^3$$

Base: $1, x, x^2$

Sp. vett $\simeq \mathbb{F}_5^3$

* Divisori di 0: sono i polinomi NON coprimi con $f(x) = (x-1)^2(x+2)$

$$D_1 = \left\{ \overline{g(x)} \in A \mid x-1 \mid g(x) \right\}$$

$$D_2 = \left\{ \overline{g(x)} \in A \mid x+2 \mid g(x) \right\}$$

$$\# D_1 = \# \left\{ (x-1)\, h(x) \right\} = 25 \quad \text{con} \quad h(x) = ax+b \text{ è di grado} \leq 1$$

Dato $\overline{g(x)} \in A$ con $x-1 \mid g(x)$, esiste un unico rappresentante $q(x)$ con $\deg q(x) \leq 2$ e $x-1 \mid q(x)$

$$q(x) = (x-1)\, h(x)$$

$$\# D_2 = 25$$

$$\# (D_1 \cup D_2) = \# D_1 + \# D_2 - \# (D_1 \cap D_2)$$

$$D_1 \cap D_2 = \left\{ \overline{g(x)} : (x-1)(x+2) \mid g(x) \right\}$$

$$\Rightarrow \begin{cases} x-1 \mid g(x) \\ x+2 \mid g(x) \end{cases} \qquad g(x) = k(x-1)(x+2)$$

$\hookrightarrow \in \mathbb{F}_5$

$$\#(D_1 \cup D_2) = 25 + 25 - 5 = 45$$

* Invertibili: $125 - \#$ divisori di zero $= 80$

* Nilpotenti: sono le classi $\overline{g(x)}$ divisibili per ognuno dei fattori irriducibili di $f(x)$

$$\mathbb{Z}/_{3^3 5^2 7^8}\mathbb{Z}$$

multipli di $(x-1)(x+2)$

$\| \quad \| \quad \|$

$D_1 \cap D_2$

I nilpotenti sono 5

$A = \mathbb{F}_3[x]/(x^2+1)$

$\#A = 3^2$ (s.v. su $\mathbb{F}_3$ di dim 2)

Siccome x^2+1 è irriducibile in $\mathbb{F}_3[x]$ (grado 2 e no radici),

A è un campo con 9 elementi

Chiamiamo $\alpha = \overline{x}$. Chi sono le potenze di α?

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

$$\alpha^3 = -\alpha$$

$$\alpha^4 = (\alpha^2)^2 = (-1)^2 = 1$$

$$A = \{ \overline{a+bx} \text{ con } a,b \in \mathbb{F}_3 \} = \{ a+bi \mid a,b \in \mathbb{F}_3 \}$$

$$(a+bi)(c+di) = (ac-bd) + i(bc+ad)$$

$$\overline{(a+bx)} \cdot \overline{(c+dx)} = \overline{ac+bcx+adx+bdx^2}$$

$$= \overline{ac + bcx + adx + bd(x^2+1) - bd}$$

$$= \overline{\underbrace{ac - bd}_{} + \underbrace{(ad + bc)}_{} x}$$

Oss $\{ a + bi \mid a, b \in \mathbb{F}_5 \}$ non e' un campo!

$(2+i)(2-i) = 4 - (-1) = 5 = 0$

$$\rightarrow \frac{\mathbb{F}_5[x]}{(x^2+1)} = \frac{\mathbb{F}_5[x]}{(x^2-4)}$$

Oss

$$\begin{array}{c} A \\ | \\ \mathbb{F}_3 \end{array}$$

- e' un'est. di campi di grado 2
- $\mathbb{F}_3(\alpha) = A$

$0, \quad 1, \quad 2, \quad \alpha$

$1+\alpha, \quad 2+\alpha, \quad 2\alpha$

$1+2\alpha, \quad 2+2\alpha$

$$\begin{array}{c} A \\ | \\ \mathbb{F}_3(\alpha) \\ | \\ \mathbb{F}_3 \end{array}$$

$$\mathbb{F}_3 \subseteq \mathbb{F}_3(\alpha) \subseteq A$$

$$1 < [\mathbb{F}_3(\alpha) : \mathbb{F}_3]$$

$$\Rightarrow \underbrace{[A : \mathbb{F}_3]}_{2} = [A : \mathbb{F}_3(\alpha)] \cdot \underbrace{[\mathbb{F}_3(\alpha) : \mathbb{F}_3]}_{>1}$$

$$\Rightarrow [\mathbb{F}_3(\alpha) : \mathbb{F}_3] = 2$$

Allora $\mathbb{F}_3(\alpha) \subseteq A$ ed entrambi hanno dim 2 su $\mathbb{F}_3$

$\Rightarrow$ sono uguali.

- $\langle \alpha \rangle \subseteq A^\times$ ← ha 8 elementi: $A^\times \neq \langle \alpha \rangle$

  $\{\alpha, -1, -\alpha, 1\}$

Polinomi minimi

$f(x) = x^4 + 2x^2 + 2 \in \mathbb{Q}[x]$. Sia $\alpha \in \mathbb{C}$ radice di $f(x)$

- Pol. min. di $\alpha^2 + 1$ su $\mathbb{Q}$
- Pol. min di $\frac{1}{\alpha + 2}$ su $\mathbb{Q}$

$t = x^2$ $\qquad t^2 + 2t + 2 = 0$ $\qquad t_{1,2} = -1 \pm \sqrt{-1} = -1 \pm i$

$x_1, x_2, x_3, x_4 = \pm\sqrt{-1+i}, \pm\sqrt{-1-i}$

α è uno di questi 4 numeri, $\alpha^2 + 1 = \pm i$ ha polinomio minimo $x^2 + 1$

$$0 = f(\alpha) \implies \alpha^4 + 2\alpha^2 + 2 = 0$$

$$(\alpha^2+1)^2 + 1 = 0$$

In particolare $g(x) := x^2+1$ si annulla in α^2+1

Cerchiamo $q(x) \in \mathbb{Q}[x]$ che si annulli in $\alpha+2$.

$$q(x) = f(x-2)$$

$$q(\alpha+2) = f((\alpha+2)-2) = f(\alpha) = 0$$

Ora cerco $r(x)$ che si annulli in $\frac{1}{\alpha+2}$.

$$r(x) = x^4 q\left(\frac{1}{x}\right)$$

$$q(x) = f(x-2) = (x-2)^4 + 2(x-2)^2 + 2 =$$

$$= x^4 - 8x^3 + 26x^2 - 40x + 26$$

$$q\left(\frac{1}{x}\right) = \frac{1}{x^4} - \frac{8}{x^3} + \frac{26}{x^2} - \frac{40}{x} + 26$$

$$= \frac{1 - 8x + 26x^2 - 40x^3 + 26x^4}{x^4}$$

$$x^4 \cdot q\left(\frac{1}{x}\right) = 26x^4 - 40x^3 + 26x^2 - 8x + 1$$

Candidato pol. minimo: $x^4 - \frac{20}{13}x^3 + x^2 - \frac{4}{13}x + \frac{1}{26}$

Fatto Il grado del pol. min. coincide con il grado

$$\left[\mathbb{Q}\left(\frac{1}{\alpha+2}\right) : \mathbb{Q} \right]$$

$$\left[\mathbb{Q}\left(\frac{1}{\alpha+2}\right) : \mathbb{Q} \right] = \left[\mathbb{Q}(\alpha+2) : \mathbb{Q} \right] =$$

$$= \left[\mathbb{Q}(\alpha) : \mathbb{Q} \right] = 4$$

Ci basterebbe $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ } cioè ci basta x^4+2x^2+2
α radice di x^4+2x^2+2 } irriduc. in $\mathbb{Q}[x]$

(o anche in $\mathbb{Z}[x]$, lemma di Gauss)

x^4+2x^2+2 è irriducibile (in $\mathbb{Z}[x]$) per Eisenstein $p=2$

Pol. min. di $\sqrt{2+\sqrt{7}}$

$\alpha = \sqrt{2+\sqrt{7}} \in \mathbb{C}$

1) $[\mathbb{Q}(\alpha) : \mathbb{Q}]$

2) Il grado del campo di spezz. su $\mathbb{Q}$ del pol. min. di α

$\alpha^2 = 2+\sqrt{7} \Rightarrow \alpha^2 - 2 = \sqrt{7} \Rightarrow (\alpha^2-2)^2 = 7$

$\Rightarrow \alpha^4 - 4\alpha^2 + 4 - 7 = 0$

$f(x) = x^4 - 4x^2 - 3$ è UN polinomio che si annulla per $x = \alpha$. Mostriamo che è irrid.

$f(x)$ ha 4 radici, $\pm\sqrt{2+\sqrt{7}}$, $\pm\sqrt{2-\sqrt{7}}$ $=$ $\underset{\in\mathbb{R}}{x_1}, \underset{\in\mathbb{R}}{x_2}, \underset{\in\mathbb{C}\setminus\mathbb{R}}{x_3, x_4}$

Se $x_i \in \mathbb{Q} \Rightarrow x_i^2 - 2 = \pm\sqrt{7} \in \mathbb{Q}$, assurdo.

$$f(x) = \left(x - \sqrt{2+\sqrt{7}}\right)\left(x + \sqrt{2+\sqrt{7}}\right)\left(x^2 - (2-\sqrt{7})\right) \text{ in } \mathbb{R}[x]$$

$$f(x) = g(x)\ h(x) \text{ in } \mathbb{Q}[x]$$

Se fossero 2 fattori irriduc. di grado 2 in $\mathbb{Q}[x]$, uno dei due dovrebbe essere $x^2 - (2-\sqrt{7})$, assurdo (non è in $\mathbb{Q}[x]$)

Allora $f(x)$ è monico, rispetta $f(\alpha)=0$, ed è irriduc

$\Rightarrow$ è il pol. minimo di α

1) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f(x) = 4$

2) Il c.d.s. è $\mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(x_1, x_3)$

$= \mathbb{Q}(\sqrt{2+\sqrt{7}}, \sqrt{2-\sqrt{7}})$

$$\begin{cases} \mathbb{Q}(\sqrt{2+\sqrt{7}}, \sqrt{2-\sqrt{7}}) = K \\ | \\ \mathbb{Q}(\sqrt{2+\sqrt{7}}) = L \\ | \\ \mathbb{Q} \end{cases} \begin{matrix} \} 2 \\ \} 4 \end{matrix}$$

Vorrei $[K : L]$.

$x_3^2 = 2 - \sqrt{7} \in L$

Il pol.

$x^2 - (2 - \sqrt{7}) \in L[x]$

si annulla in $x_3 \Rightarrow [L(x_3) : L] \leq 2$

Ma $L \neq K$, perché $L \subseteq \mathbb{R}$ mentre $K \not\subseteq \mathbb{R}$ perché $x_3 \notin \mathbb{R}$. Quindi $[K : L] > 1 \Rightarrow [K : L] = 2$

Per torri, $[K : \mathbb{Q}] = [K : L] \cdot [L : \mathbb{Q}] = 2 \cdot 4 = 8$

Oss Può succedere

$K(x_1, x_2)$

3 | 1

$K(x_1)$

4 | 1

K

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

dove $f(x) = (x - x_1)(x - x_2)(x - x_3)(x - x_4)$ è irrid in $K[x]$.

Oss $K(x_1, x_2) = \{ p(x_1, x_2) \mid p \in \mathbb{Q}[s, t] \}$

Estensioni quadratiche

Sia K un campo con $\operatorname{char}(K) \neq 2$, sia L/K un'estensione di grado 2. Allora $\exists\, \alpha \in K$ t.c. $L = K(\sqrt{\alpha})$

Sia $\beta \in L \setminus K$. Osservo che $K(\beta) = L$

$$1 < [K(\beta) : K] \leq 2 \quad \Rightarrow \quad [K(\beta) : K] = 2$$

$$\Rightarrow L = K(\beta)$$

$\{1, \beta, \beta^2\}$ sono 3 el. di L (che ha dim 2)

$\Rightarrow$ Sono lin. dip.

$$c_2 \beta^2 + c_1 \beta + c_0 = 0 \quad \text{con } c_i \in K \text{ non tutti nulli}$$

Se $c_2 = 0 \Rightarrow c_1 \beta + c_0 = 0 \Rightarrow \beta = -c_0/c_1 \in K$ No

Divido per c_2: $\beta^2 + \frac{c_1}{c_2}\beta + \frac{c_0}{c_2} = 0$

$$\left(\beta + \frac{c_1}{2c_2}\right)^2 + \frac{c_0}{c_2} - \frac{c_1^2}{4c_2^2} = 0 \qquad (*)$$

↖ char $K \neq 2$

Detto $\gamma := \beta + \frac{c_1}{2c_2}$

$$K(\gamma) = K(\beta) = L, \quad \text{e} \quad \gamma^2 = \frac{c_1^2}{4c_2^2} - \frac{c_0}{c_2} \in K$$

In particolare, detto $\alpha := \frac{c_1^2}{4c_1^2} - \frac{c_0}{c_2} \in K$, $L = K(\sqrt{\alpha})$.

Fatto $K(\sqrt{u}) = K(\sqrt{v}) \iff u \cdot v$ è un $\square$ in K

(cioè $x^2 - uv = 0$ ha soluzione in K)

CAMPI

Titolo nota

$X^3 - 4$ irriducibile

$$\alpha = \sqrt[3]{4} = (\sqrt[3]{2})^2$$

$$\mathbb{Q}(\alpha) = \mathbb{Q}(1/\alpha)$$

$\subseteq$ $\alpha \in \mathbb{Q}(1/\alpha)$, perché $\mathbb{Q}(1/\alpha)$ è campo e contiene $\frac{1}{\alpha}$, quindi contiene $(1/\alpha)^{-1} = \alpha$

$\Rightarrow \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(1/\alpha)$

$\supseteq$ Simmetricamente, perché $1/\alpha \in \mathbb{Q}(\alpha)$

$$\mathbb{Q}(\alpha) = \mathbb{Q}(1/\alpha) = \mathbb{Q}(2/\alpha) = \mathbb{Q}(\sqrt[3]{2})$$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$ = grado pol. min. di $\sqrt[3]{2}$

= grado $(x^3 - 2)$, che si annulla in $\sqrt[3]{2}$

e è irrid. per Eisenstein.

Est. quadratiche

K = campo di car $\neq 2$, $\alpha, \beta \in K^\times$

$K(\sqrt{\alpha}) = K(\sqrt{\beta})$ $\iff$ $\alpha \cdot \beta \in K^{\times 2} = \{t^2 \mid t \in K^\times\}$

$\iff$ l'eqz $t^2 - \alpha\beta$ ha una radice in K

$\alpha\beta = \beta^2 \cdot (\alpha/\beta)$ $\iff$ $\alpha/\beta \in K^{\times 2}$

$\Leftarrow$ Se $\alpha\beta = t^2$ con $t \in K^\times$, allora

$$K(\sqrt{\beta}) = K\left(\sqrt{t^2/\alpha}\right) = K(t/\sqrt{\alpha}) = K(1/\sqrt{\alpha}) \overset{(1)}{=} K(\sqrt{\alpha})$$

$\Rightarrow$ In particolare $\sqrt{\beta} \in K(\sqrt{\alpha})$

Oss Se $\alpha \in K^{\times 2}$ allora $K(\sqrt{\alpha}) = K$ e l'uguagl.

$K(\sqrt{\beta}) = K(\sqrt{\alpha}) = K$ dice $\sqrt{\beta} \in K$, cioè

anche $\beta \in K^{\times 2}$ $\Rightarrow$ $\alpha\beta \in K^{\times 2}$

Supponiamo quindi $[K(\sqrt{\alpha}) : K] = 2$. Allora $1, \sqrt{\alpha}$

formano una base del K-sp. vett. $K(\sqrt{\alpha})$

Lineare indip: $x \cdot 1 + y \cdot \sqrt{\alpha} = 0$ con $x, y \in K$

Se $y = 0 \Rightarrow x = 0$ ok

Se $y \neq 0 \Rightarrow \sqrt{\alpha} = -x/y \in K$, ma α non è un $\square$ in K, assurdo

In particolare: $K(\sqrt{\beta}) = K(\sqrt{\alpha}) \Rightarrow \sqrt{\beta} \in K(\sqrt{\alpha})$

$\Rightarrow \exists\, x, y \in K$ t.c. $\sqrt{\beta} = x + y\sqrt{\alpha}$

$$\Downarrow$$

$$\beta = x^2 + 2xy\sqrt{\alpha} + \alpha y^2$$

$$\Leftrightarrow \quad \underbrace{(x^2+\alpha y^2-\beta)}_{\in K}\cdot 1 + \underbrace{(2xy)}_{\in K}\cdot\sqrt{\alpha} = 0$$

Per lin. indip $\Rightarrow$
$$\begin{cases} x^2+\alpha y^2-\beta = 0 \\ 2xy = 0 \end{cases}$$
$2xy=0$:
- $2=0$ no char $K\neq 2$
- $x=0$
- $y=0$ no, vedi sotto

Se $y=0 \rightsquigarrow x^2=\beta$, cioè $\beta \in K^{\times 2}$

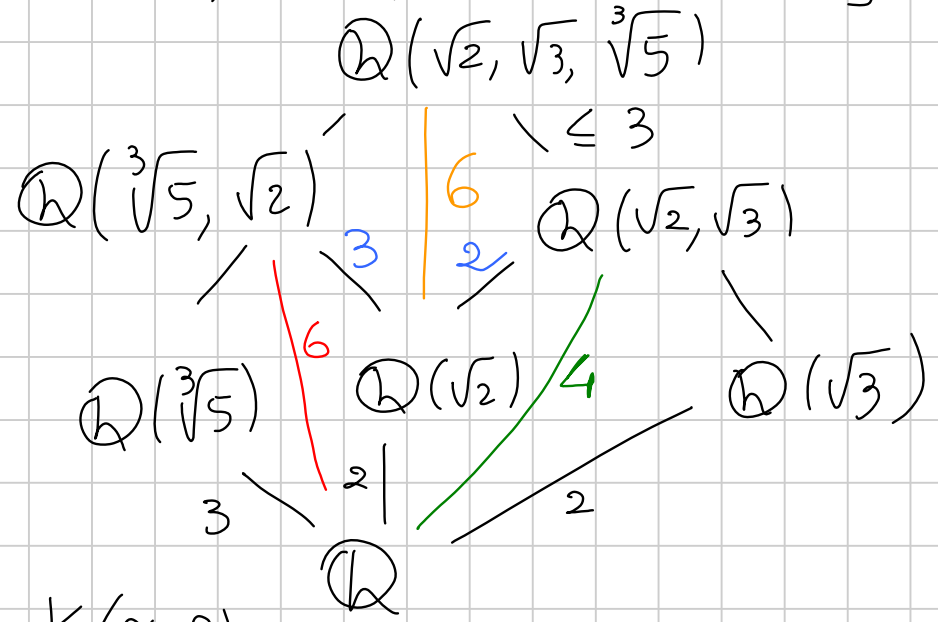
$K(\sqrt{\beta}) = K$ non è $= K(\sqrt{\alpha})$

(perché $[K(\sqrt{\alpha}):K] = 2$)

Se $x=0 \rightsquigarrow \beta = \alpha\cdot y^2 \rightsquigarrow \alpha\cdot\beta = (\alpha y)^2 \in K^{\times 2}$ □

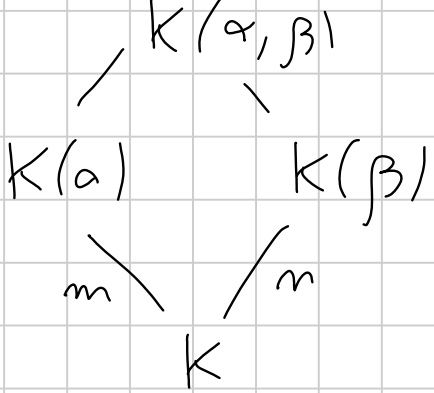
Esempio $\left[\mathbb{Q}\left(\sqrt[3]{5}, \sqrt{2}, \sqrt{3}\right) : \mathbb{Q}\right] \leq 12$ e $\equiv 0 \pmod{12}$,

quindi è 12



$x^3 - 5$
$x^2 - 2$
$x^2 - 3$
} irriducibili su $\mathbb{Q}$

Lemma



- $\left[K(\alpha, \beta) : K\right] \leq m \cdot n$
- Se $(m, n) = 1$, allora $\left[K(\alpha, \beta) : K\right] = mn$

Dim • $[K(\alpha,\beta):K] = \underbrace{[K(\alpha,\beta):K(\beta)]}_{\leq m} \cdot \underbrace{[K(\beta):K]}_{n} \leq mn$

$[K(\alpha,\beta):K(\beta)]$ = grado pol. min. $f(x)$ di α sul campo $K(\beta)$

Per ipotesi il pol. min. di α su K, chiamiamolo $g(x)$, ha grado m. In particolare $g(x) \in K(\beta)[x]$ è divisibile per il pol. $f(x)$

$$\Rightarrow \deg f(x) \leq \deg g(x) = m$$

$$\deg f(x) = [K(\alpha,\beta):K(\beta)]$$

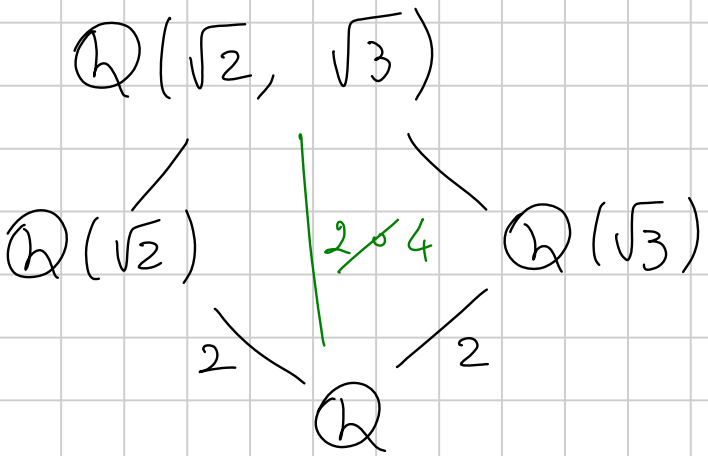
• $[K(\alpha,\beta):K] = n \cdot [K(\alpha,\beta):K(\beta)] \equiv 0 \pmod{n}$

$$[K(\alpha,\beta):K] = [K(\alpha,\beta):K(\alpha)] \cdot \underbrace{[K(\alpha):K]}_{m} \equiv 0 \pmod{m}$$

$$\Rightarrow \quad mn \mid [K(\alpha,\beta):K] \leq mn$$

$$\Rightarrow \quad [K(\alpha,\beta):K] = m \cdot n$$

Oss In generale $[K(\alpha,\beta):K] \equiv 0 \mod \operatorname{mcm}(m,n)$



Se $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 2$:

$$\Rightarrow \quad \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3})$$

$$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$$

spazi vett. su $\mathbb{Q}$ di dim 2

$\Downarrow$

$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$

Ma $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$, perché $2 \cdot 3 = 6 \notin \mathbb{Q}^{\times 2}$

Es.

$\alpha \in \mathbb{C}$ radice di $X^3 - X^2 - 2X - 1$, $\beta = \alpha^4 - 3\alpha^2$

i) Det. pol. min. di β

ii) Trovare $g(x) \in \mathbb{Q}[x]$ t.c. $\beta \cdot g(\alpha) = 1$

Oss Il campo $\mathbb{Q}(\alpha) \simeq \dfrac{\mathbb{Q}[x]}{(\text{pol. min } \alpha)}$ ha base $1, \alpha, \alpha^2, \ldots, \alpha^{\deg \text{pol min} - 1}$

$\beta \in \mathbb{Q}(\alpha)$ $\qquad 1/\beta = c_0 + c_1\alpha + c_2\alpha^2$

$g(x) = c_0 + c_1 x + c_2 x^2$

Oss β si deve poter scrivere come comb. lin. di $1, \alpha, \alpha^2$

Oss $f(x) = x^3 - x^2 - 2x - 1$ è il pol min di α (monico, si annulla in α, irriducibile (teo radici raz. o riduz. mod 2))

$0 = f(\alpha) = \alpha^3 - \alpha^2 - 2\alpha - 1 \qquad \alpha^3 = \alpha^2 + 2\alpha + 1$

$\alpha^4 = \alpha \cdot \alpha^3 = \alpha \cdot (\alpha^2 + 2\alpha + 1) = \alpha^3 + 2\alpha^2 + \alpha$

$= (\alpha^2 + 2\alpha + 1) + 2\alpha^2 + \alpha$

$= 3\alpha^2 + 3\alpha + 1$

$$\beta = \alpha^4 - 3\alpha^2 = 3\alpha + 1$$

$f(x) \rightsquigarrow f\left(\frac{x-1}{3}\right)$ è un polinomio che si annulla in β

$$g(x) = 27\left[\left(\frac{x-1}{3}\right)^3 - \left(\frac{x-1}{3}\right)^2 - 2\left(\frac{x-1}{3}\right) - 1\right]$$

$$= (x-1)^3 - 3(x-1)^2 - 18(x-1) - 27$$

$$= x^3 - 3x^2 + 3x - 1 - 3x^2 + 6x - 3 - 18x + 18 - 27$$

$$= x^3 - 6x^2 - 9x - 13$$

Per mostrare che $g(x)$ è pol. min. basta dim. che

$$[\mathbb{Q}(\beta):\mathbb{Q}] = 3$$

Siccome $\mathbb{Q}(\beta) = \mathbb{Q}(3\alpha+1) = \mathbb{Q}(3\alpha) = \mathbb{Q}(\alpha)$

vale $[\mathbb{Q}(\beta):\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = 3$, ok.

ii) $\beta \cdot h(\alpha) = 1$, ovvero: scrivere $1/\beta$ come pol. in α

Modo 1 $\quad 0 = g(\beta) = \beta^3 - 6\beta^2 - 9\beta - 13$

$$\beta \cdot (\beta^2 - 6\beta - 9) = 13$$

$$\Leftrightarrow \quad \frac{\beta^2 - 6\beta - 9}{13} = 1/\beta$$

$$1/\beta = \frac{1}{13}\left((3\alpha+1)^2 - 6(3\alpha+1) - 9\right)$$

$$= \frac{1}{13}\left(9\alpha^2 + 6\alpha + 1 - 18\alpha - 6 - 9 \right)$$

$$= \frac{1}{13}\left(9\alpha^2 - 12\alpha - 14 \right) \qquad h(x) = \frac{1}{13}\left(9x^2 - 12x - 14 \right)$$

Modo 2 $\qquad \beta = 3\alpha + 1 \qquad 1/\beta = c_0 + c_1\alpha + c_2\alpha^2$

$$1 = \underbrace{(3\alpha+1)}_{\beta}\underbrace{(c_0 + c_1\alpha + c_2\alpha^2)}_{1/\beta} = c_0 + c_1\alpha + c_2\alpha^2 +$$

$$+ 3c_0\alpha + 3c_1\alpha^2 + 3c_2\alpha^3$$

$$/\ (\alpha^2 + 2\alpha + 1)$$

$$= c_0 + 3c_2 +$$

$$(c_1 + 3c_0 + 6c_2)\alpha +$$

$$(c_2 + 3c_1 + 3c_2)\alpha^2$$

$$\begin{cases} C_0 + 3C_2 = 1 \\ C_1 + 3C_0 + 6C_2 = 0 \\ C_2 + 3C_1 + 3C_2 = 0 \end{cases} \Rightarrow \begin{array}{l} C_0 = -14/13 \\ C_1 = -12/13 \\ C_2 = 9/13 \end{array}$$

Modo 3 I polinomi $A(x) = 3X + 1$ e $B(x) = X^3 - X^2 - 2X - 1$ sono primi fra loro. L'identità di Bézout dice:

$$A(x) \cdot C(x) + B(x) \cdot D(x) = 1$$

Valutando in $X = \alpha$

$$\beta \cdot C(\alpha) + \underbrace{B(\alpha)}_{0} D(\alpha) = 1$$

Es. 193

$\alpha \in \mathbb{C}$ radice di $x^4 - 2x^3 + x - 1$ (irriducibile)

1) Trovare $g(x) \in \mathbb{Q}[x]$ t.c. $\alpha^2 g(\alpha) = 1$

2) Determinare, al variare di $k \in \mathbb{Z}$, il grado

$$[\mathbb{Q}(\alpha^2 + k\alpha) : \mathbb{Q}] \mid 4$$

2)

$$4 \left[\begin{array}{c} \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q}(\alpha^2 + k\alpha) \\ | \\ \mathbb{Q} \end{array} \right] \begin{array}{l} c \\ b \end{array}$$

$b \cdot c = 4$

$b = \cancel{1} \quad 0 \quad 2 \quad \sigma \quad 4$

$\alpha^4 - 2\alpha^3 + \alpha - 1 = 0$

Se $b=1$, cioè se $\alpha^2 + k\alpha = q \in \mathbb{Q}$, allora il pol. $x^2 + kx - q \in \mathbb{Q}[x]$ si annullerebbe in α, impossibile (il pol. min. di α ha grado 4)

$\alpha^2 + k\alpha$ ha grado 2 $\iff$ esistono $c_1, c_0 \in \mathbb{Q}$ t.c. $\alpha^2 + k\alpha$ sia radice di $x^2 + c_1 x + c_0 \in \mathbb{Q}[x]$

$$(\alpha^2 + k\alpha)^2 + c_1(\alpha^2 + k\alpha) + c_0 = 0$$

$$\boxed{\alpha^4} + 2k\alpha^3 + k^2\alpha^2 + c_1\alpha^2 + c_1 k\alpha + c_0 = 0$$

α radice di $f(x) = x^4 - 2x^3 + x - 1$

$$0 = f(\alpha) = \alpha^4 - 2\alpha^3 + \alpha - 1$$

$$\alpha^4 = 2\alpha^3 - \alpha + 1$$

$$(2K+2)\cdot\alpha^3 + (K^2 + C_1)\alpha^2 + (-1 + C_1 K)\alpha + (1 + C_0)\cdot 1 = 0$$

$$\begin{cases} 2K+2 = 0 & K = -1 \\ K^2 + C_1 = 0 & C_1 = -1 \\ -1 + C_1 K = 0 & \checkmark \\ 1 + C_0 = 0 & C_0 = -1 \end{cases}$$

Quindi: per $K \neq -1$ $\left[\textcircled{2}(\alpha^2 + K\alpha) : \textcircled{2} \right] = 4$

$K = -1$ $\alpha^2 - \alpha$ è una radice di

$$X^2 - X - 1$$

$$\Rightarrow \left[\mathbb{Q}(\alpha^2+k\alpha):\mathbb{Q}\right]=2$$

Campo di spezzamento di $(x^3-2)(x^4-3)$

Su $\mathbb{Q}$, $\mathbb{F}_3$, $\mathbb{F}_{11}$

Nel caso dei campi finiti ricordiamo che il campo di sp. di $f(x)\in \mathbb{F}_{p^n}[x]$ è $\mathbb{F}_{p^{nk}}$ e $k=$ m.c.m. dei gradi dei fattori irriid. di f.

- $\mathbb{F}_3$: il c.d.s. è $\mathbb{F}_{3^k}$ con $k=$ mcm gradi dei fattori irriid. di $(x^3-2)(x^4-3)\in\mathbb{F}_3[x]$

  $\Rightarrow$ è $\mathbb{F}_3$

  $\|$

  $(x-2)^3\cdot x^4$

• $\mathbb{F}_{11}$: è $\mathbb{F}_{11^k}$

$f(x) = (x^3 - 2)\cdot(x^4 - 3)$ in $\mathbb{F}_{11}[x]$

$x = -4$

$x^3 \equiv 2 \quad (11)$ ha 1 e 1 sola soluzione

$3 \nmid p-1$

$\Rightarrow \quad x^3 - 2 = (\deg 1)\cdot(\deg 2)$ irriid.

$(x^3 - 2,\ 3x^2) = (1)$

$x^3 - 2 = (x+4)(\ \ldots\ )$

E $x^4 - 3$? $\quad x^2 = t$ $\quad t^2 - 3 = (t-5)(t+5)$ in $\mathbb{F}_{11^2}$

$x^4 \overset{11}{-} 25 = (x^2 - 5)(x^2 + 5)$

$= (x-4)(x+4)(x^2+5)$

$$\left(\frac{-5}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{5}{11}\right) = \left(\frac{-1}{11}\right)\cdot 1 = -1\cdot 1$$

$\Rightarrow$ -5 non è $\square$ mod 11

Il mcm gradi è 2 $\Rightarrow$ c.d.s. $\simeq \mathbb{F}_{11^2}$.

- $\mathbb{Q}$: il cds è $\mathbb{Q}\left(\sqrt[3]{2},\ \sqrt[3]{2}\cdot\zeta_3,\ \sqrt[3]{2}\cdot\zeta_3^2,\ \pm\sqrt[4]{3},\ \pm\sqrt[4]{3}\cdot i\right)$

$= \mathbb{Q}\left(\sqrt[3]{2},\ \zeta_3,\ \sqrt[4]{3},\ i\right)$

$= \mathbb{Q}\left(\sqrt[3]{2},\ i\sqrt{3},\ \sqrt[4]{3},\ i\right)$

$= \mathbb{Q}\left(\sqrt[3]{2},\ \sqrt[4]{3},\ i\right)$

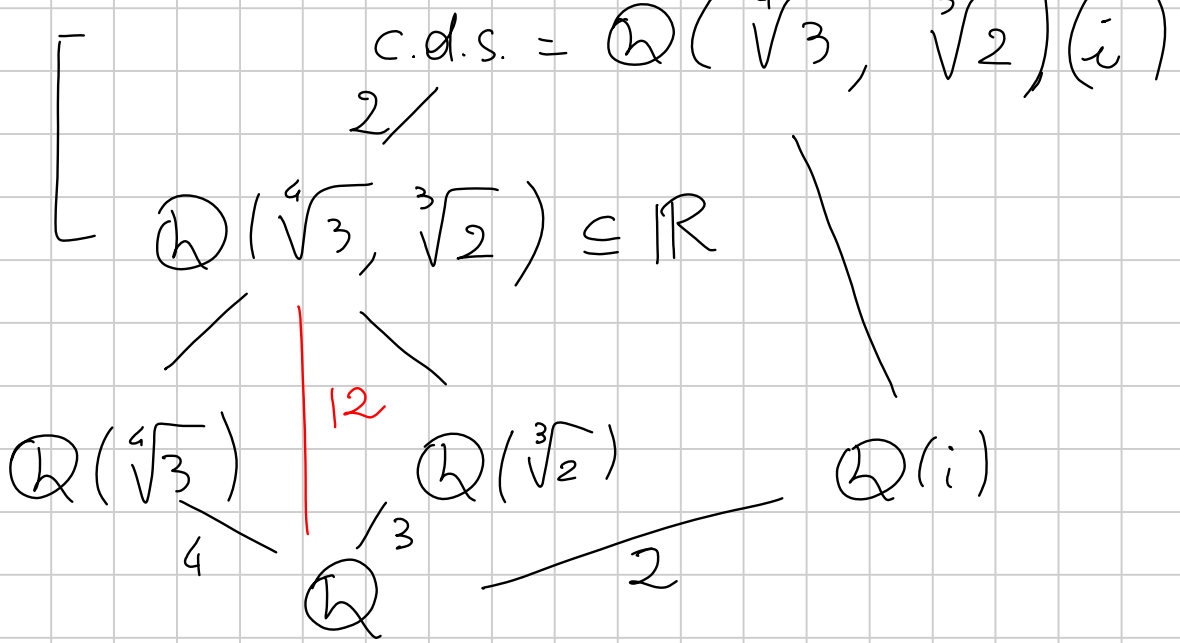
$i\sqrt{3} = i\cdot\left(\sqrt[4]{3}\right)^2$

$$x^3 - 1 = 0$$

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

$$\frac{-1 \pm i\sqrt{3}}{2}$$

Usando x^2+1 vedo che il grado è ≤ 2



Grado c.d.s. $= 24 = [\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{2}, i) : \mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{2})]$

$\times [\mathbb{Q}(\sqrt[4]{3}, \sqrt[3]{2}) : \mathbb{Q}]$

CAMPI (FINITI)

Titolo nota

Es 204 modificato

$\alpha = \sqrt{5 - \sqrt{24}} \in \mathbb{R}$: pol. min. e suo campo di spezz.

$\alpha^2 = 5 - \sqrt{24} \iff \sqrt{24} = 5 - \alpha^2 \implies 24 = \alpha^4 - 10\alpha^2 + 25$

$\alpha^4 - 10\alpha^2 + 1 = 0$

Candidato pol. min.: $p(t) = t^4 - 10t^2 + 1$

- Δ :
- Mod 5 : $t^4 + 1 \in \mathbb{F}_5[t]$ $\quad t^4 - 4 = (t^2 - 2)(t^2 + 2)$
- Mod 2 : $p(t) \equiv t^4 + 1 \equiv (t^2)^2 + 1 \equiv (t^2 + 1)^2$

$\equiv (t+1)^4 \pmod 2$

$x^2 - 10x + 1 = 0 \qquad 5 \pm \sqrt{24} \qquad (x = t^2)$

$t = \pm \sqrt{5 \pm \sqrt{24}} \quad \in \mathbb{R}$

$$p(t) = \left(t - \sqrt{5+\sqrt{24}}\right)\left(t + \sqrt{5+\sqrt{24}}\right)\left(t - \sqrt{5-\sqrt{24}}\right)\left(t + \sqrt{5-\sqrt{24}}\right)$$

Proviamo i 3 modi di accoppiare i fattori troviamo

- $t^2 - (5+\sqrt{24})$ che non è in $\mathbb{Q}[x]$
- $t^2 - t\left(\underbrace{\sqrt{5+\sqrt{24}} + \sqrt{5-\sqrt{24}}}\right) + 1$

  ↓ elevo al quadrato: $(5+\sqrt{24}) + (5-\sqrt{24}) + 2 = 12$

  $\sqrt{12} \notin \mathbb{Q}$

$$\cdot \quad t^2 - \underbrace{\left(\sqrt{5+\sqrt{24}} - \sqrt{5-\sqrt{24}} \right)} t - 1$$

al quadrato: $5+\sqrt{24} + 5 - \sqrt{24} - 2 = 8$

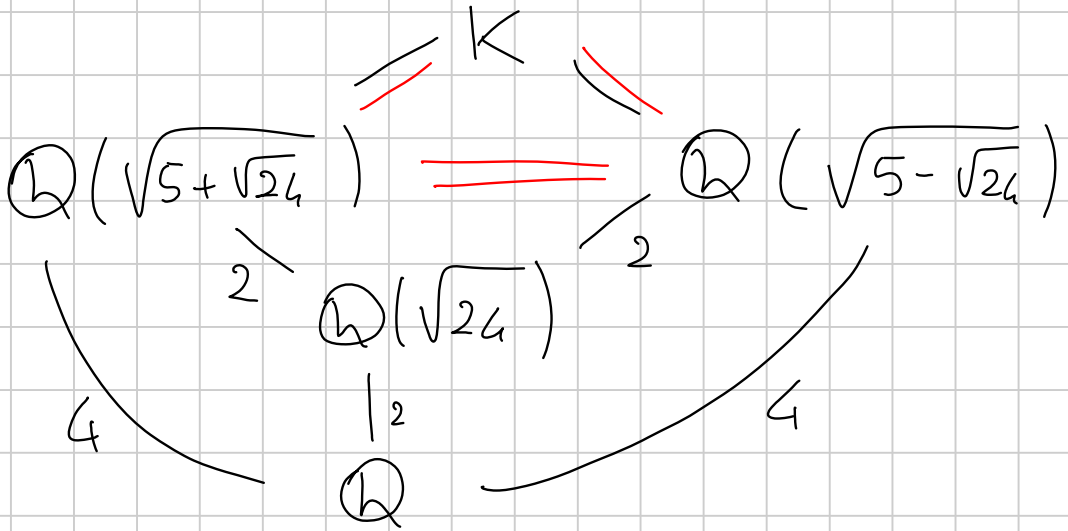
Quindi: il pol. min. è $p(x)$. Il campo è

$$\mathbb{Q}\left(\pm\sqrt{5+\sqrt{24}}, \pm\sqrt{5-\sqrt{24}} \right) = K$$

$$\left.\begin{array}{l} K = L\left(\sqrt{5+\sqrt{24}}\right) \\ \Big| \\ \mathbb{Q}\left(\sqrt{5-\sqrt{24}}\right) = L \\ \Big| \\ \mathbb{Q} \end{array}\right\} \leq 2$$

$$4 \left[\right.$$

Oss $\sqrt{24} \in L$: $-\left[\left(\sqrt{5-\sqrt{24}}\right)^2 - 5\right] = \sqrt{24}$



Ci basta capire se le due est.

$\mathbb{Q}(\sqrt{5+\sqrt{24}})/\mathbb{Q}(\sqrt{24})$ e $\mathbb{Q}(\sqrt{5-\sqrt{24}})/\mathbb{Q}(\sqrt{24})$

siano uguali $\Leftrightarrow$ $(5+\sqrt{24})\cdot(5-\sqrt{24}) = \square$

$1 = \square$ sì

Abbiamo dim che $K = \mathbb{Q}(\sqrt{5+\sqrt{24}})$, quindi $[K:\mathbb{Q}] = 4$

$$\frac{1}{\sqrt{5+\sqrt{24}}} = \sqrt{5-\sqrt{24}}$$

$$K = \mathbb{Q}(\pm\alpha, \pm 1/\alpha) = \mathbb{Q}(\alpha)$$

Es 192

$f(x) = x^6 + 1$. Per quali primi p ha radice mod p?

- $p = 2$: sì, $x = 1$

$$x^6 + 1 = \frac{x^{12}-1}{x^6-1} = (x^2)^3 + 1^3 = (x^2+1)(x^4 - x^2 + 1)$$

- $p = 3$: $f(x) \equiv (x^2+1)^3 \pmod 3$ $\qquad x^2 \equiv -1 \pmod 3$

non ha radici

- Se $x^6+1 \equiv 0 \ (p) \Rightarrow (x^3)^2 \equiv -1 \ (p)$

$\Rightarrow \left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \ (4)$

Cioè: se $p \equiv 3 \ (4)$, $f(x)$ non ha radici mod p

- Se $p \equiv 1 \ (4)$: $\exists \ a \in \mathbb{Z}/p\mathbb{Z}$ t.c. $a^2 \equiv -1 \pmod p$,

e questo a è una radice:

$$f(a) \equiv (a^2+1)(a^4-a^2+1) \equiv 0 \ (p)$$

Es 229 p dispari (primo), $f(x) = x^6 + ax^3 + b \in \mathbb{F}_p[x]$

1. Dim che il c.d.s. di $f(x)$ su $\mathbb{F}_{p^2}$ ha grado 1 o 3

2. Dim che il grado del c.d.s. su $\mathbb{F}_p$ NON ha grado 4 o 5

3. Se $p \equiv 2 \pmod 3$, il c.d.s. su $\mathbb{F}_p$ non ha grado 3

— o —

$t = x^3$, tento di fattorizzare $t^2 + at + b = (t - t_1)(t - t_2)$

Sia $\Delta = a^2 - 4b$.

* Se Δ è un quadr in $\mathbb{F}_p$: $t^2 + at + b = (t - t_1)(t - t_2)$ in $\mathbb{F}_p[x]$

* Altrimenti $\mathbb{F}_p(\sqrt{\Delta}) = \mathbb{F}_{p^2}$, e quindi in $\mathbb{F}_{p^2}$ il disc. è un $\square$ e $t^2 + at + b = (t - t_1)(t - t_2) \in \mathbb{F}_{p^2}[x]$

$$x^6 + ax^3 + b = (x^3 - t_1)(x^3 - t_2)$$

Come si fattorizza $x^3 - t_i$ in $\mathbb{F}_{p^2}[x]$?

- se non ha radici è irriid. (grado 3)
- se ha almeno una radice, chiamiamola α_1, le altre radici sono $\alpha_2 = \alpha_1 \cdot \zeta_3$ e $\alpha_3 = \alpha_1 \cdot \zeta_3^2$, dove ζ_3 è una soluzione di $x^3 - 1 = 0$ diversa da $x = 1$,

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

di grado 2 $\Rightarrow \zeta_3, \zeta_3^2 \in \mathbb{F}_{p^2}$

cioè è una radice di $x^2 + x + 1 = 0$

$$\left(\alpha_2^3 = \alpha_1^3 \cdot \zeta_3^3 = t_i \cdot 1, \quad \alpha_3^3 = t_i \right)$$

$$x^3 - t_i = (x - \alpha_1)(x - \alpha_1 \zeta_3)(x - \alpha_1 \zeta_3^2) \quad \text{in } \mathbb{F}_{p^2}[x]$$

Oss Se $p=3$: $x^3-1=0$ $\qquad (x-1)^3=0$

$$f(x) = x^6 + ax^3 + b \equiv (x^2+ax+b)^3$$
$$\equiv x^6 + a^3x^3 + b^3$$
$$\equiv x^6 + ax^3 + b \qquad (3)$$

Su $\mathbb{F}_q$ ho quindi $f(x) = (x-t_1)^3(x-t_2)^3$ e il suo cds sarà $\mathbb{F}_q$ stesso

$f(x)$ si fattorizza in $\mathbb{F}_{p^2}[x]$ con fattori irriducibili di gradi 1 o 3. Il mcm (gradi dei fatt. irriducibili) $=: h \in \{1,3\}$ e sappiamo dalla teoria che

$$[\text{c.d.s.} : \mathbb{F}_{p^2}] = h \in \{1,3\}$$

③ $p \equiv 2 \ (3) \rightsquigarrow$ il grado del c.d.s. F di $f(x)$ su $\mathbb{F}_p$ non può essere 3

$$F = \mathbb{F}_p\left(\alpha_1, a, \zeta_3, a\zeta_3^2; \ \beta_1, \beta, \zeta_3; \beta_1\zeta_3^2\right)$$

$$= \mathbb{F}_p\left(\alpha_1, \beta_1, \zeta_3\right)$$

sto supponendo $\alpha_1 \neq 0$ o $\beta_1 \neq 0$. In caso contrario $f(x) = x^6$ e il c.d.s. è $\mathbb{F}_p$

Oss Se $\zeta_3 \notin \mathbb{F}_p$, allora $\mathbb{F}_p(\zeta_3) = \mathbb{F}_{p^2}$

Questo contraddice $[F : \mathbb{F}_p] = 3$ per la moltiplicat. nelle torri.

$$2\left\{\begin{array}{c} F \\ | \\ \mathbb{F}_p(\zeta_3) \\ | \\ \mathbb{F}_p \end{array}\right\}3$$

Ora: $p \equiv 2\ (3) \Rightarrow p-1 \equiv 1\ (3)$

$\Rightarrow x^3 \equiv 1\ (p)$ ha solo una soluz., che è $x = 1 \Rightarrow \zeta_3, \zeta_3^2 \notin \mathbb{F}_p$.

Oss $\zeta_3 \in \mathbb{F}_p \Rightarrow \zeta_3 \in \mathbb{F}_p^\times$ e avrebbe ordine 3

$\Rightarrow 3 \mid \#\mathbb{F}_p^\times = p-1 \Rightarrow p \equiv 1\ (3)$, assurdo

Oss Vale il viceversa: $p \equiv 1\ (3) \Rightarrow$ l'eqz. $x^3 \equiv 1\ (p)$ ha 3 soluz. mod $p \Rightarrow \zeta_3 \in \mathbb{F}_p$

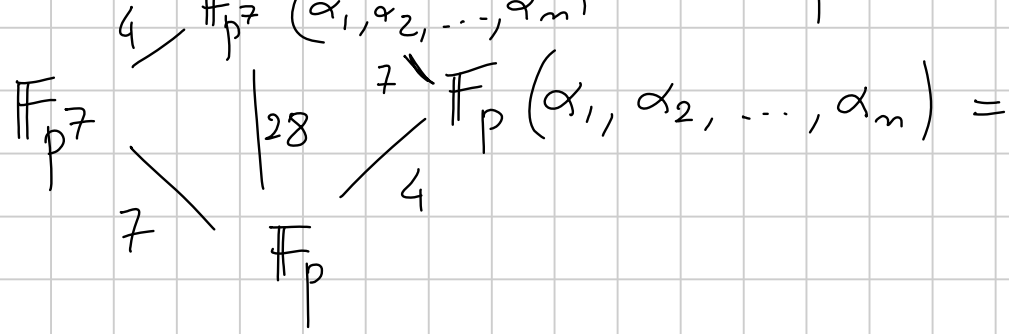
② Vogliamo escludere $[F : \mathbb{F}_p] = 4$ o 5

$$4\left[\begin{array}{c} F = \mathbb{F}_{p^4} \\ / \\ \mathbb{F}_{p^2} \\ / \\ \mathbb{F}_p \end{array}\right]\begin{array}{l} 2 \\ \\ 2 \end{array}$$

$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n} \iff m \mid n$

Se $[F : \mathbb{F}_p] = 4$, allora $[F : \mathbb{F}_{p^2}] = 2$, ma questo contraddice il pto 1: F è anche il c.d.s. di $f(x)$ su $\mathbb{F}_{p^2}$, e avevamo detto che allora $[F : \mathbb{F}_{p^2}] \in \{1, 3\}$

Oss Sia $g(x) \in \mathbb{F}_p[x]$ il cui c.d.s. sia $\mathbb{F}_{p^4}$. Chi è il c.d.s. di $g(x)$ su $\mathbb{F}_{p^7}$? $\mathbb{F}_{p^{28}}$



$[F : \mathbb{F}_p] = 5 = \text{mcm}$ (gradi fattori irrid di $f(x) \in \mathbb{F}_p[x]$)

$\Rightarrow$ $f(x) = f_5(x) \cdot f_1(x)$ con $f_i(x)$ irrid. di grado i

Allora: $f(x)$ ha una radice x_1

$\Rightarrow$ $t^2 + at + b$ ha una radice x_1^3, e una seconda radice t_2

$\Rightarrow$ $(t^2 + at + b) = (t - x_1^3)(t - t_2)$

$\Rightarrow$ $x^6 + ax^3 + b = (x^3 - x_1^3)(x^3 - t_2)$

non ha fattori irrid. di grado 5

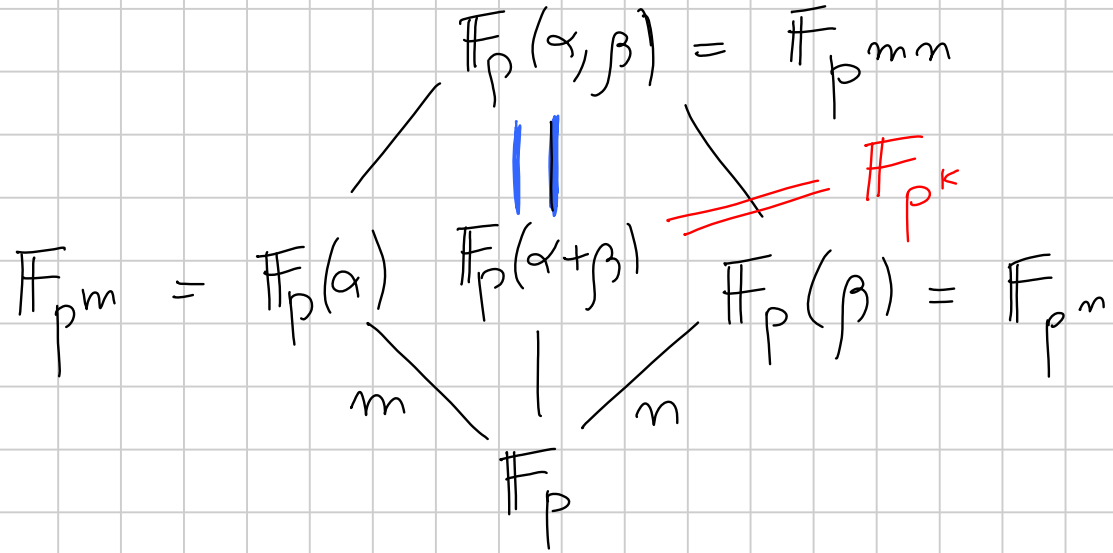
$\mathbb{F}_p(\alpha+\beta)$

Siano $\alpha, \beta \in \overline{\mathbb{F}_p}$ e $\left[\mathbb{F}_p(\alpha) : \mathbb{F}_p\right] = m$

$\left[\mathbb{F}_p(\beta) : \mathbb{F}_p\right] = n$

Supponiamo $(m, n) = 1$. Allora $\mathbb{F}_p(\alpha+\beta) = \mathbb{F}_p(\alpha, \beta)$

o equivalentemente $\left[\mathbb{F}_p(\alpha+\beta) : \mathbb{F}_p\right] = m \cdot n$



Oss ① Chiamiamo $\gamma := \alpha + \beta$. Si ha $\gamma \in \mathbb{F}_p(\alpha, \beta)$

② Lemma di ieri: $[\mathbb{F}_p(\alpha, \beta) : \mathbb{F}_p] = m \cdot n$

③ $\mathbb{F}_p(\alpha, \gamma) = \mathbb{F}_p(\alpha, \alpha+\beta) = \mathbb{F}_p(\alpha, \beta)$

$$[\mathbb{F}_p(\alpha, \gamma) : \mathbb{F}_p] = [\mathbb{F}_p(\alpha, \beta) : \mathbb{F}_p] = mn$$

$\mathbb{F}_p(\alpha, \gamma)$ = Composto di $\mathbb{F}_{p^m}$ e $\mathbb{F}_{p^k}$ = $\mathbb{F}_{p^{mcm(m,k)}}$

$mcm(m, k)$

$n \mid mcm(m, k)$
$(n, m) = 1$
$\Rightarrow n \mid k$

④ Stesso ragion. con $\mathbb{F}_p(\beta, \gamma) \Rightarrow m \mid k$

⑤ Quindi $mcm(m, n) \mid k \Rightarrow mn \mid k \Rightarrow k = mn$.

Radici comuni (189)

$f(x) = x^3 + 3x - 1, \qquad g(x) = x^2 - 2$

Per quali primi p esiste $a \in \mathbb{F}_p$ t.c. $f(a) = g(a) = 0$?

$$\begin{cases} a^3 + 3a - 1 = 0 \\ a^2 = 2 \end{cases} \qquad \begin{cases} 0 = a \cdot a^2 + 3a - 1 = 5a - 1 \\ a^2 = 2 \end{cases}$$

Se $p = 5$ assurdo; altrimenti $a \equiv 1/5 \pmod p$

e quindi $2 \equiv a^2 \equiv \left(\frac{1}{25}\right) \mod p$

$$\Rightarrow \quad 2 \cdot 25 \equiv 1 \ (p) \quad \Rightarrow \quad 49 \equiv 0 \ (p) \Rightarrow p = 7$$

$x^2 - 2 \equiv 0 \ (7) \Rightarrow x \equiv \pm 3 \ (7)$ è $f(3) \equiv 0 \ (7)$

Quindi $p = 7$ funziona, ed è l'unico.

Oss $(f(x), g(x)) = 1$ in $\mathbb{Q}[x]$

$\Rightarrow \exists \ A(x), B(x) \in \mathbb{Q}[x]$ t.c.

$$f(x) A(x) + g(x) B(x) = 1$$

Sia N un denom. comune fra $A(x)$, $B(x)$

$$\Rightarrow f(x) \cdot (N A(x)) + g(x) \cdot (N B(x)) = N$$

Riducendo mod p: $\overline{f(x)} \cdot (\overline{N A(x)}) + \overline{g(x)} \cdot \overline{N B(x)} = \overline{N} \ (p)$

Se $p \nmid N$: ho mostrato che $(\bar{f}(x), \bar{g}(x)) = (N) = (1)$

$\Rightarrow$ $\bar{f}(x)$, $\bar{g}(x)$ non hanno radici in comune

X^4+1

$$X^4+1 = \boxed{(X^2+i)(x^2-i)} =$$

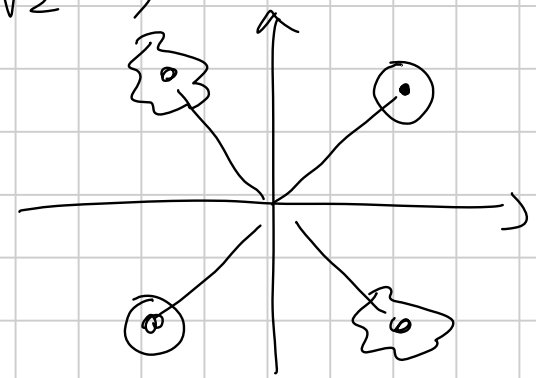
$$= \left(x - \frac{1+i}{\sqrt{2}}\right)\left(x - \frac{1-i}{\sqrt{2}}\right)\left(x - \frac{-1+i}{\sqrt{2}}\right)\left(x - \frac{-1-i}{\sqrt{2}}\right)$$

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

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

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

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



Oss Se $\mathbb{F}_p$ contiene o un elem. α t.c. $\alpha^2 \equiv -1 \ (p)$

β t.c. $\beta^2 \equiv 2 \ (p)$

γ t.c. $\gamma^2 \equiv -2 \ (p)$

allora x^4+1 è RIDUCIBILE in $\mathbb{F}_p$

Ovvero: vorrei che almeno uno fra $\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{-2}{p}\right)$

fosse $= +1$, ma non possono essere tutti -1 per moltiplicatività.

$\sqrt{24}$ $\sqrt{8}$ $\sqrt{12}$

$$\left(\frac{24}{p}\right) = \left(\frac{4}{p}\right)\cdot\left(\frac{6}{p}\right) = \left(\frac{2^2}{p}\right)\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)^2\left(\frac{6}{p}\right) = \left(\frac{6}{p}\right)$$

$$x^4 + 3x^2 + x + 1 = (x^2 + bx \pm 1)(x^2 + ex \pm 1)$$

$f(x) \in \mathbb{Z}[x]$ $\quad f(x) = g(x)\,h(x)$ in $\mathbb{Z}[x]$

$\overline{f(x)} = \overline{g(x)}\cdot\overline{h(x)}$ $\quad \downarrow$ $\quad \mathbb{Z}/p\mathbb{Z}[x]$

$$G = (\mathbb{Z}/35\mathbb{Z})^\times \cong (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

i) $\forall n$ det. il n° degli elem. di ord n di G

ii) det. il n° di sgp di G di ord 6

$$\begin{bmatrix} G & \longrightarrow & \mathbb{Z}/4\mathbb{Z} \\ (x,y) & \longmapsto & y \\ (x,y) & \longmapsto & -y \end{bmatrix}$$

i) $n \mid \#G = 24$

$n = 1, 2, 3, 4, 6, \cancel{8}, 12, 24$ (4)

1 | 1 | 2 | 0

$(4a, 4b) = (0,0)$

$\begin{cases} 4a \equiv 0 \ (6) \\ 4b \equiv 0 \ (4) \end{cases}$ $a \equiv 0 \ (3)$

$(2a, 2b) = (0,0)$

$\begin{cases} 2a \equiv 0 \ (6) \\ 2b \equiv 0 \ (4) \end{cases}$

$\begin{cases} a \equiv 0 \ (3) \\ b \equiv 0 \ (2) \end{cases}$ 2 2

$$2 \cdot 4 - 3 - 1 = 4$$

ii) $|H| = 6 \Rightarrow H \simeq \mathbb{Z}/6\mathbb{Z}$ o ~~$H \simeq S_3$~~

sgp. di ord 6 = # sgp. ciclici di ord 6

$$= \frac{\#\{\text{elt. ord } 6\}}{\varphi(6)}$$

$\varphi(6)$: n° di elem. di ord 6 in un sgp $\simeq \mathbb{Z}/6\mathbb{Z}$

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm K\}$$

$$i \cdot j = K \qquad j \cdot i = -K \qquad j \cdot K = i, \quad K \cdot i = j$$

$$i^2 = j^2 = k^2 = -1$$

$$\{i, -1, -i, 1\} = \langle i \rangle$$

$$\{j, -1, -j, 1\} = \langle j \rangle$$

165) G grp, $H \triangleleft G$ $|H| = n$, $(m, n) = 1$

Dim che G/H ha elem. ord m $\Leftrightarrow$ G li ha

$\Rightarrow$ Sia $x \in G/H$ di ord m e sia $\pi : G \to G/H$ la proiez. can. Allora $\exists\, y \in G$ t.c. $\pi(y) = x$,

$m = \text{ord}(\pi(y)) \mid \text{ord}(y)$

$\text{ord}(y) = km$, $\text{ord}(y^k) = m$

$\Leftarrow$ Sia $x \in G$ di ordine m. È vero che $\pi(x)$ ha ord m?

Se $\text{ord}(\pi(x)) = k < m$, allora $x^k \in H$

$\Rightarrow \text{ord}(x^k) \mid \#H$

↳ divide m

$\Rightarrow \text{ord}(x^k) = 1$

$\Rightarrow \boxed{x^k = 1}$

$\pi(x)^k = e \rightsquigarrow x^k H = H \iff x^k \in H$

$(x^k)^m = (x^m)^k = e^k = e$

$m = \text{ord}(x) \mid k < m$

G gruppo, $f: G \longrightarrow \mathbb{Z}/12\mathbb{Z}$

$g: G \longrightarrow \mathbb{Z}/12\mathbb{Z}$

i) $K = \{x \in G \mid f(x) = g(x)\}$ è $\trianglelefteq G$

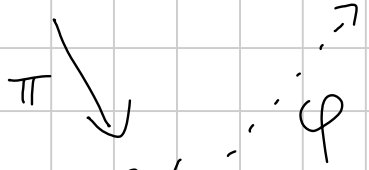
ii) Se $G \cong S_3 \times \mathbb{Z}/2\mathbb{Z}$ e $H = \langle ((1,2,3), \bar{0}) \rangle$, descrivere tutti gli hom $\varphi: G \longrightarrow \mathbb{Z}/12\mathbb{Z}$ t.c. $\varphi(h) = 0 \ \forall h \in H$.

i) $\lambda: G \longrightarrow \mathbb{Z}/12\mathbb{Z}$ è omom, $K = \ker \lambda$

$x \longmapsto f(x) - g(x)$

$x K x^{-1} = K \quad \forall x \in G$

ii) $f: G \longrightarrow G'$, $H \triangleleft G$ contenuto in $\ker f$



$f = \varphi \circ \pi$

Il nostro H è normale: $H = \{((1,2,3), 0); ((3,2,1), 0), (id, 0)\}$

$$G = S_3 \times \mathbb{Z}/2\mathbb{Z} \xrightarrow{\Psi} S_3/N \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$(x, y) \longmapsto (xN, y)$$

$N = \langle (1,2,3) \rangle$

$$\ker \Psi = \{(\sigma, 0) \mid \sigma \in N\} = H$$

Oss $N_1 \trianglelefteq G_1, \quad N_2 \trianglelefteq G_2 \Rightarrow N_1 \times N_2 \trianglelefteq G_1 \times G_2$

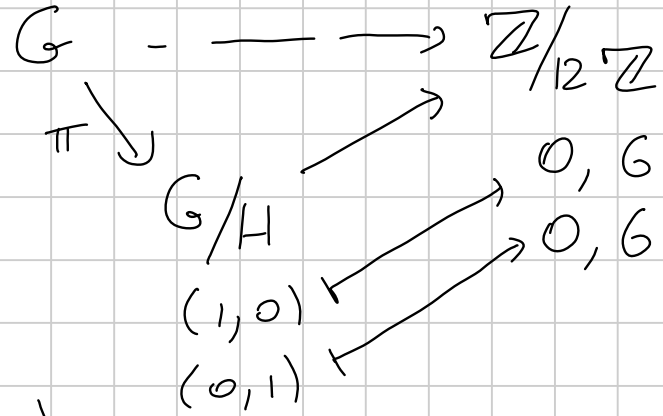
$$G_1 \times G_2 \longrightarrow G_1/N_1 \times G_2/N_2$$
$$(x, y) \longmapsto (xN_1, yN_2)$$

Gli $\{ f : G \longrightarrow \mathbb{Z}/12\mathbb{Z} \mid \ker f \supseteq H \}$ sono in bigez.

Con $\{ f : G/H \to \mathbb{Z}/12\mathbb{Z} \} \longleftrightarrow \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/12\mathbb{Z})$

$$\underbrace{\mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/12)}_{2} \times \underbrace{\mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/12)}_{2}$$

4 elementi



1) $\{$ banale

2) $(1,0) \mapsto 0$
$(0,1) \mapsto 6$
$(\sigma, y) \mapsto 6y$

$S_3 \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$
$(x, y) \longmapsto 6y$

3) (σ, y)

$S_3 \times \mathbb{Z}/2\mathbb{Z}$ → 0 se $\sigma \in \langle(1,2,3)\rangle$, 6 altrimenti

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$
$(x, y) \longmapsto 6x$

4) (σ, y)

$S_3 \times \mathbb{Z}/2\mathbb{Z}$ → $0 \circ 6$

π

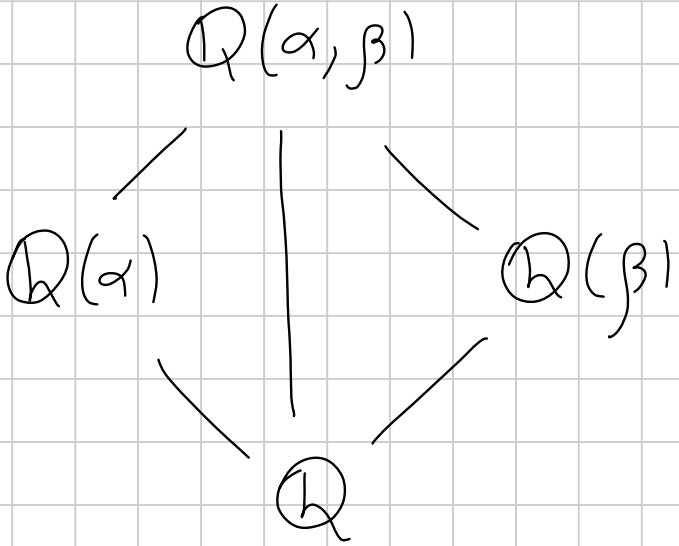
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/12\mathbb{Z}$
$(x, y) \longmapsto 6x + 6y$

$$f(\sigma, y) = \begin{cases} 0 & \text{se } \sigma \in \langle (1,2,3) \rangle \text{ e } y = 0 \quad \text{oppure} \\ & \sigma \notin \langle (1,2,3) \rangle \text{ e } y = 1 \\ 6 & \text{altrimenti} \end{cases}$$

$$\varphi((x,y)) = \begin{cases} 0 \\ 6x \\ 6y \\ 6(x+y) \end{cases}$$

$$|G/H| = |G| / |H| \overset{=25}{}$$

$$|H| \cdot |G/H| = |G|$$



$$[\mathbb{Q}(\alpha,\beta):\mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\beta):\mathbb{Q}]$$