EQUAZIONI CONGRUENZIALI

$ax \equiv_m b$ ⟶ Ha soluzione se $d := MCD(a,m) \mid b$

Per arrivare a $x \equiv_m c$, bisogna trovare l'INVERSO MOLTIPLICATIVO di a e moltiplicarlo da tutte e due le parti.

$\exists$ se $MCD(a,m) = 1$

Se $\exists$, o lo "vedi a occhio", oppure cerca un'identità di Bézout di 1.

□

SISTEMI DI EQUAZIONI CONGRUENZIALI

$$(*) = \begin{cases} x_1 \equiv a_1 \pmod{m_1} \\ x_2 \equiv a_2 \pmod{m_2} \\ \dots \\ x_m \equiv a_m \pmod{m_m} \end{cases}$$

SOSTITUZIONI SUCCESSIVE

1- Da $(*)$ scrivi la "prima" equazione del tipo $x_1 \equiv_{m_1} a_1$ come $x_1 = a_1 + m_1 \cdot h$ $\quad h \in \mathbb{Z}$

2- Sostituisci l'espressione di x nelle eq. "sottostanti"

3- Arriverai a qualcosa del tipo $\begin{cases} x = a_1 + m_1 \cdot h \\ h \equiv_{m_2} c \\ h \equiv_{m_3} d \\ \vdots \\ h \equiv_{m_m} a \end{cases}$

4- Ripeti 1, 2, fino alla penultima eq.

5- Trova la soluz. dell'ultima eq. e scrivila come 1.

6- Sostituisci il risultato trovato nell'equazione immediatamente "sopra" e così via

7- Ricava valore di x

□

TEOREMA CINESE DEL RESTO

Se (m_i, m_j) sono coprimi $\forall i \neq j$, il sistema ammette un'unica soluzione modulo $m_1 \cdot m_2 \cdot \dots \cdot m_m$.

0- Controllo se $MCD(m_i, m_j) = 1 \quad \forall i \neq j$

1- Denoto $N = m_1 \cdot m_2 \cdot \dots \cdot m_m$

2- Denoto $N_k = \frac{N}{m_k}$

3- Creo un nuovo sistema $\begin{cases} N_1 \tilde{x}_1 \equiv a_1 \pmod{m_1} \\ N_2 \tilde{x}_2 \equiv a_2 \pmod{m_2} \\ \dots \\ N_m \tilde{x}_m \equiv a_m \pmod{m_m} \end{cases}$

4- Trovo una soluzione per ogni congruenza

5- La soluz. finale sarà $\bar{x} = N_1 \tilde{x}_1 + N_2 \tilde{x}_2 + \dots + N_m \tilde{x}_m$

□

DETERMINARE RESTO NELLA DIVISIONE DI α PER β

SITUAZIONE GENERALE

Generalmente si ha qualcosa del tipo $\alpha = a^b$ e $\beta = m$ con a e b molto grandi.

OSSERVAZIONE

Il resto è sicuramente compreso tra $0 \leq \dots < m$

Quindi il resto è CONGRUO MODULO m ad α. $\longrightarrow$ $\bar{r} = \bar{\alpha} = \bar{a}^b$

COME RISOLVERE

1- Semplifica il più possibile a (possibilmente numeri positivi). $\bar{a}^b \equiv_m \bar{c}^b$ con $c <<<$

2- Ora puoi avere due casi:

CASO 1: $\bar{c} \in \mathcal{U}(\mathbb{Z}_m)$ $(MCD(c,m) = 1)$

1- Per il teorema di EULERO so che $\bar{c}^{\phi(m)} = 1$

2- Trovo $\phi(m)$: se m è primo $\phi(m) = m-1$

se m non è primo lo scrivo come $d^\gamma \cdot f^\delta$ con d e f primi.
Ora so che $\phi(p^l) = p^l - p^{l-1} = p^{l-1}(p-1)$

3- Divido b per $\phi(m)$

4- Ora $b = \phi(m) \cdot q + r$

5- $\bar{c}^b = \bar{c}^{(\phi(m)\cdot q)+r} = (\bar{c}^{\phi(m)})^q \cdot \bar{c}^r = \bar{c}^r$ ($\bar{c}^{\phi(m)} = 1$)

CASO 2: $\bar{c} \notin \mathcal{U}(\mathbb{Z}_m)$ $(MCD(c,m) \neq 1)$

0- Cerca di scomporre $\bar{c}$, se riesci a ricavare almeno un fattore $\in \mathcal{U}(\mathbb{Z}_m)$ vai con CASO 1. Per il restante fattore $\notin \mathcal{U}(\mathbb{Z}_m)$ continua con CASO 2.

1- Trova e_0, e_+ (calcola a mano $\bar{c}^1, \bar{c}^2, \bar{c}^3, \dots$ finchè non trovi due congruenti modulo m)

2- e_0 è l'esponente più piccolo, e_+ è quello più grande.

3- Se $b < e_0$ non posso fare nulla
Se $b \geq e_+$ dividi $b - e_0$ per $e_+ - e_0$

4- Ora $(b-e_0) = (e_+ - e_0)\cdot q + r$

5- $\bar{c}^b$ lo scrivo come $\bar{c}^{e_0+(b-e_0)}$

6- $\bar{c}^{e_0+(b-e_0)} = \bar{c}^{e_0+(e_+-e_0)\cdot q + r} = \bar{c}^{e_0+(e_+-e_0)\cdot q} \cdot \bar{c}^r$

$\bar{c}^{e_0} \cdot \bar{c}^r$

3- Ora che è tutto semplificato cerca una congruenza.

□

NUMERO GRANDE α DIVISIBILE PER β SENZA FARE DIVISIONI

1- α è divisibile per β se $r = 0$

2- Importa che $\alpha \equiv_\beta 0$

3- Semplifica il più possibile α (scrivi con potenze in base oppure th. Eulero).

4- Vedi se il numero "semplificato" $\equiv_\beta 0$

□

CAMBIAMENTI DI BASE

CONVERTIRE DA BASE α a BASE β con $\alpha, \beta \neq$ DIECI

COME PROCEDERE

1- Converti da base α a base DIECI

2- Converti da base DIECI a base β □

CONVERTIRE DA BASE α A BASE DIECI

1- Comincia dalla cifra più a destra del numero in base α $(1234)_\alpha$

2- Moltiplica la cifra per α^i con i posiz. corrispondente (1234) $3\ 2\ 1\ 0$

3- Somma il risultato ottenuto con il risultato della cifra successiva $4 \cdot \alpha^0 + 3 \cdot \alpha^1 + 2 \cdot \alpha^2 + 1 \cdot \alpha^3$

4- Il risultato finale è in BASE DIECI. □

CONVERTIRE DA BASE DIECI A BASE β.

$(\dots\dots)_\alpha$ | β	Resti

1- Crea la seguente tabella:

2- Dividi il numero in base dieci per β.

3- Metti il quoziente sotto il numero, riscrivi β e metti il resto nella colonna resti

4- Itera finchè il quoziente non è zero.

5- Il numero $r_3\ r_2\ r_1$ è il risultato.

$(\dots\dots)_{DIECI} = (r_3\ r_2\ r_1)_\beta$ □

$(\dots\dots)_\alpha$	β	Resti
	β	r_1
q_1	β	r_2
q_2	β	r_3
$\emptyset$		

$(\dots\dots)_\alpha$	β	Resti
	β	r_1
q_1	β	

DIMOSTRAZIONI PER INDUZIONE

INDUZIONE DEBOLE

1- Dimostra per $n = 0$
2- Supponi vera per n
3- Dimostra per $n+1$

INDUZIONE FORTE

Se la proprietà P vale per tutti gli $m < n$, allora vale anche per n.

ESERCIZI RETICOLI / DIAGRAMMI DI HASSE.

COME SCOMPORRE UN NUMERO IN FATTORI PRIMI

1- Dividi il numero per il più piccolo numero primo che sia suo divisore
2- Dividi il quoziente per il più piccolo numero primo che sia suo divisore
3- Ripeti finchè il quoziente non sia 1. □

COME TROVARE TUTTI I DIVISORI DI UN NUMERO

1- Scomponi in fattori primi
2- Forma una tabella così:

Esempio: $540 = 2^2 \cdot 3^3 \cdot 5$ ⟶

1	2^1	2^2
1	3^1	3^2 3^3
1	5^1	

⟶

1	2	4	
1	3	9	27
1	5		

3- Moltiplica tutti i numeri della prima riga per ogni numero della seconda riga

1 2 4
1 3 9 27 $= \{1, 2, 4\}$
1 5

1 2 4
1 3 9 27 $= \{3, 6, 12\}$
1 5

1 2 4
1 3 9 27 $= \{9, 18, 36\}$
1 5

1 2 4
1 3 9 27 $= \{27, 54, 108\}$
1 5

5- Moltiplica OGNI numero trovato per la terza riga □

NUMERO DI DIVISORI DI UN NUMERO

$540 = 2^{\textcircled{2}} \cdot 3^{\textcircled{3}} \cdot 5^{\textcircled{1}}$

2 3 1
+1 +1 +1
$3 \cdot 4 \cdot 2 = 24$

□

RETICOLO

Insieme ordinato $(L, \leq)$ t.c. $\forall x,y \in L \quad \exists \sup(x,y) \in L \;,\; \exists \inf(x,y) \in L$

$\forall (x,y) \in L \longrightarrow \begin{matrix} (x \wedge y) = \inf(L') \\ (x \vee y) = \sup(L') \end{matrix}$ $\quad L'$ = sottoinsieme di L formato da x, y

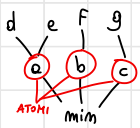
ALGEBRA DI BOOLE

DEF. 1 È un reticolo distributivo, limitato, complementato

- distributivo: se al suo interno non ha sena struttura "pentagonale" o a "diamante"
- limitato: dunque ha un MAX e un MIN
- complementato: se $\forall$ elemento $a \in$ reticolo, $\exists \lambda$ t.c. $a \wedge \lambda = \emptyset$, $a \vee \lambda = 1$

ATOMI

Se $\exists \emptyset := \min(L)$, a si dice ATOMO se $\emptyset \longrightarrow a$ & $\nexists\, b \in L$ t.c. $\emptyset < b < a$



ELEMENTI V-RIDUCIBILI

a è V-RIDUCIBILE se $\exists\, b,c \in L$ t.c. $a = b \vee c$

ELEMENTI V-IRRIDUCIBILI

Se non sono V-riducibili

ELEMENTI MINIMALI

$e_- \in E'$ si dice MINIMALE in E' se $\forall e' \in E'$ si ha $e' \leq e_- \longrightarrow e' = e_-$

ELEMENTI MASSIMALI

$e_+ \in E'$ si dice MASSIMALE in E' se $\forall e' \in E'$ si ha $e' \geq e_+ \longrightarrow e' = e_+$

MINIMO

$e_- \in E'$ si dice MINIMO in E' se $e_- \leq e' \;\forall e' \in E'$ (e_- è l'unico MINIMALE)

MASSIMO

$e_+ \in E'$ si dice MASSIMO in E' se $e_+ \geq e' \;\forall e' \in E'$ (e_+ è l'unico MASSIMALE)

Generalmente:

$\delta \longrightarrow \begin{matrix} \vee = \text{m.c.m.} \\ \wedge = \text{M.C.D} \end{matrix}$

$\subseteq \longrightarrow \begin{matrix} \vee = \cup \\ \wedge = \cap \end{matrix}$

$\leq \longrightarrow \begin{matrix} \vee = \max \\ \wedge = \min \end{matrix}$

ESERCIZI SU RELAZIONI

PROPRIETÀ RELAZIONI

$\forall$ insieme E, $\forall \rho \in \mathcal{R}(E)$, si dice che ρ è:

- (R) RIFLESSIVA se $\forall a \in E \quad a \rho a$
- (T) TRANSITIVA se $\forall a,b,c \in E$, si ha che $(a \rho b) \wedge (b \rho c) \longrightarrow a \rho c$
- (S) SIMMETRICA se $\forall a,b \in E$ si ha che $a \rho b \longrightarrow b \rho a$
- (A) ANTISIMMETRICA se $\forall a,b \in E$ si ha che $(a \rho b) \wedge (b \rho a) \longrightarrow a = b$

TIPI DI RELAZIONI

PREORDINE se è (R) & (T)

ORDINE se è (R), (T) & (A)

ORDINE TOTALE se è ORDINE e $\forall a,b \in E$ si ha $(a \rho b) \vee (b \rho a)$

EQUIVALENZA se è (R), (T) & (S)

CLASSI DI EQUIVALENZA

OGNI SOTTOINSIEME DELLA PARTIZIONE (Insieme degli elementi in relazione ρ con a) $[a]_\rho$ (rappresentante della classe)

INSIEME QUOZIENTE

Insieme formato dalle classi di equivalenza

CRITERI DI DIVISIBILITÀ

Un numero è divisibile per

- 2 se → CIFRA UNITÀ PARI
- 3 o 9 se → SOMMA SUE CIFRE È MULTIPLO DI 3
- 4 o 25 se → ULTIME DUE CIFRE FORMANO MULTIPLO DI 4 (o 25) o SONO 00
- 5 se → CIFRA UNITÀ È 0 o 5
- 10, 100, 1000 se → ULTIME CIFRE SONO RISPETTIVAMENTE 0, 00, 000
- 11 se → DIFFERENZA TRA SOMMA CIFRE POSTO DISP E SOMMA CIFRE PARI È MULTIPLO DI 11.

POLINOMI BOOLEANI

COME SEMPLIFICARE IL POLINOMIO

$(a \wedge b)' = a' \vee b'$
$(a \vee b)' = a' \wedge b'$ — De Morgan → Parti dalle parentesi più esterne

$a \vee a = a$
$a \wedge a = a$ — Idempotenza

Può risultare più semplice mettere (pensare) $\cdot$ al posto di $\wedge$ e $+$ al posto di $\vee$.

$a \vee ab = a$
$a \wedge (a \vee b) = a$ — Assorbimento

$a \wedge 1 = a$
$a \vee 0 = a$ — Identità

$a \wedge 0 = 0$
$a \vee a' = 1$ — Complementi

$a \wedge a' = 0$
$a \vee 1 = 1$ — Annullamento

COME TROVARE FND

1- Semplifica il polinomio il più possibile
2- I termini incompleti moltiplicali per $(a \vee a')$ con a termine mancante ($a \vee a' = 1$) □

COME TROVARE S.T.I.P.

1- Semplifica il polinomio il più possibile
2- Trova i vari coseni (se due termini hanno in comune la lettera "opposta").
3- Aggiungi tutti i coseni al polinomio semplificato
4- Semplifica ancora dove possibile (generalmente con assorbimento) □

COME TROVARE F.m.

1- Trova S.T.I.P.
2- "Completa" ogni implicante primo
3- Vedi termini in comune
4- Se i termini di un implicante sono TUTTI in comune con gli altri implicanti, rimuovi quell'implicante da S.T.I.P. □