

OMOMORFISMO - CASO D'USO  $(G, \cdot) \rightarrow \mathbb{Z}_{18}$ 

"Dato il gruppo  $(G, \cdot)$ , e la funzione  $f: (G, \cdot) \rightarrow \mathbb{Z}_{18}$   $f(g^n) = \overline{6n}$

Verificate che sia omomorfismo, iniettiva, suriettiva.  $G$  ha periodo  $30^u$   
ogni elemento di  $G$  può essere definito come  $g^k$  per qualche  $k \in \mathbb{Z}$

In questo caso particolare, siccome il periodo di  $G$  è  $30$ , allora

$$g^k = g^{k+30t} \quad \text{Procedendo a dimostrare:}$$

- Bon definito: Dati  $a, b \in G$  con  $a = b$  allora

$$\text{se } a = b = 0$$

$$\text{se } a = b = \overline{6n}$$

$$\text{sse } 6(n-30t) = 6(n-30t) = 0$$

$$\text{sse } 6n - 180t = 6n - 180t = 0$$

$$\text{sse } \overline{6n} = \overline{6n} = 0 \quad \text{Verificate}$$

applicando  $f$

$$180t = \overline{0} \text{ in } \mathbb{Z}_{18}$$

- Iniettività (tramite Kernel)

$$\text{Kernel } (f) = \{ \overline{0} \} \rightarrow f \text{ è iniettiva}$$

$$= \{ n \in \mathbb{Z} \mid 6n = \overline{0} \}$$

$$= \{ \overline{0}, \overline{3}, \overline{6}, \dots \} \neq \{ \overline{0} \} \quad f \text{ non è iniettiva}$$

- Suriettività

$$\text{Im}(f) = \{ \overline{6n} \in \mathbb{Z}_{18} \}$$

$$= \{ \overline{0}, \overline{6}, \overline{12} \} \neq \mathbb{Z}_{18} \quad \text{non è suriettiva}$$

OMOMORFISMO - CASO D'USO  $\mathbb{Z}_n^{\times} \rightarrow \mathbb{Z}_{20}$

"Dimostrare che la funzione

$f: \mathbb{Z}_n^{\times} \rightarrow \mathbb{Z}_{20} \quad f([2]_n^k) = [2k]_{20}$  è Omomorfismo iniettivo"

1) Sappiamo che per defi  $\mathbb{Z}_n^{\times} \not\models n$  quindi  $\exists 0$  quindi si procede definendo che

Dati  $a, b \in \mathbb{Z}_n^{\times}$ , se  $a=b$  allora

2.) Suolgo la dimostrazione

$$[2]_n^k = [2]_n^h \iff k-h=0 \iff \text{Applicando } f \Rightarrow \begin{aligned} &\iff 10|k-h \\ &\iff 20|2(k-h) \\ &\iff 20|2k-2h \end{aligned}$$

3.) Verifico se è omomorfismo

$$\begin{aligned} f([2]_n^k \cdot [2]_n^h) &= f([2]_n^k) + f([2]_n^h) \\ f([2]_n^{k+h}) &= [2k]_{20} + [2h]_{20} \\ [2^{(k+h)}]_{20} &= [2^{(k+h)}]_{20} \quad \text{Verificata} \end{aligned}$$

4.) Verifico se è Iniettivo  $\iff \text{Kernel}(f) = \{e_{20}\}$

$$\begin{aligned} \text{In } \mathbb{Z}_n^{\times} \text{ c'è } \pm & \quad \text{Kernel}(f) = \{n \in \mathbb{N} \mid [2]_n^n = \pm 1\} \\ &= \{[2]_n^0\} \leftarrow \text{è iniettiva} \end{aligned}$$

$\hookrightarrow$  è nella forma  
delle formule  
è verificata.

CASO D'USO: TROVARE CONTRO-IMMAGINE  $\rightarrow$  IN:  $f: \mathbb{Z} \rightarrow \mathbb{Z}_n^{\times} \times \mathbb{Z}_m^{\times} \quad ([ky]_n, [hx]_m)$

Dato l'omomorfismo  $f: \mathbb{Z} \rightarrow \mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2}, n \mapsto ([2n]_{l_1}, [3n]_{l_2})$ , Trova se possibile la contro-immagine di  $([\frac{3}{l_1}], [\frac{3}{l_2}])$

Una tupla simile si trova soltanto se vale il sistema di congruenze:

$$\begin{cases} ky \equiv r_1 \pmod{n} \\ hx \equiv r_2 \pmod{m} \end{cases} \rightarrow \begin{cases} 2n \equiv 3 \pmod{l_1} \\ 3n \equiv 3 \pmod{l_2} \end{cases}$$

$$3n \equiv 3 \pmod{l_2}$$

$$\text{MCD}(3, l_2) = 3 \iff 3 \text{ non è inv. in } \mathbb{Z}_{l_2}$$

$$2l_2 = 7 \cdot 3 \cdot 10 \quad \text{ma } 3 \nmid 3 \quad \text{quindi } \frac{3n}{3} \equiv \frac{3}{3} \pmod{\frac{2l_2}{3}} \nmid \frac{3}{3} \rightarrow n \equiv 1 \pmod{l_2}$$

Risoltto 1, si applica le def. per risolvere l'altro

$$n \equiv 1 \pmod{l_2} \iff n = 1 + 4t \rightarrow 2n = 2 + 4t \rightarrow 2 + 4t \equiv 3 \pmod{l_1} \\ 6 \times 6 \rightarrow 6 \qquad \qquad \qquad 2 \equiv 3 \pmod{l_1}$$

Assurdo!  $(\frac{3}{l_1}, \frac{3}{l_2})$  non può esistere.

OMOMORFISMO - CASO DIVISO  $\mathbb{Z} \rightarrow \mathbb{Q}^\times \times \mathbb{Z}_6$

" Si consideri il Gruppo prodotto  $(\mathbb{Q}^\times \times \mathbb{Z}_6, *)$  ricordandosi che su  $\mathbb{Q}^\times$  l'operazione è la moltiplicazione e su  $\mathbb{Z}_n$  l'operazione è l'addizione. Date la funzione

$$f: \mathbb{Z} \rightarrow \mathbb{Q}^\times \times \mathbb{Z}_6 \quad n \mapsto [(-1)^n, \bar{n}]$$

Verificare che:

- $f$  è Omomorfismo
- Calcolare  $\text{Ker}(f)$  è dire se è iniettiva
- Calcolare  $\text{Im}(f)$  è dire se è un gruppo ciclico. Se lo è esibire un generatore.

o) Skip controllo ben definita

(1) Omomorfismo

$$f(a+b) = f(a) * f(b)$$

$$(\underline{-1})^{a+b}, \bar{a+b} = (\underline{-1})^a, \bar{a} * ((-1)^b, \bar{b}) \rightarrow$$

$$(\underline{-1})^{a+b}, \bar{a+b} = (\underline{-1})^{a+b}, \bar{a+b}$$

z)  $\text{Ker}(f)$

$$\begin{aligned} \text{Ker}(f) = \{ n \in \mathbb{Z} \mid f(n) = (1, \bar{0}) \\ = \{ 0, 6, 12, \dots \} \end{aligned}$$

Quindi è

$$\begin{aligned} & \{ n \in \mathbb{Z} \mid 2|n \wedge 6|n \} \text{ mcm}(2, 6) \\ & = \{ n \in \mathbb{Z} \mid 6|n \} \end{aligned}$$

Non è iniettiva

3)  $\text{Imm}(f)$

Calcolata manualmente

$$\text{Im}(f) = \{ (1, \bar{0}), (-1, \bar{1}), (1, \bar{2}), (-1, \bar{3}), (1, \bar{4}), (-1, \bar{5}) \}$$

Siccome su  $\mathbb{Q}^\times$  l'operazione è la moltiplicazione e  $\mathbb{Z}_n$  l'operazione è l''addizione'

$$-1^n = \underbrace{1 + 1 + 1 + 1 + \dots}_{n \text{ volte}} \text{ su } \mathbb{Q}^\times$$

$$1^n = \underbrace{1 + 1 + 1 + 1 + \dots}_{n \text{ volte}} \text{ su } \mathbb{Z}_n$$

Su due  $n$ -uple si esegue come operazione quella definita nei loro insiemi di origine.  $(\underline{-1})^a \cdot (-1)^b = (\underline{-1})^{a+b}$

- Per il dominio di  $\mathbb{Q}^\times \times \mathbb{Z}_6$  l'elemento neutro è  $\underline{1}$  quindi per avere  $\underline{1}$   $n$  deve essere pari.  $\underline{2|n}$
- Per il co-dominio, l'elemento neutro è  $\bar{0}$  o  $6|n$ .

Dette queste info si può vedere come  $(-1, \bar{1})^n$  genera tutti gli elementi e che quindi  $\text{Im}(f)$  è ciclico.

# COMBINATORICA

1

## DISPOSIZIONI CON RIPETIZIONE >

In quanti modi si possono scegliere  $K$  elementi da un insieme di  $n$  elementi

$$\overbrace{n \cdot n \cdot n \cdots n}^{K \text{ volte}} = n^K$$

- ✓ conta ordine
- ✓ accettate ripetizioni

## DISPOSIZIONI SEMPLICI >

In quanti modi si possono scegliere  $K$  elementi da un insieme con  $n$  elementi

$$n \cdot (n-1) \cdot (n-2) \cdots (n-(K-1))$$

- ✓ conta ordine
- ✗ accettate ripetizioni

## COMBINAZIONI >

In quanti modi si possono scegliere  $K$  elementi da un insieme con  $n$  elementi

$$C_{n,K} = \binom{n}{K} = \frac{n!}{K! \cdot (n-K)!} = \frac{n \cdot (n-1) \cdots (n-K+1)}{K!}$$

- ✗ conta ordine
- ✗ accettate ripetizioni

## COMBINAZIONI CON RIPETIZIONE >

In quanti modi si possono scegliere  $K$  elementi da un insieme con  $n$  elementi

$$C'_{n,K} = \binom{K+n-1}{n-1} = \frac{(K+n-1)!}{(n-1)! \cdot K!}$$

- ✗ conta ordine
- ✓ accettate ripetizioni

## ANAGRAMMA >

In quanti modi si possono formare riordinamenti di lettere da una parola di  $K$  elementi su un alfabeto di  $n$  elementi in cui

$$\frac{K!}{i_1! \cdot i_2! \cdots i_n!}$$

$i_1, i_2, \dots, i_n$  sono le frequenze delle lettere.

Número di apparizioni:

ES: Anagrammi di "ANNA"  $|w|=4$

$$E = \{a, n\}$$

$$\frac{4!}{2! \cdot 2!}$$

## PERMUTAZIONI &gt;

In quanti modi si possono riordinare tutti gli elementi di un insieme con  $n$  elementi.

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

## PRODOTTO TRA COPPIE &gt; X Insiemi disgiunti

Dati 2 insiemi disgiunti, è il numero di coppie ordinate

## ESEMPIO:

"Date 8 donne e 12 uomini, calcolare le possibili coppie"

$$D = \text{donne}, |D| = 8,$$

$$U = \text{uomini}, |U| = 12$$

$$\Rightarrow |D \times U| = 8 \cdot 12 = 96$$

## INCLUSIONE-ESCLUSIOME &gt;

## [ UNIONE ]

Dati 2 insiemi potenzialmente non disgiunti, è la cardinalità dell'unione.

$$[2 \text{ INSIEMI}] : |X \cup Y| = |X| + |Y| - |X \cap Y|$$

$$[3 \text{ INSIEMI}] : |X \cup Y \cup Z| = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z| + |X \cap Y \cap Z|$$

[per più guardare notes]

ESEMPIO : "Quanti sono i numeri  $\leq 30$  co-primi con 30"

$$1) \text{ Scompongo } 30 : 30 = 2 \cdot 3 \cdot 5$$

$$2) \text{ Sono tutti i numeri divisibili per } 2, 3 \text{ o } 5 \text{ definisco insiemi} \\ x = \{n \in \mathbb{N} \mid 1 \leq n \leq 30 \wedge 2 \mid n\} \quad y = \{n \in \mathbb{N} \mid 1 \leq n \leq 30 \wedge 3 \mid n\} \\ z = \{n \in \mathbb{N} \mid 1 \leq n \leq 30 \wedge 5 \mid n\}$$

3) Definisco le intersezioni con le [regole di semplificaz.]

$$x \cap y = \{n \in \mathbb{N} \mid 1 \leq n \leq 30 \wedge 6 \mid n\} \quad x \cap z = \{n \in \mathbb{N} \mid 1 \leq n \leq 30 \wedge 10 \mid n\}$$

$$y \cap z = \{n \in \mathbb{N} \mid 1 \leq n \leq 30 \wedge 15 \mid n\}$$

4) Definisco gli elementi e applico la formula

$$|X| = \left[ \frac{30}{2} \right] = 15, \quad |Y| = \left[ \frac{30}{3} \right] = 10, \quad |Z| = \left[ \frac{30}{5} \right] = 6, \quad |X \cap Y| = \left[ \frac{30}{6} \right] = 5, \quad |X \cap Z| = 3$$

$$|Y \cap Z| = \left[ \frac{30}{15} \right] = 2 \quad |X \cap Y \cap Z| = 1$$

## INCLUSIONE-ESCLUSIONE ➤

## [ESCLUSIONE]

Dati  $z$  insiemi potenzialmente non disgiunti, è la cardinalità dell'unione.

$$[2 \text{ INSIEMI}] : |x \cup y| = |x| + |y| - |x \cap y|$$

$$[3 \text{ INSIEMI}] : |x \cup y \cup z| = |x| + |y| + |z| - |x \cap y| - |x \cap z| - |y \cap z| + |x \cap y \cap z|$$

[per più guardare notes]

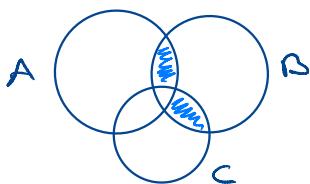
## CASO DI USO ➤ [Elezioni]

"Alle elezioni in Freedonia partecipano 3 liste, A, B, C, ciascuna con 10 candidati e vi sono 2556 cittadini con diritto di voto.

1) Ogni votante deve scegliere esattamente 2 liste altrimenti il voto è nullo. Quelli che hanno votato per A e B, 745 per A e C, B ha ricevuto 1658 voti validi.

Quanti sono i voti nulli? Quale lista ha ottenuto più voti?"

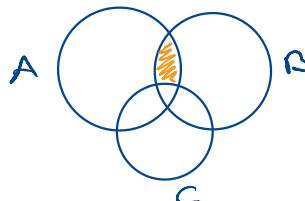
Rappresentandole con insiemi:



Per essere validi, i voti di B sono

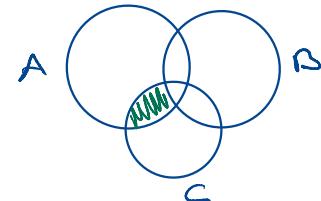
$$1658 = |A \cap B|$$

$$1 + |B \cap C| \\ - 2 \cdot |A \cap B \cap C|$$



Quelli che hanno votato solo A e B

$$\text{ovvero} \quad |A \cap B| = \\ |A \cap B| - |A \cap B \cap C|$$



745 hanno votato solo A e C

$$745 = |A \cap C| \\ - |A \cap B \cap C|$$

liste

$$B = 1658$$

$$C = (1658 + 745) - 910 \\ = 1493$$

$$A = (1658 + 745) - 1658 \\ + 910 = 1495$$

Per sapere i validi basta sommare i voti validi di B e 745 e toglierli dal totale

$$2556 - (1658 + 745) = 1523 \text{ non validi}$$

La prima lista è la A

## CASO D'USO &gt; [elezioni continuazione]

"Alle elezioni in Freedonia partecipano 3 liste, A,B,C, ciascuna con 10 candidati e vi sono 2556 cittadini con diritto di voto.

- 2) Per costituire il consiglio si devono fare 3 scelte successive di combinazioni di 4, 3, 2 candidati. Quante sono le possibili costituzioni?

I 30 candidati delle 3 liste sono disgiunti. In questo caso: - Non conta l'ordine, - Non ci sono ripetizioni

$$\binom{10}{4} \cdot \binom{10}{3} \cdot \binom{10}{2}$$

- 3) Al voto è associato un referendum per la scelta delle bandiere. Essa deve contenere il rosso, il vero e il blu e può avere 3 strisce verticali o 4 strisce orizzontali senza colori uguali adiacenti. Quante sono le bandiere possibili?

Se 3 strisce orizzontali =  $3! = 6$

Se 4 strisce orizzontali =

fissando un dato colore C le possibili posizioni sono:

$$\begin{matrix} 2 \cdot 1 & 2 \cdot 1 & 2 \cdot 1 \\ C-C-C, -C-C-, C-C- \end{matrix} \Rightarrow 2 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 = 6$$

Le posizioni mancanti saranno riempite dai 2 colori rimanenti. Quindi fissato 1 colore si hanno 6 possibilità.

Cambiando colore su 3 abbiamo 28 possibilità.

Sommendo tutto abbiamo 24.

## CASO DIVISO ➤ INSIEMI

"Dato  $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ ,  $T = \{1, 2, 3, 4\}$

- Quanti sono i sotto-insiemi di  $S$  che non contengono il sotto-insieme  $T$ ?
- Quanti sono i sotto-insiemi di cardinalità 8 non contenenti  $T$ ?
- Quanti sono i sotto-insiemi di cardinalità 3 non contenenti 2 numeri consecutivi?

1) Cardinalità  $\mathcal{P}(S-T)$  Per definizione, se un insieme  $X$  è finito  $\mathcal{P}(X) = 2^n$   $n = |X|$

Dato un insieme  $X$  e un sotto-insieme  $B$   $B \subseteq X$  i sotto-insiemi che contengono  $B$  sono  $2^{|X|-|B|}$

Quindi  $\mathcal{P}(S-X) = 2^{10} - 2^6 \rightarrow$  I sotto-insiemi che contengono  $T$

2) Sotto-insiemi da 8 che non contengono  $T$

$$\text{Sotto-insiemi di card 8 generici} = \binom{10}{8}$$

$$\binom{10}{8} - \binom{6}{4} = 45 - 15 = 30$$

Quelli contenenti il sotto-insieme si ottengono sottraendo

$$\binom{6}{4}$$

3) Sotto-insiemi da 3 senza consecutivi:

$$\text{Sotto-insiemi di card 3 generici} = \binom{10}{3} \quad \begin{array}{l} \text{I consecutivi sono:} \\ \{0,1,2\}, \{1,2,3\}, \dots, \{7,8,9\} \end{array}$$

sono 3 da togliere

Scendendo a 2 sotto-insiemi, i possibili sono  $= \{0,1\}, \{1,2\}, \dots, \{8,9\}$  V dei quali per avere elementi non consecutivi

-  $\{0,1,4,8,9\}$ : in 7 modi  $\rightarrow \{0,1,4\} \times$  non deve essere 2 ne 0 ne 1,  $10-3=7$

-  $\{1,2,5,7,8\}$ : in 6 modi  $\rightarrow \{1,2,5\} \times$  non deve essere 3, 0  $\{1,2,5\}$  ne 1 o 2  $10-4=6$

Quindi sarebbe

$$\binom{10}{3} - (8 + 7 + 2 + 6 + 2) = 56$$

# CLASSI DI RESTO • 1

## SOLUZIONI DI CONGRUENZE LINEARI

1. Data la forma  $ax \equiv y \pmod{N}$   
in cui  $y$  è noto, sarà l'insieme

$$\{ \text{MCD}(i, N) | y \mid i \in \mathbb{N}, i > 0 \wedge i \mid y \}$$

Ovvero tutti i numeri per i quali  
l'MCD col modulo divide  $y$

ES "Per quali  $\bar{a} \in \mathbb{Z}_{12}$   
la congruenza  
 $a\bar{x} \equiv 3 \pmod{12}$

ha almeno 1 soluzione?"

gli unici divisori di 3 sono 3, 1

$$\text{MCD}(12, 1) = 1, \text{MCD}(12, 3) = 3 \times$$

$$\text{MCD}(12, 3) = 3, \text{MCD}(12, 4) = 4 \times$$

$$\text{MCD}(12, 6) = 6 \times$$

$$\text{MCD}(12, 7) = 1, \text{MCD}(12, 11) = 1, \text{MCD}(12, 11) = 1$$

$$= \{3, 1, 3, 3, 6, 1, 11\}$$

## DATA $\bar{x}$ , CALCOLARE INVERSA DI $\bar{a}\bar{x}$

1. Avendo a nota, calcolare la  
sua inversa nel modulo

2. Ri-scrivere l'equivalenza usando  
come valori l'incognita inversa  
e l'inversa trovata

ES "Se  $\bar{y}$  è inversa di  $\bar{x}$  in  $\mathbb{Z}_7$ ,  
quell'è l'inversa di  $\bar{ax}$ ?"

1. Calcolo l'inversa di  $\bar{x} \pmod{7}$

$$7 = 3 \cdot 2 + 1 \rightarrow 1 = 7 - 3 \cdot 2$$

2 = 2 · 1 + 0 <sup>\*Bezout</sup>

$$\bar{x} = \bar{7} - 3 \cdot 2 \rightarrow \bar{x} = -3 \cdot 2$$

L'inversa è  $\bar{-3} + \bar{7} \Rightarrow \bar{4}$

2. Risolvendo eq

$$(\bar{ax})^{-1} = (\bar{x})^{-1} \cdot (\bar{a})^{-1} = \bar{4} \cdot \bar{4} \Rightarrow \bar{16}$$

## DETERMINARE L'INVERSO

1. Determinare se è invertibile

$$\text{MCD}(a, b) == 1$$

2. Se lo è, calcolare  $\varphi(n)$   
di  $\mathbb{Z}_n$

3. Semplificare la potenza.

NB: Se si ha che  $\varphi(n) = x$

e  $a^{x-1} \pmod{n}$  si può

semplificare con  $\bar{a}^1 \pmod{n}$

Da lì calcolare l'inverso

ES: "Determinare l'inverso di  
 $\bar{s}$  in  $\mathbb{Z}_{231}$ "

$$(1) \text{ MCD}(5, 231) = 1 \Leftrightarrow 5 \text{ è invertibile}$$

$$(2) \varphi(231) = \varphi(3) \cdot \varphi(7) \cdot \varphi(11) = 120$$

$$(3) 231 = 24 \cdot 120 + 11$$

$$231 = 5^{11} \cdot 5^{11} \pmod{231}$$

$$5^{11} = 5^{12-1} = 5^{-1} \pmod{231}$$

$$5^{-1} \cdot 5^{-1} = 1 \pmod{231}$$

$\bar{s}^{-1} \cdot \bar{s}^{-1} = \bar{1}$  quindi  
l'inverso di  $\bar{s}$  è  $\bar{s}^{-1}$

## CLASSI DI RESTO • 2

[CASO D'OSO]

## CONGRUENZE LINEARI ➤ ELEMENTI INVERTIBILI

Risolvere  $5x \equiv 8 \pmod{26}$ 

- Si verifica se è invertibile:  $\text{RCD}(5, 26)$

$$26/5 \rightarrow 26 = 5 \cdot 5 + \underline{1} \pmod{5}$$

$$5 = 1 \cdot 5 + 0$$

- Si utilizza l'Id. di Bezout per ricavare l'inverso

$$26 = 5 \cdot 5 + 1 \Rightarrow 1 = 26 - 5 \cdot 5 \quad \text{ovvero} \quad 1 = \frac{26}{5} - \frac{5 \cdot 5}{5} \quad \text{quindi}$$

$$\alpha^{-1} = -5$$

- Si calcola l'equazione con l'inverso:

$$-\overline{5} \cdot \overline{5} x = \overline{8} \cdot -\overline{5} \pmod{26} \Rightarrow x = -40 \pmod{26} \Rightarrow x = 12 \pmod{26}$$

## CONGRUENZE LINEARI ➤ NON RISOLVIBILE

Data la congruenza  $6x \equiv 10 \pmod{33}$ , risolvere l'equazione.

- Determino se  $a=6$  è invertibile:  $33/6 \rightarrow 33 = 5 \cdot 6 + 3 \pmod{6}$   
 $6/3 \rightarrow 6 = 2 \cdot 3 + 0$   
 $\text{RCD}(33, 6) = 3$  e non è invertibile.  
 Però...  
 Proseguo...

- Determino se  $d=3$  è divisore di  $10$ :  $3 \nmid 10$   
 3 non è div. di 10. **NON RISOLV.**

## CONGRUENZE LINEARI ➤ RANGE

"Determinare gli  $x \in \mathbb{Z}$  tali che  $150 \leq x \leq 300$  che soddisfano  $4u \equiv 11 \pmod{49}$ "

$$\text{RCD}(11, 49) = 1 \quad 1 = \frac{49 \cdot 11 - 2 \cdot 49}{49} = 1 = \frac{49 \cdot 11}{49}$$

Quindi  $9 \cdot 49 \equiv 11 \pmod{49}$

$$49 = 4 \cdot 11 + 5 \quad 1 = 11 - 2 \cdot (49 - 4 \cdot 11) \rightarrow 11 - 2 \cdot 49 + 8 \cdot 11$$

$$11 = 2 \cdot 5 + 1 \quad 1 = 11 - 2 \cdot 5$$

$$49x \equiv 11 \pmod{49}$$

$$\text{P}(49) = 42 \quad 11 = 11 \rightarrow 8 \pmod{49} \quad 49x \equiv 8 \pmod{49}$$

$$\text{RCD}(49, 4) = 1$$

$$4x \equiv 12 \cdot 4 + 1 \quad 1 = \frac{49 \cdot 12 - 12 \cdot 49}{49}$$

$$4x \equiv 12 \pmod{49}$$

$$-12 \cdot 4x \equiv -8 \cdot 12 \pmod{49}$$

$$x \equiv 2 \pmod{49}$$

$$2 + 49k \quad k \in \mathbb{Z}$$

$$2 + 4 \cdot 49 = 198, \quad 2 + 5 \cdot 49 = 247$$