

CONGRUENZA

$A \equiv_n B$

$(A-B)$ è multiplo di n

A congruo B modulo n

TEOREMA

$$A \equiv_n B \iff A \bmod B = B \bmod A$$

$$\text{dim. } \left. \begin{array}{l} A \equiv_n B \rightarrow A - nk = B \\ A = nq + r \quad (n \text{ divide } B) \end{array} \right\} B = n(q-k) + r \quad (n \text{ divide } B)$$

$$A \equiv_n B \rightarrow A - B = n \cdot k$$

$$17 \equiv_4 3 \quad 17 - 3 = 4k \quad k = \frac{14}{4} \cdot 35 \quad 17 \not\equiv_3 3 \quad \text{dove } k \text{ deve essere un numero intero}$$

$$n \equiv_2 7 \quad n = 7 + 20k \quad k \text{ è multiplo di } 20$$

$$\alpha_x \equiv_n b \quad \alpha_x - nk = b = A_x - B_y = C \quad (\text{DIOFANTICA})$$

PROPRIETÀ:

$$\text{RIFLESSIVA: } A \equiv A$$

$$\text{SIMMETRICA: } A \equiv B \rightarrow B \equiv A$$

$$\text{TRANSITIVA: } \begin{array}{c} A \equiv B \\ B \equiv C \end{array} \rightarrow A \equiv C$$

es. ADDITIVA

$$\begin{array}{c} 5 \equiv_3 23 \\ -35 \equiv_3 22 \end{array} \rightarrow (5 - 35) \equiv_3 (23 - 22) \rightarrow -30 \equiv_3 45 \rightarrow -30 - 45 = 3k \rightarrow -75 \equiv_3 3k$$

\downarrow
 $k = -25$

$$\text{ADDITIVA: } \begin{array}{c} A \equiv A \\ B \equiv B \end{array} \rightarrow A + B \equiv A + B$$

es. MOLTIPLICATIVA

$$\begin{array}{c} 9 \equiv_4 25 \\ 17 \equiv_4 23 \end{array} \rightarrow \begin{array}{c} -16 = 4k \\ 40 = 4k \end{array} \rightarrow \begin{array}{c} k = 4 \\ k = 10 \end{array} \rightarrow 9 \cdot 17 \equiv_4 25 \cdot (-23)$$

$$\text{MOLTIPLICATIVA: } // \rightarrow A \cdot B \equiv A \cdot B$$

$$\text{es. } 6x \equiv_9 1 \quad ? \quad 6x - 9k = 1 \quad (\text{DIOFANTICA}) \quad \exists \frac{1}{\text{MCD}(6, 9)} \quad ? \quad \text{No, non ammette soluzioni}$$

$$\text{es. } 6x \equiv_{11} 1 \quad ? \quad 6x - 1 = 11k \rightarrow 6x - 11y = 1 \rightarrow \exists \frac{1}{\text{MCD}(6, 11)} \quad ? \quad \frac{1}{1} = 1 : \text{Sì, ora troviamo } k$$

$$\text{DIOFANTICA: } \left[\begin{array}{c|c} 6 & 11 \\ 11 & 5 \\ 5 & 1 \\ 1 & 0 \end{array} \middle| \begin{array}{c} 1 \\ 11+5(-1) \\ 1 = 11(1) + 5(2) \\ 5 = 11+5(-1) \end{array} \right] \rightarrow -11(1) + 6(2) = 1 \rightarrow x = \frac{A}{\text{MCD}} = -11 \quad \rightarrow \begin{array}{c} x = 2 \cdot -11k \\ y = 1 - 6k \end{array}$$

CON PIÙ VARIABILI:

$$\begin{cases} n \equiv_1 1 \\ n \equiv_2 2 \end{cases} \longrightarrow \begin{cases} n-1 = 5K_1 \\ n-2 = 3K_2 \end{cases} \dots \rightarrow n=11 \quad \begin{matrix} K=2 \\ K=3 \end{matrix}$$

TEOREMA CINESE DEL RESTO:

$$\begin{cases} n \equiv_a X \\ n \equiv_b Y \end{cases}$$

$\left[\begin{array}{l} \text{se ammette soluzione} \\ \text{ne avrà infinite} \end{array} \right]$

• ha soluzione solo se $\frac{Y-X}{\text{MCD}(a,b)}$

$$n = n_0 + \text{mcm}(a,b) \cdot K$$

$$\downarrow \frac{|a-b|}{\text{MCD}}$$

nella k trova dalla definizione un'equazione

es) $\begin{cases} n \equiv_{22} 5 \\ n \equiv_{12} 1 \end{cases}$

$$\begin{cases} n = 5 + 22K \\ n = 1 + 12K' \end{cases} \longrightarrow 5 + 22K = 1 + 12K'$$

$$22K - 12K' = -4 \quad \text{BIOFANTEN} \rightarrow K = 2$$

$$K' = 4$$

$$n = 5 + 22(2) = 49$$

$$\text{mcm}(22,12) = 132$$

$$\left\{ \begin{array}{l} n = 49 + 132K \\ \longrightarrow n = 49 \end{array} \right.$$

es)

$$\begin{cases} n \equiv_{24} -1 \\ n \equiv_{39} 4 \end{cases} \quad \text{MCD}(24,39) = 3$$

$$\exists \frac{-1 - (-1)}{3} ?$$

NO, non ha soluzioni

SISTEMA A 3

$$\begin{cases} n \equiv_7 3 \\ n \equiv_4 1 \\ n \equiv_5 3 \end{cases}$$

(1) risolvo i primi 2

(risolvo a 2 a 2
mettendo a sistema il risultato precedente)

(1)

$$\begin{cases} n = 3 + 7k \\ n = 1 + 4k' \end{cases} \rightarrow 3 + 7k = 1 + 4k' \rightarrow 7k - 4k' = -2 \rightarrow k = -2$$

$n_0 = 3 + 7(-2) \leftarrow$ soluzione

 $n_0 = -11$
 $n = -11 + mcm(7, 4)k$

(2) risolvo anche il risultato della ziga rotolante

$$\begin{cases} n = -11 + 28k \\ n = 3 + 5k' \end{cases} \rightarrow 28k - 5k' = 14 \rightarrow$$

a mente:
 $k = 3$
 $k = 4$

 $n_0 = -11 + 28(3) \rightarrow n_0 = -11 + 84$
 $n = n_0 + mcm(28, 5)k$

ricordando che 5 non può dare
il n finale = 4 $\rightarrow 28 + 5k \rightarrow 4$

$n = n_0 + mcm(28, 5)k$

VARIABILI INCOGNITE

$$\begin{cases} n \equiv_{180} 21 + A \\ n \equiv_{105} 2A + 1 \end{cases}$$

• trova A

• trovare le soluzioni per $A = -68$

(1) ΔOMNIO
(trova A)

(2) riempienti
risolvo con

$$\begin{cases} n \equiv_{180} 21 - 68 \\ n \equiv_{105} 2(-68) - 1 \end{cases} \rightarrow \begin{cases} n = -47 + 180k \\ n = -137 + 105k \end{cases}$$

$$\frac{(2A+1) - (21+A)}{\text{MCD}(180, 105)}$$

?

$$\frac{A - 22}{45}$$

$$A \equiv_{45} 22$$

$$180x - 105y = -30 \rightarrow n = 180x - 105y$$

NOTO: puoi dividere la diseguale, e non puoi escluderla

$$\frac{180k - 105k' = -30}{15} \rightarrow 12k - 7k' = -6$$

non puoi dividere da 12

$$\begin{aligned} 12 &= 7 + 5 \\ 7 &= 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} S &= 12 \cdot 1 + 7 \cdot (-1) \\ &= 2 \cdot 7 \cdot (1) + 12 \cdot (-1) \\ &= 5 \cdot (2) \cdot (1) + 12 \cdot (-1) \\ T &= 12 \cdot (2) + 7 \cdot (-3) \end{aligned}$$

Divisione Password: CONDIVISIONE SEGRETI *

voglio che per ricavare la password serve la combinazione di m elementi, per farlo divido la password in n elementi

$$n \cdot e \quad n \cdot 3$$

PASSWORD $\begin{cases} a \\ b \\ c \end{cases}$ $a < b < c$
 (COPRIMI TRA LORO) $(\text{GCD} = 1)$

la combinazione di 2 di questi darà la password

$$\text{range value} = [\alpha, (\alpha \cdot b) - 1]$$

$$\text{PASSWORD: } \begin{cases} x \equiv_a (\text{x mod } a) \\ x \equiv_b (\text{x mod } b) \end{cases} \longrightarrow x = \dots + \dots \cdot k$$

il valore che rientra
nel range è
la password

($x \text{ mod } \dots$) viene chiamato
non deve appartenere al range x

es.

IL BOSS DÀ UN PEZZO DI PASSWORD A 5 DIPENDENTI, PER RICOSTRUIRE LA PASSWORD SERVE UNA COMBINAZIONE DI 3 PEZZI

$$a < b < c < d < e \quad \text{range: } [\emptyset, (a \cdot b \cdot c) - 1]$$

$$\begin{cases} x \equiv_a (\text{x mod } a) \\ x \equiv_b (\text{x mod } b) \\ x \equiv_c (\text{x mod } c) \end{cases} \quad X \equiv \dots \text{ risultato}$$

$$\left. \begin{array}{l} \text{es. 1} \\ \left. \begin{array}{l} a = 121 \\ b = 122 \\ c = 123 \end{array} \right\} h_0 \\ m = a \cdot b = 14762 \\ 0 < x < m-1 \rightarrow x = 8374 \\ \text{soltanto corso} \end{array} \right\}$$

$$\text{trovo in t.c. } x \text{ è in ogni gruppo}$$

$$\begin{array}{l} x \equiv_{121} n \\ x \equiv_{122} n' \\ x \equiv_{123} n'' \end{array} \rightarrow \begin{array}{l} x \equiv_{121} 57 \\ x \equiv_{122} 102 \\ x \equiv_{123} 26 \end{array} \xrightarrow{\text{perche}} 8374 = \begin{array}{l} 121k + 57 \\ = 122k + 102 \\ = 123k + 26 \end{array} \begin{array}{l} \text{con } k = 77 \\ \text{con } k = 76 \\ \text{con } k = 75 \end{array}$$

$$\left. \begin{array}{l} \text{es. 2} \\ \left. \begin{array}{l} a = 31 \quad b = 32 \quad c = 33 \\ m = 31 \cdot 32 = 992 \quad \boxed{x = 719} \quad \text{prova con } k=1 \\ 1^{\circ}: x \equiv_{31} 29 \quad \text{trovo} \quad \text{no modulo 2} \\ 2^{\circ}: x \equiv_{32} 7 \quad \rightarrow \quad \begin{cases} x \equiv_{32} 7 \\ x \equiv_{33} 18 \end{cases} \quad \xrightarrow{\text{teorema cinese}} x = -345 + 1056k \\ 3^{\circ}: x \equiv_{33} 18 \end{array} \right\} \end{array} \right\}$$

* Dati $a, b, c /$ combinazione di 2

① $m = a \cdot b$

② $x = \text{prendo un valore in } (0 < x < m-1)$

③ $\begin{cases} x \equiv_a \dots \\ x \equiv_b \dots \\ x \equiv_c \dots \end{cases} \xrightarrow{\text{TROVO ...}} \begin{cases} x \equiv_{ak} \dots \\ x \equiv_{bk} \dots \\ x \equiv_{ck} \dots \end{cases} \quad (\text{il resto dev'essere il resto della c})$

④ Prendo le combinazioni e risolvo

$$\begin{cases} x \equiv_a n \\ x \equiv_b n' \\ x \equiv_c n'' \end{cases} \quad x \equiv \dots \text{ risultato}$$

multipl di 3: $x \equiv_3 0$ perche: $x = 3k$

Esercizio 10 Costruire uno schema di condivisione di segreti che permetta a **cinque** partecipanti A, B, C, D, E di condividere un segreto. Lo schema deve essere tale che **il segreto deve poter essere ricostruito solo mediante la collaborazione di A e di altri 2 partecipanti**. Il modulo assegnato ad ogni partecipante deve essere maggiore o uguale a 40.

$$A = n \cdot n \cdot n \quad B = n \quad C = n \quad D = n \quad E = n$$

Soluzione. È sufficiente scegliere 7 numeri primi tra loro maggiori o uguali a 40. Possiamo prendere 41, 42, 43, 47, 49, 51, 53. Il segreto è identificato da una chiave k compresa fra 0 e $41 \cdot 42 \cdot 43 \cdot 47 \cdot 49 - 1 = 170527937$ (usiamo quindi il prodotto di 5 moduli). Ad A viene assegnato il valore $k \text{ mod } 41 \cdot 42 \cdot 43 = 74046$. Ai partecipanti B, C, D, E vengono assegnati rispettivamente i valori k modulo 47, 49, 51, 53. È immediato verificare che senza la collaborazione di A il segreto non può essere ricostruito in quanto gli altri partecipanti insieme possono ottenere solo $k \text{ mod } 47 \cdot 49 \cdot 51 \cdot 53 = 6225009$. Utilizzando invece i 3 moduli conosciuti da A e altri due moduli qualsiasi è sempre possibile ricostruire il segreto. \square