Calcolare l'MCD tra 2 numeri	Si procede con l'algoritmo di Euclide (come si vede a pagina 2). Il risultato del MCD è l'ultimo resto non nullo (ovvero $r_n \neq 0$).
Trovare l'identità di Bèzout	Si procede con l'algoritmo di Euclide e poi a partire dall'ultimo resto non nullo si va a ritroso fino ad arrivare ad un' equazione di questo tipo $r_n = A \cdot a + B \cdot b$
Come trovare l'inverso moltiplicativo di $[A]_n$	Controllo che l' MCD (A, n) = 1 e procedo facendo la divisione tra A e n usando l'algoritmo di Euclide (come si vede a pagina 2). Poi trovo l'identità di Bèzout di A e n che sarà nella forma $1 = a \cdot A + b \cdot n$ L'inverso moltiplicativo sarà il coefficiente di A, perciò $[a]_n$
Come risolvere una congruenza	$a\boldsymbol{x} + k \equiv b \bmod N$ La nostra incognita è **X** e il nostro obiettivo è quello di trovare la classe in modulo N che soddisfi la congruenza. La congruenza ha soluzione sse MCD(a, N)| b (se $k \neq 0$ ha soluzione sse MCD(a, N)| (b-k)). Verificato questo, se $k \neq 0$, lo sposto al secondo membro e diventa $a\boldsymbol{x} \equiv b \bmod N + k \bmod N \rightarrow a\boldsymbol{x} \equiv (b-k) \bmod N$ (pongo c =(b-k) per semplicità) Procedo con l'algoritmo di Euclide con a e N e poi trovo l'identità di Bèzout $1 = A \cdot a + B \cdot N$ Moltiplico entrambi membri per A e la congruenza diventa $\boldsymbol{x} \equiv Ab \bmod N$, se $k \neq 0$ $\boldsymbol{x} \equiv Ac \bmod N$
Come trovare il resto di una divisione per un numero	Il testo chiede "di trovare il resto della divisione tra $7^{777} + 3^{333}$ per 7" Controllo che l'MCD(7,7) e MCD(3,7) siano uguali a 1. MCD(7,7) = 7 mentre MCD(3,7) = 1 Applico il teorema di Eulero per cui $3^{\varphi(7)} \equiv 1 \bmod 7$ $\varphi(7) = 7-1 = 6$ Faccio la divisione intera tra l'esponente del 3 e $\varphi(7)$ $333 = 55 \cdot 6 + 3$ $7^{777} + 3^{333} = 7^{777} + 3^{(55\ 6\ +\ 3)} = 7^{777} + 3^{55\ 6} \cdot 3^3$ In modulo 7 l'espressione diventa $7^{777} + 3^{55\ 6} \cdot 3^3 \equiv 0 + 1 \cdot 3^3 \bmod 7 \equiv 3^3 \bmod 7$ Facciamo la divisione intera di 3^3 per 7 per trovare la classe di resto di 3^3 mod 7 $3^3 = 27 \rightarrow 27 = 3 \cdot 7 + 6$ Perciò la soluzione dell'esercizio è 6
Come vedere se una funzione è ben definita	Una funzione è ben definita se per ogni elemento esiste una ed una sola immagine. Prendendo come esempio una funzione f definita così $\mathbb{Z}_8 \rightarrow S_8$, $[k]_8 \mapsto \sigma^k$ (con per(σ) = 4). In $\mathbb{Z}_8$ $[0]_8 = [16]_8$ ma $0 \neq 16$, perciò dobbiamo controllare se 0 e 16 hanno la stessa immagine. Prendo $[k]_8$ e $[l]_8 \in \mathbb{Z}_8 : [k]_8 = [l]_8$ perciò il mio obiettivo è che $\sigma^k = \sigma^l$ $[k]_8 = [l]_8 \rightarrow k = 8 \cdot n + l$ Applico la funzione: $\sigma^k = \sigma^{8n+l} = \sigma^{8n} \cdot \sigma^l = id \cdot \sigma^l = \sigma^l \quad \forall n \in \mathbb{Z}$ $\sigma^k = \sigma^l \rightarrow f$ è ben definita