Esercizio !!
Calcola il reciproco di 98 mod. 191 e il reciproco di 101 mod. 127.

TEOREMA CINESE DEL RESTO
Problema introduttivo
Vogliamo trovare un numero X che abbia come resto della divisione per 7 pari a 2 e come resto della divisione per 15 pari a 4.

Soluzione
I numeri 7 e 15 sono primi fra loro. Con queste condizioni la soluzione non è unica: ce ne sono infinite, distanti fra loro come il prodotto 7x15 = 105. Quindi basta trovarne una, la chiamiamo X_0, tutte le altre soluzioni sono della forma:

$$X_0 + k105$$

Per trovare la prima soluzione si può andare per tentativi, elencando i multipli di 7 (a cui aggiungere 2), e i multipli di 15 (a cui aggiungere 4). Il primo numero comune ai due elenchi è il nostro X_0.

2,9,16,23,30,37,44,51,58,65,72,79,86,93,100,107, 114,128,135,142,149,156, e così via;
4,19,34,49,64,79,94,109,124,139,154, e così via.

Il primo numero naturale comune ai due elenchi è 79: infatti 79 = 15x5 + 4 = 7x11 + 2.

Quindi tutte le soluzioni cercate sono: 79 + k105.

Ma ad elencarli tutti è lento … potrebbe essere necessario fare elenchi lunghissimi.
Introduciamo allora i "Numeroni": si tratta del **mcm di tutti i divisori meno uno**, cosa che diventa fondamentale quando le divisioni considerate sono almeno tre. Nel nostro caso i "Numeroni" altro non sono che i divisori stessi, ma "scambiati", dato che ci sono solo due divisori (2 – 1 = 1).

Partendo da: $x = 2 + n7$ e $x = 4 + m15$ si ricorda il simbolo di congruenza
$x \equiv 2 \bmod 7$ e $x \equiv 4 \bmod 15$
$N_1 = 15$ $N_2 = 7$
si usano ora i "numeroni", risolvendo invece:

$$N_1 x_1 \equiv 2 \bmod 7 \qquad N_2 x_2 \equiv 4 \bmod 15$$

cioè: $15 x_1 \equiv 2 \bmod 7$, $7x_2 \equiv 4 \bmod 15$ (dato che 7x13=91≡1 mod15)
$x_1 \equiv 2 \bmod 7$, $x_2 \equiv 7 \bmod 15$ (13x4=52≡7mod 15)

da cui si ricava la X_0 :

$$X_0 = N_1 x_1 + N_2 x_2 = 15x2+7x7= 79.$$

Notiamo che questo metodo funziona se i divisori sono primi fra loro. (c'è un teorema ..)

La legione Z.
Di ritorno dalla faticosa campagna militare di Cesenaticus, la legione Zeta, agli ordini del console Mario Puppius, si ritrova con delle perdite: si tratta principalmente della gens "Boltionella", che si attarda abitualmente nelle taverne e nelle bettole per giocare alla LudoStationes. Il numero iniziale dei legionari era di 25mila. Ad una rapida occhiata, il console Mario si avvede che mancano all'appello alcune centinaia di soldati. Per procedere al conteggio utilizza il metodo delle file di diverso numero: basta contare i resti e in un attimo si saprà quanti sono i dispersi. I legionari, prontamente grazie all'addestramento, si dispongono in fila per 7 e ne restano fuori cinque. Si dispongono poi celermente in fila per 10, e ne restano nove. In fila per 11, e ne restano due, così

come due ne restano quando si dispongono in fila per 13. Quanti sono i dispersi ?

Soluzione
In questo caso le congruenze sono quattro e tanti dovranno essere i Numeroni:

$$x = 5 + n7 = 9 + m10 = 2 + p11 = 2 + q13$$

$$x \equiv 5 \bmod 7 \quad , \quad x \equiv 9 \bmod 10 \quad , \quad x \equiv 2 \bmod 11 \quad , \quad x \equiv 2 \bmod 13$$

$N_1 = 10x11x13 = 1430$, $N_2 = 7x11x13 = 1001$, $N_3 = 7x10x13 = 910$, $N_4 = 7x10x11 = 770$.

Le congruenze da risolvere saranno quindi:

$$N_1x_1 \equiv 5 \bmod 7 \quad , \quad N_2x_2 \equiv 9 \bmod 10 \quad , \quad N_3x_3 \equiv 2 \bmod 11 \quad , \quad N_4x_4 \equiv 2 \bmod 13$$

$$1430x_1 \equiv 5 \bmod 7 \quad , \quad 1001x_2 \equiv 9 \bmod 10 \quad , \quad 910x_3 \equiv 2 \bmod 11 \quad , \quad 770x_4 \equiv 2 \bmod 13$$

$$2x_1 \equiv 5 \bmod 7 \quad , \quad x_2 \equiv 9 \bmod 10 \quad , \quad 8x_3 \equiv 2 \bmod 11 \quad , \quad 3x_4 \equiv 2 \bmod 13$$
$$x_1 \equiv 6 \bmod 7 \quad , \quad x_2 \equiv 9 \bmod 10 \quad , \quad x_3 \equiv 3 \bmod 11 \quad , \quad x_4 \equiv 5 \bmod 13$$

Da cui si ricava la soluzione $X_0 = N_1x_1 + N_2x_2 + N_3x_3 + N_4x_4 =$
$= 1430x6 + 1001x9 + 910x3 + 770x5 = 24.169.$

l'unica possibilità minore di 25mila, quindi la soluzione cercata è 25000 – 24169 = **831 dispersi.**

Il teorema cinese del resto ha quindi questo enunciato.

TEOREMA
In un sistema di k congruenze, quando i divisori sono primi tra loro, la soluzione esiste. Anzi, ci sono infinite soluzioni, tutte distanti fra loro come il prodotto di questi divisori.

$$x \equiv a \bmod p_1 \quad , \quad x \equiv b \bmod p_2 \quad , \quad x \equiv c \bmod p_3 \quad .. \quad x \equiv k \bmod p_k$$

Ogni soluzione è del tipo: $\mathbf{X = X_0 + h \cdot p_1 \cdot p_2 \cdot p_3 \cdot .. \cdot p_k}$

e per trovare la soluzione "iniziale" X_0 occorre risolvere k congruenze:

$$N_1 x_1 \equiv a \bmod p_1 \quad , \quad N_2 x_2 \equiv b \bmod p_2 \quad , \quad N_3 x_3 \equiv c \bmod p_3 \quad , \quad .. \quad N_k x_k \equiv k \bmod p_k$$

dove i "numeroni" Ni sono i prodotti di tutti i p_i tranne uno (proprio quello della congruenza).

La soluzione iniziale, dopo aver trovato i valori di tutte le x_i, sarà infine:

$$\mathbf{X_0 = N_1 x_1 + N_2 x_2 + N_3 x_3 + .. + N_k x_k}$$

ESERCIZIO
Risolvere il sistema:

$$\begin{cases} x \equiv 2 \ (mod\ 5) \\ x \equiv 0 \ (mod\ 4) \\ x \equiv 4 \ (mod\ 7) \end{cases}$$