Esercizio 1. Utilizzando la dimostrazione del teorema cinese del resto determinare l'unica soluzione mod $385 = 5 \cdot 7 \cdot 11$ del sistema cinese

$$(1) \qquad \begin{cases} X \equiv 3(5) \\ X \equiv 4(7) \\ X \equiv 4(11) \end{cases}.$$

$R = 385$

1) $R_1 = 77$ hw $77t_1 + 5y_1 = 1 \Rightarrow 1 = 77(-2) + 5 \cdot (31)$ $\tilde{X}_1 = -2 \cdot 3$

2) $R_2 = 55$ hw $55t_2 + 7y_2 = 1 \Rightarrow 1 = 55 \cdot (-1) + 7 \cdot (8)$ $\tilde{X}_2 = -1 \cdot 4$

3) $R_3 = 35$ hw $35t_2 + 11y_2 = 1 \Rightarrow 1 = 35 \cdot (-5) + 11 \cdot (16)$ $\tilde{X}_3 = -5 \cdot 4$

$\tilde{X} = -6 \cdot 77 + (-4) \cdot 55 + (-20) \cdot 35 = -1382 = 158 \pmod{385}$

Esercizio 3. Ho comprato un grosso barattolo di caramelle; il negoziante mi ha assicurato che sono circa mille ma mi ha anche detto che se le metto in fila per 13 ne rimangono 11, se le metto in fila per 11 ne rimangono 7 e ne manca una per riuscire a metterle in fila per 7. Quante caramelle ci sono nel barattolo ?

$$\begin{cases} X = 11 \mod 13 \\ x = 7 \mod 11 \\ x = 1 \mod 7 \end{cases}$$

1) $R_1 = 77$ hw $1 = 77t_1 + 13y_1 \Rightarrow 1 = 77(-1) + 13(6)$ $\tilde{X}_1 = 11 \cdot (-1) = -11$

2) $R_2 = 91$ hw $1 = 91(4) + 11(-33)$ $\tilde{X}_2 = 7 \cdot 4 = 28$

3) $R_3 = 143$ hw $1 = 143(-2) + 7(41)$ $X_3 = 1 \cdot (-7) = -2$

$\tilde{X} = 77(-11) + 91 \cdot 28 + 143(-2) = -847 + 2548 - 286 = 1415 = 414 \mod (1001)$

Il negoziante è un truffatore.

Esercizio 4. Risolvere il sistema congruenziale

$$\begin{cases} 4X \equiv 2\,(22) \\ 3X \equiv 2\,(7) \end{cases}$$

$4x \equiv 2 \ (22)$, $MCD(4, 22) = 2$

$3x \equiv 2 \ (7)$, $MCD(3, 7) = 1$

$$\begin{cases} 2x \equiv 1 \ (11) & \text{moltiplico per } 6 \\ 3x \equiv 2 \ (7) & \text{moltiplico per } 5 \end{cases}$$

$$\begin{cases} x \equiv 6 \ (11) \\ x \equiv 10 \ (7) \end{cases}$$

1) $R_1 = 7$ hw $7(-3) + 11(2) = 1$ $\tilde{X}_1 = -3 \cdot 6 = (-18)$

2) $R_2 = 11$ hw $11(2) + 7(-3) = 1$ $\tilde{X}_2 = 2 \cdot 10 = 20$

$\tilde{X} = 7 \cdot (-18) + 11 \cdot 20 = 94 \pmod{77} = 17$

Esercizio 5. Risolvere il sistema congruenziale

$$\begin{cases} 18X \equiv 12(30) \\ 7X \equiv 4(9) \\ 28X \equiv 14(98) \end{cases}$$

1) MCD(18,30) = $30 = 18\cdot 1 + 12 \Rightarrow 18 = 12\cdot 1 + 6 \Rightarrow 12 = 6\cdot 2 + 0$ $\quad 6|12$

2) MCD(7,9) = 1 $\quad 1|4$

3) MCD(28,98) = $98 = 28\cdot 3 + 14 \Rightarrow 28 = 14\cdot 2 + 0$ $\quad 14|14$

$$\begin{cases} 3X \equiv 2 \ (5) \\ 7X \equiv 4 \ (9) \\ 2X \equiv 1 \ (7) \end{cases}$$ moltiplic. per gl. inversi $$\begin{cases} X \equiv 4 \ (5) \\ X \equiv 7 \ (9) \\ X \equiv 4 \ (7) \end{cases}$$

1) $R_1 = 63$ lw $1 = 63(2) + 5(-25)$ $\quad \tilde{X}_1 = 2\cdot 4 = 8$

2) $R_2 = 35$ lw $1 = 35(-1) + 9(4)$ $\quad \tilde{X}_2 = -1\cdot 7 = -7$

3) $R_3 = 45$ lw $1 = 45(5) + 7(-32)$ $\quad \tilde{X}_3 = 5\cdot 4 = 20$

$\tilde{X} = 63\cdot 8 + 35\cdot(-7) + 45(20) = 1159 \pmod{315} = 214$

Esercizio 6. È dato il sistema congruenziale dipendente dal parametro $a \in \mathbb{Z}$:

$$\begin{cases} 3X \equiv 4(10) \\ 2X \equiv 7(9) \\ 5X \equiv a(12) \end{cases}$$

Determinare per quali $a \in \mathbb{Z}$, $1 \le a \le 11$, tale sistema è compatibile. Per tali a risolvere il sistema.

Suggerimento: il metodo di sostituzione può essere utile ....

per essere trasformato in un sistema cinese, è necessario che gli argomenti dei moduli siano CO-PRIMI fra loro. 10 e 12 non lo sono! posso moltiplicare 12 o 10 per qualsiasi $k \in \mathbb{Z}$ ma resteranno sempre con MCD $\neq 1$. Questo sistema NON è risolvibile a cinese. divido per i rispettivi inversi

$$\begin{cases} X \equiv 8 \ (10) \\ X \equiv 8 \ (9) \\ X \equiv 5a \ (12) \end{cases}$$

posso considerare le eq. incompatibili equivalenti a:

$$\begin{cases} X \equiv 8 \ (10) \\ X \equiv 8 \ (9) \\ X \equiv 5a \ (12) \end{cases} \quad \begin{cases} X \equiv 8 \ (5) \\ X \equiv 8 \ (2) \end{cases} \quad \begin{cases} X \equiv 5a \ (4) \\ X \equiv 5a \ (3) \end{cases}$$

se $a \equiv 0 \ (2)$, posso eliminare $X \equiv 8 \ (2)$, e se $a \equiv 1 \ (3)$, posso eliminare $X \equiv 5a \ (3)$.

Il sistema ha sol. per $\begin{cases} a = 4 \\ a = 10 \end{cases}$

Esercizio 9. Utilizzando la seconda formulazione del teorema cinese del resto determinare il resto della divisione per 385 di 3^{302}.

So che $3^{302}(385) = 3^{302}(5) = 3^{302}(7) = 3^{302}(11)$

Applico il Teorema di Eulero

P = PRIMO SE K è MULTIPLO DI P-1, $K \equiv P-1\ (P)$, QUINDI: $a^{P-1}(P)$
$a^K(P)$ t. eulero $= a^{P-1}(P) \equiv 1\ (P)$

$3^{302}(5) = 3^{300} \cdot 3^2(5)$ se 300 è multiplo di $n-1 \Rightarrow$

$\Rightarrow$ 300 è multiplo di 4? SI $\Rightarrow 3^{300} = 1\ (5) \Rightarrow 3^{302}(5) = 9\ (5)$

$3^{302}(7) = 3^{300} \cdot 3^2(7)$ 300 è mult. di 6 $\Rightarrow 3^2(7) = 9\ (7)$

$3^{302}(11) = 3^{300} \cdot 9\ (11)$ 300 è mult. di 10 $\Rightarrow 9\ (11)$

$$3^{302} \equiv 9\ (385)$$

Esercizio 13. Siano $(G, \star_G)$ e $(H, \star_H)$ due gruppi. Verificate che il prodotto cartesiano $G \times H$ ha una naturale struttura di gruppo, $(G \times H, \star)$, rispetto all'operazione

$$(g, h) \star (g', h') := (g \star_G g', h \star_H h').$$

$(G \times H, \star)$ è detto *prodotto diretto di G ed H*.

φ è l'applicazione $(G, *_G) \times (H, *_H) \to (G \times H, *)$. presi due qualsiasi $g \in G$ e $h \in H$, la coppia $(g, h) \in G \times H$, che è il gruppo "immagine", φ è suriettiva, inoltre poi ogni distinta coppia $(g, h) \in G \times H$, è generata da distinti valori $g \in G$ e $h \in H$, è biettiva. quindi φ è un ISOMORFISMO.

$*$ è ben definita. SIA $g = g'$, $h = h'$, $K = K'$ e $F = F'$.

Deve valere che $(g, h) * (K, F) = (g' *_G K', h' *_G F')$

$$\left.\begin{array}{l} (g, h) * (K, F) = (g *_G K, h *_G F) \\ (g' *_G h', K' *_G F') = (g', h') * (K', F') = (g, h) * (K, F) \end{array}\right\} * \text{ è ben posta.}$$

Esercizio 16. Verificare che se A e B sono anelli commutativi unitari ed F è un isomorfismo di anelli allora $F(\mathcal{U}(A)) = \mathcal{U}(B)$.
(Vi ricordo che $\mathcal{U}(A)$ è il gruppo degli elementi invertibili di A.)
Verificare che

$$\mathcal{U}(A \times B) = \mathcal{U}(A) \times \mathcal{U}(B)\,.$$

Se F è un isomorfismo, è una applicazione biettiva, quindi $|A| = |B|$.

Se unità di A e B sono rispettivamente 1_A e 1_B.

$$\left.\begin{array}{l} F(1_A) = F(1_A \cdot_A 1_A) = F(1_A) \cdot_B F(1_A) \\ 1_B = (F(1_A))^{-1} \cdot_B F(1_A) = (F(1_A))^{-1} \cdot_B F(1_A) \cdot_B F(1_A) = F(1_A) \end{array}\right\} \Rightarrow F(1_A) = 1_B$$

Se $a \in \mathcal{U}(A)$, allora $F(a) \cdot_B F(a^{-1}) = F(a \cdot_A a^{-1}) = F(1_A) = 1_B$, se $b \in \mathcal{U}(B)$ allora $1_B = b \cdot_B b^{-1} \Rightarrow F(a) \cdot_B F(a^{-1}) = b \cdot_B b^{-1}$ $\forall (a,b) \in (\mathcal{U}(A) \times \mathcal{U}(B))$, dalla precedente biiettività si ha:

$$(F(a) = b \wedge F(a^{-1}) = b^{-1}) \vee (F(a) = b^{-1} \wedge F(a^{-1}) = b)$$

Un esempio di una cosa, un elemento di $\mathcal{U}(A)$ viene mandato in un elemento di $\mathcal{U}(B)$. ∎