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

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

$R=(5\cdot 7\cdot 11) \qquad R_1 = 77 \qquad R_2 = 55 \qquad R_3 = 35$

1- $\tilde{X}_1 = 77\cdot t_k + 5\cdot q_k \Rightarrow 77\cdot\underline{(-2)} + 5\cdot 31 \Rightarrow \tilde{X}_1 = (-2)\cdot 3 = -6$

2- $\tilde{X}_2 = 55\cdot t_k + 7\cdot q_k \Rightarrow 55\cdot\underline{(-1)} + 7\cdot 8 \Rightarrow \tilde{X}_2 = (-1)\cdot 4 = -4$

2- $\tilde{X}_3 = 35\, t_k + 11\cdot q_k \Rightarrow 35\cdot\underline{(-5)} + 11\cdot 16 \Rightarrow X_3 = (-5)\cdot 4 = -20$

$\tilde{X} = -6\cdot 77 - 4\cdot 55 - 20\cdot 35 = -462 - 220 - 700 = -1382\ (385) \equiv 158\ (385)$

Esercizio 2. Utilizzando un metodo di sostituzione trovare l'unica soluzione mod $385 = 5\cdot 7\cdot 11$ del sistema cinese (1).

Suggerimento. L'idea è di arrivare per successive sostituzioni ad una soluzione scritta nella forma $k + 5\cdot 7\cdot 11\ell$, $k < 385$, in modo tale che k sia l'unica soluzione cercata. Procedete come segue: la prima equazione ha soluzione generica $x = 3 + 5t_1$; sostituiamo questa soluzione generica nella seconda equazione; deve essere $3 + 5t_1 \equiv 4(7)$ che possiamo riscrivere come $5t_1 = 1(7)$. Ma 5 e 7 sono comprimi (è qui che utilizziamo l'ipotesi) e quindi 5 ammette un inverso moltiplicativo mod (7) e questo inverso è 3. Ne segue che $t_1 = 3(7)$ e cioè $t_1 = 3 + 7t_2$. Quindi

$$x = 3 + 5(3 + 7t_2) = 18 + 5\cdot 7t_2$$

(e ora il secondo addendo nel membro a destra fa comparire $5\cdot 7$). Sostituiamo ora questa espressione nella terza equazione......

$$\begin{cases} X \equiv 3\ (5) \Rightarrow X + 5Y = 1 \Rightarrow (x,y) = (6,-1) \Rightarrow (\tilde{x},\tilde{y}) = (18,-3) \Rightarrow (\underbrace{18 + t_1 5}_{x\,=\,3+5t_1}, -3-K) \\ X \equiv 4\ (7) \\ X \equiv 4\ (11) \end{cases}$$

$$\begin{cases} (3+5)t_1 \equiv 4\ (7) \Rightarrow 5t_1 \equiv 1\ (7) \Rightarrow t_1 \equiv 3\ (7) \Rightarrow t_1 = 3 + 7t_2 \\ (3+5)t_1 \equiv 4\ (11) \end{cases}$$

$X = 3 + 5(3 + 7t_2) = 3 + 15 + 5\cdot 7t_2 = 18 + 7\cdot 5\cdot t_2$

$\{18 + 35t_2 \equiv 4 \Rightarrow \{35t_2 \equiv -14\ (11) \Rightarrow \{2t_2 \equiv 8\ (11) \Rightarrow \{t_2 \equiv 4\ (11) \Rightarrow t_2 = 4 + 11t_3$

$X = 18 + 7\cdot 5\cdot(4 + 11t_3) = 18 + 7\cdot 5\cdot 4 + 385t_3 = 140 + 385t_3$

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 ?

$\begin{cases} x \equiv 11\ (13) \\ x \equiv 7\ (11) \\ x \equiv 6\ (7) \end{cases}$ posso applicare il teo. cinese $\Rightarrow R = 13\cdot 11\cdot 7 \Rightarrow$

$R_1 = 77$ risolvo $77t + 13K = 1 \Rightarrow t = (-1) \Rightarrow \tilde{x}_1 = -11 \equiv 2$

$R_2 = 91$ risolvo $91t + 11K = 1 \Rightarrow t = 4 \Rightarrow \tilde{x}_2 = 4\cdot 7 = 28 \equiv 6$

$R_3 = 143$ risolvo $143t + 7K = 1 \Rightarrow t = (-2) \Rightarrow \tilde{x}_3 = (-2)\cdot 6 = -12 \equiv 2$

$\tilde{x} = 77\cdot 2 + 91\cdot 6 + 143\cdot 2 = 154 + 546 + 286 = 986\ (\mathrm{mod}\ 1001)$

Esercizio 4. Risolvere il sistema congruenziale

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

$$\begin{cases} 4X \equiv 2\ (22) \\ 3X \equiv 2\ (7) \end{cases} \Rightarrow \begin{cases} 2X \equiv 1\ (11) \\ 3X \equiv 2\ (7) \end{cases} \Rightarrow \begin{cases} X \equiv 6\ (11) \\ X \equiv 10\ (7) \end{cases} \Rightarrow \begin{cases} X = 6 + 11\ell \\ 11\ell \equiv 4\ (7) \end{cases} \Rightarrow \begin{cases} X = 6 + 11(1+7t) \Rightarrow X = 17 + 77t \\ \ell \equiv 1\ (7) \Rightarrow \ell = 1 + 7t \end{cases}$$

Esercizio 5. Risolvere il sistema congruenziale

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

$$\begin{cases} 18X \equiv 12 \ (30) \\ 7X \equiv 4 \ (9) \\ 28X \equiv 14 \ (94) \end{cases} \quad \begin{matrix} MCD(18,30)=6 \\ \Rightarrow MCD(7,9)=1 \\ MCD(28,94)=2 \end{matrix} \Rightarrow \begin{cases} 3X \equiv 2 \ (5) \\ 7X \equiv 4 \ (9) \\ 14X \equiv 7 \ (47) \end{cases} \quad \begin{matrix} 3^{-1} \bmod 5 = 2 \\ 7^{-1} \bmod 9 = 4 \\ 14^{-1} \bmod 47 = 37 \end{matrix} \Rightarrow \begin{cases} X \equiv 4 \ (5) \\ X \equiv 7 \ (9) \\ X \equiv 24 \ (47) \end{cases} \quad R = 2115$$

$R_1 = 423 \Rightarrow 423 \cdot t + 5 \cdot K = 1 \Rightarrow 423 \cdot 2 + 5 \cdot (-169) \Rightarrow \tilde{X}_1 = 2 \cdot 4 = \underline{8}$

$R_2 = 235 \Rightarrow 235 \cdot t + 9 \cdot K = 1 \Rightarrow 235 \cdot 1 + 9 \cdot (-26) \Rightarrow \tilde{X}_2 = 1 \cdot 7 = \underline{7}$

$R_3 = 45 \Rightarrow 45 \cdot t + 47 \cdot K = 1 \Rightarrow 45 \cdot 23 + 47 \cdot (-22) \Rightarrow \tilde{X}_3 = 23 \cdot 24 = \underline{552}$

$$\tilde{X} = 8 \cdot 423 + 7 \cdot 235 + 552 \cdot 45 \pmod{2115} = 29869 \pmod{2115} = 259 \pmod{2115}$$

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 $a \in \mathbb{Z}$, $1 \leq a \leq 11$, tale sistema è compatibile. Per tali a risolvere il sistema.
Suggerimento: il metodo di sostituzione può essere utile ....

RIDUCO A CINESE

$$\begin{cases} X \equiv 8 \ (10) \\ X \equiv 8 \ (9) \\ X \equiv 5a \ (12) \end{cases} \Rightarrow \begin{cases} X = 8+10K \\ 8+10K \equiv 8 \ (9) \\ '' \end{cases} \Rightarrow \begin{cases} '' \\ 10K \equiv 0 \ (9) \\ '' \end{cases} \Rightarrow \begin{cases} X = 8+10 \cdot 9l \\ K = 9l \\ 8+10 \cdot 9l \equiv 5a \ (12) \end{cases}$$

$$\begin{cases} X = 8+10 \cdot 9l \\ K = 9l \\ 90l \equiv 5a-8 \ (12) \end{cases} \Rightarrow \begin{cases} '' \\ '' \\ 6l \equiv 5a-8 \ (12) \end{cases} \quad \text{AMMETTE SOL.} \Leftrightarrow \overset{6}{\overset{\shortparallel}{MCD(6,12)}} \text{ DIVIDE } 5a-8$$

$$\Leftrightarrow 5a-8 = 6 \cdot q \Leftrightarrow 5a \equiv 8 \ (6) \Rightarrow 5a \equiv 2 \ (6) \Rightarrow a \equiv 4 \ (6) \qquad a = 4+6t$$

ESSENDO $1 \leq a \leq 11$, IL SISTEMA È COMPATIBILE SE

$t=0 \Rightarrow a=4$ oppure $t=1 \Rightarrow a=10$.

Esercizio 7. Sia p un primo e sia $a \in \mathbb{N}$ tale che $1 \leq a < p^2$. Quali sono gli a privi di inverso aritmetico mod p^2 ?

Come prima cosa voglio capire se p^2 sia o no un primo, so che non lo e' perche' e' divisibile per 1, per se stesso, ma anche per p. Gli privi di inverso aritmetico, sono quelli NON-COPRIMI con p^2, ma abbiamo detto gia' quali sono i numeri che dividono p^2. L'unico a privo di inverso aritmetico e' $a = p$.

Esercizio 8. Sia $p > 2$ un primo. Determinare $\{x \in \mathbb{Z}_p : x^2 = 1\}$.

$\{x \in \mathbb{Z}_p \mid x^2 = 1\} = \{x \in \mathbb{Z}_p \mid x^{-1} = x\} = \{x \in \mathbb{Z}_p \mid x^2 = (K \cdot p)+1$ per qualche $K\}$

$x^2 = Kp+1 \Rightarrow x = \sqrt{Kp+1} \Leftrightarrow Kp+1$ e' un quadrato

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

$x = 3^{302}\ (385) \Rightarrow$

$385 = 11 \cdot 5 \cdot 7$

$$\begin{cases} x \equiv 3^{302}\ (11) \\ x \equiv 3^{302}\ (5) \\ x \equiv 3^{302}\ (7) \end{cases} \quad \begin{matrix} \varphi(11)=10 \\ \Rightarrow \varphi(5)=4 \\ \varphi(7)=6 \end{matrix} \quad \begin{cases} x \equiv (3^{10})^{30} \cdot 3^2\ (11) \\ x \equiv (3^4)^{75} \cdot 3^2\ (5) \\ x \equiv (3^6)^{50} \cdot 3^2\ (7) \end{cases} \Rightarrow \begin{cases} x \equiv 1^{30} \cdot 9\ (11) \\ x \equiv 1^{75} \cdot 9\ (5) \\ x \equiv 1^{50} \cdot 9\ (7) \end{cases}$$

teo di eulero

$$\begin{cases} x \equiv 9\ (5) & R_1 = 77 \\ x \equiv 9\ (7) & R_2 = 55 \\ x \equiv 9\ (11) & R_3 = 35 \end{cases} \Longrightarrow \begin{matrix} 77t + 5k = 1 \Rightarrow t = -7\ (5) = 3\ (5) \Rightarrow \tilde{x}_1 = 3 \cdot 9\ (5) = 2 \\ 55t + 7k = 1 \Rightarrow t = -1\ (7) = 6\ (7) \Rightarrow \tilde{x}_2 = 6 \cdot 9\ (7) = 5 \\ 35t + 11k = 1 \Rightarrow t = -5\ (11) = 6\ (11) \Rightarrow \tilde{x}_3 = 6 \cdot 9\ (11) = 10 \end{matrix}$$

$$\tilde{x} = 77 \cdot 2 + 55 \cdot 5 + 35 \cdot 10 = 779 \equiv 9\ (385)$$

Esercizio 10. Determinare il resto della divisione per 7 di $19^{19^{19}}$.

$$x \equiv 19^{19^{19}}\ (7) \qquad \varphi(7) = 6 \qquad 19^{19^{19}} = 19^{19^{6+6+6+1}} = 19^{19^6} \cdot 19^{19^6} \cdot 19^{19^6} \cdot 19^{19} =$$

$$= (19^6 \cdot 19^6 \cdot 19^6 + 19)^6 (19^6 \cdot 19^6 \cdot 19^6 + 19)^6 (19^6 \cdot 19^6 \cdot 19^6 + 19)^6 (19^6 \cdot 19^6 \cdot 19^6 + 19) \mod 7$$

$$\forall a \in \mathbb{Z},\ a^6\ (7) = 1 \Rightarrow (1 \cdot 1 \cdot 1 \cdot 19)^6 (1 \cdot 1 \cdot 1 \cdot 19)^6 (1 \cdot 1 \cdot 1 \cdot 19)^6 (1 \cdot 1 \cdot 1 \cdot 19) = 1 \cdot 1 \cdot 1 \cdot 19 = 19 \equiv 5 \mod 7$$

Esercizio 11. Un elemento a in un anello $(A, +, \cdot)$ è detto *nilpotente* se $\exists n \in \mathbb{N}$, $n > 0$, tale che $a^n = 0$.
(1) Sia A un anello commutativo. Verificare che la somma di due elementi nilpotenti è nilpotente.
(2) Verificare che l'unico nilpotente non-banale di $\mathbb{Z}_{60}$ è [30]

Siano a, b due NILPOTENTE $\quad a^n = 0 \quad b^m = 0$

$$a^n = 0 \Rightarrow a^n - (a^n) = 0 - a^n \Rightarrow 0 = 0 - a^n \Rightarrow -a^n = 0$$

Esercizio 12. Dimostrare che $\forall n \in \mathbb{N}$ il numero

$$n^{55} + 2n^{50} + 3n^{45} + 4n^3 + 5n^2 + 6n$$

è divisibile per 7.
Suggerimento: se n è divisibile per 7 il risultato è banalmente vero; supponiamo allora che $(n, 7) = 1$. Il piccolo teorema di Fermat può risultare utile.

$n^6 = 1\ (7)$

$$n^{55} + 2n^{50} + 3n^{45} + 4n^3 + 5n^2 + 6n =$$

$$n^{6 \cdot 9} \cdot n + 2 \cdot n^{6 \cdot 8} \cdot n^2 + 3 \cdot n^{6 \cdot 7} \cdot n^3 + 4n^3 + 5n^2 + 6^n$$

$$n + 2n^2 + 3n^3 + 4n^3 + 5n^2 + 6n = 7n + 7n^2 + 7n^3 = 7(n + n^2 + n^3) \equiv 0 \pmod 7$$

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*.

ASSOCIATIVITÁ

ASS.

$$(a, b) * (a', b') = (a *_G a', b *_H b') = (a' *_G a, b' *_H b) = (a', b') * (a, b)$$

ELEM. NEUT.

elem. neutro di $G \times H$

$$(a, b) * (e_G, e_H) = (a *_G e_G, b *_H e_H) = (a, b)$$

elem. neut. di G $\quad$ elem. neut. di H

INVERSO

$(a,b)*(a^{-1},b^{-1}) = (a *_G a^{-1}, b *_H b^{-1}) = (e_G, e_H)$

INV. DI a INV. DI b

Esercizio 14. Siano $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$ due anelli. Verificate che il prodotto cartesiano $A \times B$ ha una naturale struttura di anello, $(A \times B, +, \cdot)$, con le operazioni

$$(a,b) + (a',b') := (a +_A a', b +_B b'), \quad (a,b)\cdot(a',b') = (a \cdot_A a', b \cdot_B b').$$

$(A \times B, +, \cdot)$ è il prodotto diretto di A e B.
Verificate che se A e B sono commutativi unitari allora anche $A \times B$ lo è.

Un'applicazione $\phi : G \to H$ fra due gruppi è un omomorfismo di gruppi se $\forall g, g' \in G$.

$$\phi(g \star_G g') = \phi(g) \star_H \phi(g').$$

Se ϕ è bigettiva, allora ϕ è detto un **isomorfismo di gruppi**.

LA VERIFICA CHE $(A\times B, +)$ SIA UN GRUPPO COMM. E` ANALOGA ALL'ESERCIZIO 13.

DISTRIBUTIVITA'

$((a,b)+(a',b'))\cdot(a'',b'') = (a +_A a', b +_B b')\cdot(a'',b'') = ((a +_A a') \cdot_A a'', (b +_B b') \cdot_B b'')$

$= (a \cdot_A a'' + a' \cdot_A a'', b \cdot_B b'' +_B b' \cdot_B b'') = (a \cdot_A a'', b \cdot_B b'') + (a' \cdot_A a'', b' \cdot_B b'') = (a,b)\cdot(a'',b'') + (a',b')\cdot(a'',b'')$

IPOTESI AGGIUNTIVA: A e B sono commutativi

$(a,b)\cdot(a',b') = (a \cdot_A a', b \cdot_B b') = (a' \cdot_A a, b' \cdot_B b) = (a',b')\cdot(a,b)$

IPOTESI AGGIUNTIVA: A e B sono unitari

1_A e' l'unita' di A 1_B e' l'unita' di B l'unita' di $A\times B$ e' $(1_A, 1_B)$

$(a,b)\cdot(1_A,1_B) = (a \cdot_A 1_A, b \cdot_B 1_B) = (a,b)$

Esercizio 15. Abbiamo visto in classe che se ϕ è un omomorfismo allora $\phi(1_G) = 1_H$. Ricostruite la dimostrazione senza guardare gli appunti.
Dimostrate che $\phi(g^{-1}) = (\phi(g))^{-1}$.

- $\phi(1_G) = \phi(1_G *_G 1_G) = \phi(1_G) *_H \phi(1_G)$

$1_H = \phi(1_G)^{-1} * \phi(1_G)$

$\Rightarrow 1_H = \phi(1_G)^{-1} *_H \phi(1_G) *_H \phi(1_G) = 1_H = 1_H * \phi(1_G) = \phi(1_G)$

- $\phi(g^{-1}) = \phi(g^{-1}) * 1_H = \phi(g^{-1}) * \phi(g) * \phi(g)^{-1} = \phi(g^{-1} * g) * \phi(g)^{-1}$

$= \phi(1_G) * \phi(g)^{-1} = 1_H * \phi(g)^{-1} = \phi(g)^{-1}$

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

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

1) Sia $a \in \mathcal{U}(A)$ e sia $F(a) = b$ denoto F con ϕ

$1_B = \phi(1_A) = \phi(a \cdot a^{-1}) = \phi(a)\cdot\phi(a^{-1}) = \phi(a)\cdot\phi(a)^{-1}$

quindi se a e' invertibile, anche $\phi(a)$ lo e'.

2) Verifico per doppia inclusione, $\boxed{\mathcal{U}(A\times B) \subseteq \mathcal{U}(A)\times\mathcal{U}(B)}$: Sia $(a,b) \in \mathcal{U}(A\times B)$,

$\Rightarrow \exists (a,b)^{-1} \mid (a,b)\cdot(a,b)^{-1} = (1,1)$, tale $(a,b)^{-1}$ esiste ed e' $(a^{-1}, b^{-1}) \Rightarrow$

$(a,b)\cdot(a^{-1},b^{-1}) = (a\cdot a^{-1}, b\cdot b^{-1}) = (1,1) \Longleftrightarrow a \in \mathcal{U}(A) \wedge b \in \mathcal{U}(B) \Rightarrow (a,b) \in \mathcal{U}(A)\times\mathcal{U}(B)$.

$\boxed{\mathcal{U}(A)\times\mathcal{U}(B) \subseteq \mathcal{U}(A\times B)}$: Sia $(a,b) \in \mathcal{U}(A)\times\mathcal{U}(B) \Rightarrow a \in \mathcal{U}(A) \wedge b \in \mathcal{U}(B)$, definisco l'anello $(A\times B, +, \cdot) \Rightarrow$ Sia $(a,b) \in A\times B \Rightarrow (a,b) \in \mathcal{U}(A\times B) \Longleftrightarrow \exists (a,b)^{-1}$ ma questo esiste ed e' (a^{-1}, b^{-1}) dato che entrambi sono invertibili.