Corso di Laurea in Informatica
Algebra. a.a. 2023-24. Proff. P. Piazza e G. Viaggi
Compito a casa del 27/10/2023

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

$$\left\{ \begin{array}{l} X \equiv 3(5) \\ X \equiv 4(7) \\ X \equiv 4(11) \end{array} \right. . \tag{1}$$

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.....

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 ?

Esercizio 4. Risolvere il sistema congruenziale

$$\left\{ \begin{array}{l} 4X \equiv 2\,(22) \\ 3X \equiv 2\,(7) \end{array} \right.$$

Esercizio 5. Risolvere il sistema congruenziale

$$\left\{ \begin{array}{l} 18X \equiv 12(30) \\ 7X \equiv 4(9) \\ 28X \equiv 14(98) \end{array} \right.$$

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

$$\left\{ \begin{array}{l} 3X \equiv 4(10) \\ 2X \equiv 7(9) \\ 5X \equiv a(12) \end{array} \right.$$

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 ....

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 ?

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

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

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

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]

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.

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*.

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**.

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

Un'applicazione $F : A \to B$ fra due anelli $(A, +_A, \cdot_A)$ e $(B, +_B, \cdot_B)$ è un omomorfismo di anelli se

$$F(a +_A a') = F(a) +_B F(a')\,, \quad F(a \cdot_A a') = F(a) \cdot_B F(a').$$

Scriveremo spesso $+$ e $\cdot$ per le operazioni di A e B a meno che ciò generi confusione.
Si ha sempre: $F(0_A) = 0_B$. Se A e B sono unitari allora F è detto unitario se porta 1_A in 1_B [1].
Se F è bigettiva allora F è detto un **isomorfismo di anelli.**

[1] Non è automatico.....

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

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