Fondamenti di Aritmetica - Compito del 17/06/2008

COGNOME e NOME
MATRICOLA

Esercizio 1.
a. Dire per quali $a \in \mathbb{Z}$ la congruenza $35x \equiv 77 \pmod{a}$ ha soluzione.
b. Quale è il resto della divisione per 20 di $7^{5857561} - 5857561^7$?

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 15x \equiv 19 \pmod{161} \\ 40x \equiv 20 \pmod{345} \\ 3x \equiv 78 \pmod{1323} \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 1 a 26 rispettando l'ordine e si consideri il codice RSA a chiave pubblica $(n, v) = (253, 21)$.
a. Si calcoli l'esponente w per la decodifica.
b. Si codifichi la parola ESAME.

Esercizio 4. Siano $P, Q \in K[X]$ con K campo, tali che

$$P \equiv Q \pmod{X^2 - 2} \quad \text{e} \quad P \equiv Q \pmod{X^2 - 2X - 3} .$$

a. Con $K = \mathbb{Q}$, dimostrare che $P \equiv Q \pmod{(X^2 - 2)(X^2 - 2X - 3)}$ in $\mathbb{Q}[X]$.
b. Con $K = \mathbb{Z}/7\mathbb{Z}$, è vero che $P \equiv Q \pmod{(X^2 - 2)(X^2 - 2X - 3)}$ in $\mathbb{Z}/7\mathbb{Z}[X]$?

Esercizio 5. Si consideri l'anello $R = \mathbb{Z}_{11}[X]/(X^3 + 2X^2 + 3X + 6)$.
a. R è un campo ? Quanti sono gli elementi di R ?
b. Per ognuno dei seguenti elementi $Q \in R$ dire se è invertibile o un divisore di zero e trovare l'inverso o un elemento $S \in R - \{0\}$ tale che $QS = 0$ in R.
i) $Q = X^2 + 3$;
ii) $Q = X^2 - 3$;
iii) $Q = X^2 - 4$.

Fondamenti di Aritmetica - Compito del 14/07/2008

COGNOME e NOME
MATRICOLA

Esercizio 1.
a. Trovare tutte le soluzioni $x, y \in \mathbb{Z}$ dell'equazione $66x + 70y = 30$.
b. Trovare le soluzioni di $7^x \equiv -4 \pmod{13}$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 19x \equiv 18 \pmod{77} \\ 40x \equiv 46 \pmod{1274} \\ 41x \equiv 40 \pmod{143} \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e sia $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ definita da $f(x) = 7x - 2$ la chiave per la codifica.
a. Si calcoli f^{-1};
b. si decodifichi la parola CLPANUC.

Esercizio 4. Siano $P, Q \in \mathbb{Q}[X]$ tali che

$$P \equiv Q \pmod{X^4 - 4} .$$

Dire, giustificando la risposta, se le seguenti affermazioni sono vere o false.
a. P irriducibile $\Longrightarrow Q$ irriducibile.
b. $MCD(P, X^2 - 2) = MCD(Q, X^2 - 2)$.
c. L'equazione $PA + QB = X + 1$ ha soluzioni $A, B \in \mathbb{Q}[X]$.

Esercizio 5. Sia $P = X^4 - X^2 + 1 \in \mathbb{Z}_7[X]$ e sia $R = \mathbb{Z}_7[X]/(P)$.
a. R è un campo ? Quanti sono gli elementi di R ?
b. Per ognuno dei seguenti elementi $Q \in R$ dire se è invertibile o un divisore di zero e trovare l'inverso o un elemento $S \in R - \{0\}$ tale che $QS = 0$ in R.
i) $Q = X^2 + 2$;
ii) $Q = X^2 - 2$.

Fondamenti di Aritmetica - Compito del 15/09/2008

COGNOME e NOME
MATRICOLA

Esercizio 1.
a. Per quale $a \in \mathbb{N}$ il numero $(623a213)_7$ è divisibile per 8 ?
b. Dimostrare che, per ogni $n \in \mathbb{N}$, $n^7 - n^3$ è divisibile per 40.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 20x & \equiv & 17 & (\text{mod } 33) \\ 36x & \equiv & 68 & (\text{mod } 220) \\ 7x & \equiv & -29 & (\text{mod } 135) \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e sia $f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ definita da $f(x) = 15x + 4$ la chiave per la codifica.
a. Si calcoli f^{-1};
b. si decodifichi la parola XGCURUG.

Esercizio 4. Siano $P, Q \in \mathbb{Q}[X]$ tali che

$$P(X) \cdot (X^2 - 5X + 6) + Q(X) \cdot (X^2 - 6X + 8) = X^2 - 4 .$$

Dire, giustificando la risposta, se le seguenti affermazioni sono vere o false.
a. $MCD(P, Q) = X^2 - 4$.
b. $P(-2) = 0 \Longrightarrow MCD(P, Q) = X + 2$.
c. $P(-2) \neq 0 \Longrightarrow MCD(P, Q) = 1$.

Esercizio 5. Sia $P = X^3 - 21X^2 + 9X - 12 \in K[X]$ con K campo.
a. Con $K = \mathbb{Z}_7$, l'anello $\mathbb{Z}_7[X]/(P)$ è un campo ?
b. Con $K = \mathbb{Q}$, l'anello $\mathbb{Q}[X]/(P)$ è un campo ?
c. Trovare l'inverso di $X^2 - 1$ in $\mathbb{Z}_7[X]/(P)$.