Fondamenti di Aritmetica - Compito del 25/06/2009

COGNOME e NOME
MATRICOLA

Esercizio 1.
a. Calcolare l'ordine di 4 in $(\mathbb{Z}_{101})^*$.
b. Trovare le soluzioni $(x, y) \in \mathbb{Z}^2$ dell'equazione $1443x - 7410y = 351$.
c. Trovare a tale che $7|(612a3420)_8$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 15x & \equiv & 30 & (\text{mod } 55) \\ 25x & \equiv & 28 & (\text{mod } 33) \\ 28x & \equiv & 31 & (\text{mod } 45) \end{cases} .$$

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. verificare che f è invertibile e calcolare f^{-1};
b. decodificare la parola NCAEYLL.

Esercizio 4. Siano P, $Q \in K[X] - \{0\}$ con K campo tali che $MCD(P, Q) = X^2 - 1$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere e quali false:
a. se $K = \mathbb{Q}$ allora P e Q non hanno radici multiple;
b. se $K = \mathbb{Z}_2$ allora P e Q hanno radici multiple;
c. se $K = \mathbb{Z}_2$ allora $(X - 1)^2 \mid MCD(P', Q')$ (dove P' e Q' sono le derivate prime di P e Q).

Esercizio 5. Si consideri l'anello $R = K[X]/(X^4 + 10X^2 + 5)$ con K campo.
a. Se $K = \mathbb{Q}$, R è un campo ?
b. Se $K = \mathbb{Z}_{11}$, R è un campo ?
c. Sia $K = \mathbb{Z}_{11}$. 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) $Q = X^2 + 1$;
iii) $Q = X^2 + 2$.

Fondamenti di Aritmetica - Compito del 20/07/2009

COGNOME e NOME
MATRICOLA

Esercizio 1.
a. Per quali $a \in \mathbb{Z}$ l'equazione $65x \equiv 91 \pmod{a}$ ha soluzioni ?
b. Trovare le soluzioni $(x, y) \in \mathbb{Z}^2$ dell'equazione $1369x + 7104y = -407$.
c. Trovare le soluzioni di $5^x \equiv 2 \pmod{17}$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 3x & \equiv & 2 \pmod{91} \\ 9x & \equiv & -8 \pmod{112} \\ 5x & \equiv & 12 \pmod{52} \end{cases}.$$

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 $f(x) = 11x - 7$ la chiave per la codifica.
a. verificare che f è invertibile e calcolare f^{-1};
b. decodificare la parola ZFEYDPZ.

Esercizio 4. Siano $P, Q \in K[X] - \{0\}$ con K campo tali che esistono $R, S \in K[X]$ con $PR + QS = X^2 + 8X - 3$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere e quali false:
a. se $K = \mathbb{Q}$, se P è irriducibile e $MCD(P, Q) \neq 1$ allora $P = X^2 + 8X - 3$;
b. se $K = \mathbb{Q}$ allora P e Q non hanno radici in comune in $\mathbb{Q}$;
c. se $K = \mathbb{Z}_5$, se P è irriducibile e $MCD(P, Q) \neq 1$ allora $P = X^2 + 8X - 3$;
d. se $K = \mathbb{Z}_5$ allora P e Q non hanno radici in comune in $\mathbb{Z}_5$.

Esercizio 5. Si consideri l'anello $R = K[X]/(X^4 + 6X^2 - 6)$ con K campo.
a. Se $K = \mathbb{Q}$, R è un campo ?
b. Se $K = \mathbb{Z}_{11}$, R è un campo ?
c. Trovare, se esiste, l'inverso di $X^2 + X + 1$ in $\mathbb{Z}_{11}[X]/(P)$.

Fondamenti di Aritmetica - Compito del 23/09/2009

COGNOME e NOME
MATRICOLA

Esercizio 1.
a. Per quali $a \in \mathbb{Z}$ l'equazione $ax \equiv 65 \pmod{39}$ ha soluzioni ?
b. Trovare le soluzioni di $4^x \equiv 6 \pmod{19}$.
c. Per quale $a \in \{0, 1, \ldots, 9\}$ il numero $8127a367$ è divisibile per 101 ?

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 4x \equiv -147 \pmod{405} \\ 6x \equiv 47 \pmod{55} \\ 80x \equiv 84 \pmod{396} \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e sia $(n = 377, e = 317)$ la chiave pubblica di un codice RSA.
a. Calcolare l'esponente d necessario per la decodifica.
b. Decodificare la lettera T.

Esercizio 4. Siano $P, Q \in K[X] - \{0\}$ con K campo e sia $I = \{PR + QS$ con $R, S \in K[X]\}$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere e quali false:
a. se P e Q sono irriducibili allora $I = K[X]$;
b. se $Q = P'$ (dove P' è la derivata prima di P) allora $I = K[X]$;
c. se P e Q hanno radici in comune in K allora $I \neq K[X]$;
d. se $I = K[X]$ allora $MCD(P, Q) = 1$.

Esercizio 5. Si consideri l'anello $R = K[X]/(X^4 - 14X^2 + 26)$ con K campo.
a. Se $K = \mathbb{Q}$, R è un campo ?
b. Se $K = \mathbb{Z}_{11}$, R è un campo ?
c. Sia $K = \mathbb{Z}_{11}$. 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) $Q = X^3 + X^2 + 5X - 6$.