Fondamenti di Aritmetica - Compito del 25/06/2007

COGNOME e NOME
MATRICOLA

Esercizio 1.
a) Dire per quali $a \in \mathbb{Z}$ l'equazione $33x + ay = 22$ ha soluzioni x, $y \in \mathbb{Z}$.
b) Calcolare il resto della divisione di $1234^{4321} - 4321^{1234}$ per 13.
c) Trovare due distinte fattorizzazioni di $X^2 + 7$ in $\mathbb{Z}/16\mathbb{Z}[X]$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 11x & \equiv & 6 & (\text{mod } 48) \\ 15x & \equiv & 10 & (\text{mod } 20) \\ -5x & \equiv & 14 & (\text{mod } 28) \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e sia $f : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ definita da $f(x) = 9x + 5$ la chiave per la codifica.
a) Si calcoli f^{-1};
b) si decodifichi la parola KFCBAF.

Esercizio 4. Siano P, Q, R, $S \in \mathbb{Q}[X] - \{0\}$ tali che $PR + QS = X^2 - 1$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
a) $MCD(P, Q) = X^2 - 1$;
b) $MCD(P, Q)$ divide $X^2 - 1$;
c) se P è irriducibile allora $P = X - 1$ o $P = X + 1$;
d) se P è irriducibile e P divide Q allora $P = X - 1$ o $P = X + 1$.

Esercizio 5. Si consideri l'anello $R = \mathbb{Z}/5\mathbb{Z}[X]/(X^4 + 1)$.
a) 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) $Q = X^2 + 1$;
iii) $Q = X^3 + X^2 + 3X + 3$.
b) R è un campo ? Quanti sono gli elementi di R ?

Fondamenti di Aritmetica - Compito del 19/07/2007

COGNOME e NOME
MATRICOLA

Esercizio 1.
a) Trovare a tale che $8|(521a362)_7$.
b) Dimostrare che 25 divide $n^{22} - n^2$ per ogni $n \in \mathbb{Z}$.
c) Risolvere $3^x \equiv 5 \pmod{11}$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 20x & \equiv & 9 & (\text{mod } 91) \\ 20x & \equiv & 15 & (\text{mod } 45) \\ 5x & \equiv & -3 & (\text{mod } 21) \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e si consideri il codice RSA definito dalla coppia $(101, 13)$.
a) Si calcoli l'esponente necessario per la decodifica.
b) Codificare la parola MESE.

Esercizio 4. Siano $P \in \mathbb{Q}[X]$ e sia P' la sua derivata. Supponiamo che $MCD(P, P') = X^2 + 2$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
a) P e P' hanno radici in comune in $\mathbb{Q}$;
b) P e P' hanno radici in comune in $\mathbb{C}$;
c) P non è irriducibile in $\mathbb{Q}[X]$;
d) P' è irriducibile in $\mathbb{Q}[X]$.

Esercizio 5. Si consideri il polinomio $P = X^4 - 2X^2 + 3$.
a) L'anello $\mathbb{Z}/7\mathbb{Z}[X]/(P)$ è un campo ?
b) L'anello $\mathbb{Z}/11\mathbb{Z}[X]/(P)$ è un campo ?
c) Trovare l'inverso di $X^2 - X - 1$ in $\mathbb{Z}/7\mathbb{Z}[X]/(P)$.

Fondamenti di Aritmetica - Compito del 20/09/2007

COGNOME e NOME
MATRICOLA

Esercizio 1.
a) Dire per quali $a \in \mathbb{Z}$ l'equazione $35x + ay = 10$ ha soluzioni x, $y \in \mathbb{Z}$.
b) Calcolare l'ordine di -18 in $(\mathbb{Z}/131\mathbb{Z})^*$. (Ricordare che se $a^n = 1$ allora l'ordine di a divide n)
c) Trovare, se esiste, a tale che $8|(21a02)_3$.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 11x & \equiv & 13 & (\text{mod } 35) \\ 7x & \equiv & 56 & (\text{mod } 175) \\ 6x & \equiv & 8 & (\text{mod } 55) \end{cases} .$$

Esercizio 3. Si facciano corrispondere le lettere dell'alfabeto inglese ai numeri da 0 a 25 rispettando l'ordine e sia $f : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ definita da $f(x) = 7x + 5$ la chiave per la codifica.
a) Si calcoli f^{-1};
b) si decodifichi la parola FSHEEZ.

Esercizio 4. Sia $P \in \mathbb{Z}/13\mathbb{Z}[X]/(X^3 + 7X^2 - X + 5)$ con $P \neq 0$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
a) se P è invertibile allora non ha radici multiple;
b) se P è divisore di zero allora non ha radici multiple;
c) P è invertibile se e solo se $P(2) \neq 0$;
d) P è divisore di zero se e solo se $P(2) = 0$.
(Sugg. trovare la fattorizzazione di $X^3 + 7X^2 - X + 5$ in $\mathbb{Z}/13\mathbb{Z}[X]$)

Esercizio 5. Si consideri il polinomio $P = X^4 - 14X^2 + 35X + 14$.
a) $\mathbb{Q}[X]/(P)$ è un campo ?
b) $\mathbb{Z}/5\mathbb{Z}[X]/(P)$ è un campo ? Quanti elementi ha ?
c) Trovare l'inverso di $X^2 + 3$ in $\mathbb{Q}[X]/(P)$.

Fondamenti di Aritmetica - Compito del 17/03/2008
Riservato ai Fuori Corso

COGNOME e NOME
MATRICOLA

Esercizio 1.
a) Risolvere $2^x \equiv -1 \pmod{11}$.
b) Trovare a tale che $(1523a66)_8$ sia divisibile per 9.

Esercizio 2. Trovare le soluzioni del seguente sistema di congruenze

$$\begin{cases} 3x \equiv -5 \pmod{77} \\ 12x \equiv 6 \pmod{50} \\ 4x \equiv -3 \pmod{55} \end{cases}.$$

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 $f(x) = 7x + 3$ la chiave per la codifica.
a) Si verifichi che f è invertibile e si calcoli f^{-1}.
b) Si decodifichi la parola CDNSD.

Esercizio 4. Sia $P = X^3 - 6X^2 + 11X - 6 \in \mathbb{Q}[X]$ e sia $Q \in \mathbb{Q}[X]$ tale che $MCD(P, Q) = X - 1$. Dire, giustificando le risposte, quali delle seguenti affermazioni sono vere:
a) $Q(2) = 0$ o $Q(3) = 0$;
b) $Q(2) = 0$ e $Q(3) = 0$;
c) esistono polinomi $R, S \in \mathbb{Q}[X]$ tali che $PR + QS = X^6 - 5X^5 - 3$;
d) Q è irriducibile.

Esercizio 5. Si consideri il polinomio $P(X) = X^3 - 12X + 7$.
a) Fattorizzare P in $\mathbb{Z}_2[X]$, $\mathbb{Z}_3[X]$ e $\mathbb{Z}_5[X]$.
b) Si dica, motivando la risposta, se $\mathbb{Q}[X]/(P)$ è un campo.
c) Trovare l'inverso di $X + 2$ in $\mathbb{Q}[X]/(P)$.