Università degli Studi Roma Tre
Corso di Laurea Triennale in Matematica, a.a. 2006/2007
AL1 - Algebra 1, fondamenti
Seconda prova di valutazione intermedia
11 Gennaio 2006

*Cognome*_________________ *Nome*_________________

*Numero di matricola*_________________________

Avvertenza: Svolgere il maggior numero di esercizi nello spazio assegnato, senza consegnare altri fogli e giustificando tutte le affermazioni fatte. Non è consentito l'uso di libri, appunti e calcolatrici.

Esercizio 1. Determinare la decomposizione in cicli disgiunti, l'ordine e la parità delle seguenti permutazioni di S_9:
$\sigma = (2345) \circ (35) \circ (479) \circ (218)$;
$\tau = (48) \circ (23) \circ (267) \circ (436) \circ (2357)$

SOLUZIONE

$\sigma = (1832) \circ (4795)$ è una permutazione pari (è prodotto di due cicli dispari) e ha ordine 4 (il minimo comune multiplo delle lunghezze dei suoi cicli disgiunti).
$\tau = (17684) \circ (35)$ è dispari e ha ordine 10.

Esercizio 2. Risolvere il seguente sistema di congruenze lineari:

$$\begin{cases} 2X \equiv 10 \pmod{14} \\ 6X \equiv 8 \pmod{22} \end{cases}$$

Stabilire inoltre in quante classi modulo 308 si ripartiscono le soluzioni.

SOLUZIONE

Le soluzioni in $\mathbb{Z}$ del sistema dato sono le stesse del sistema:

$$\begin{cases} X \equiv 5 \,(\mathrm{mod}\ 7) \\ 3X \equiv 4 \,(\mathrm{mod}\ 11) \end{cases}$$

che è equivalente a

$$\begin{cases} X \equiv 5 \,(\mathrm{mod}\ 7) \\ X \equiv 5 \,(\mathrm{mod}\ 11) \end{cases}$$

Quest'ultimo sistema ha un'unica soluzione (mod 77) per il teorema cinese del resto.

Chiaramente una soluzione intera è 5, e allora tutte le soluzioni in $\mathbb{Z}$ sono gli interi del tipo

$$5 + 77h, \quad h \in \mathbb{Z}.$$

Poiché $308 = 4 \cdot 77$, Le soluzioni distinte (mod 308) sono 4 e precisamente $5, 82, 159, 236$. Esse si ottengono per $h = 0, 1, 2, 3$.

Esercizio 3. Determinare quanti sono gli elementi invertibili di $\mathbb{Z}_{169}$. Stabilire se le classi di 12 e 13 sono invertibili in $\mathbb{Z}_{169}$ e in caso affermativo determinare le loro classi inverse, illustrando il procedimento seguito.

SOLUZIONE

Gli elementi invertibili di $\mathbb{Z}_{169}$ sono le classi dei numeri interi coprimi con 169 e quindi il loro numero è

$$\varphi(169) = \varphi(13^2) = 13^2 - 13 = 156,$$

dove φ è la funzione di Eulero. Dato che $MCD(13, 169) = 13 \neq 1$, la classe di 13 non è invertibile. La classe di 12 invece è invertibile e, poiché

$$169 = 12 \cdot 14 + 1,$$

il suo inverso è la classe di -14, ovvero la classe di 155.

Esercizio 4. Determinare la classe di polinomi associati a 53750 in $\mathbb{Z}[X]$ e in $\mathbb{Q}[X]$.

SOLUZIONE

Dato che

$$U(\mathbb{Z}[X]) = U(\mathbb{Z}) = \{1, -1\},$$

i polinomi associati a 53750 in $\mathbb{Z}[X]$ sono 53750 e -53750.

Inoltre, dato che

$$U(\mathbb{Q}[X]) = U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\},$$

l'insieme dei polinomi associati a 53750 in $\mathbb{Q}[X]$ è

$$\{\alpha \cdot 53750, \alpha \in \mathbb{Q} \setminus \{0\}\} = \mathbb{Q} \setminus \{0\}.$$

Esercizio 5. Dati i polinomi

$$f(X) = X^4 + X^3 + \overline{3}X^2 + \overline{2}X + \overline{2}\,; \quad g(X) = X^3 + \overline{2}X^2 + \overline{2}X + \overline{1}$$

di $\mathbb{Z}_5[X]$, determinare, con l'algoritmo euclideo delle divisioni successive, il massimo comune divisore monico di $f(X)$ e $g(X)$ e un'identità di Bezout per esso.

SOLUZIONE

Il massimo comune divisore monico di $f(X)$ e $g(X)$ è il polinomio monico associato all'ultimo resto non nullo nell'algoritmo euclideo delle divisioni successive. In questo caso si ha:

$$f(X) = (X+4)g(X) + (3X^2 + 3X + 3)\,; g(X) = (3X^2 + 3X + 3)(2X + 2).$$

Allora

$$MCD(f(X), g(X)) = X^2 + X + 1.$$

Da $f(X) = (X+4)g(X) + (3X^2 + 3X + 3)$ si ricava una identità di Bezout:

$$X^2 + X + 1 = 2f(X) - 2(X+4)g(X).$$

Esercizio 6. Determinare le radici razionali del polinomio

$$f(X) = 2X^4 - 5X^3 + 4X^2 - 5X + 2.$$

Determinare poi i fattori irriducibili di $f(X)$ in $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X], \mathbb{C}[X]$.

SOLUZIONE

Se il numero razionale $\frac{a}{b}$ è radice di $f(X)$, a divide $c_0 = 2$ e b divide $c_n = 2$. Quindi le possibili radici razionali di $f(X)$ sono $\alpha = \pm 1, \pm 2, \pm\frac{1}{2}$. Dividendo $f(X)$ per $X - \alpha$, si vede che $\frac{1}{2}$ e 2 sono radici. Inoltre risulta

$$f(X) = (X - \frac{1}{2})(X - 2)(2X^2 + 2).$$

Poiché $X^2 + 1$ è irriducibile su $\mathbb{R}$,

$$f(X) = (2X - 1)(X - 2)(X^2 + 1)$$

è una fattorizzazione in polinomi irriducibili in $\mathbb{Z}[X], \mathbb{Q}[X], \mathbb{R}[X]$. Invece una fattorizzazione in $\mathbb{C}[X]$ è

$$f(X) = (2X - 1)(X - 2)(X + i)(X - i).$$

Esercizio 7. Sia $f(X) \in \mathbb{Z}[X]$. Stabilire se le seguenti affermazioni sono vere o false, motivando brevemente le risposte:

(a) L'anello $\mathbb{Z}_n$ è un campo per ogni $n \geq 2$.
(b) Se p è un numero primo e p non divide il prodotto ab, con $a, b \in \mathbb{Z}$, allora p non divide né a né b.

Sia $f(X)$ un polinomio a coefficienti interi:

(c) Se $f(X)$ non ha radici intere allora non ha fattori di primo grado in $\mathbb{Z}[X]$.
(d) Se $f(X)$ ha un fattore proprio in $\mathbb{Z}[X]$ allora ha un fattore proprio in $\mathbb{Q}[X]$.
(e) Se $f(X)$ ha un fattore proprio in $\mathbb{Q}[X]$ allora ha un fattore proprio in $\mathbb{Z}[X]$.
(f) Se $f(X)$ è primitivo, allora ogni suo fattore in $\mathbb{Z}[X]$ è primitivo.

SOLUZIONE

(a) FALSA: L'anello $\mathbb{Z}_n$ è un campo se e soltanto se n è un numero primo. Altrimenti $\mathbb{Z}_n$ ha zerodivisori.

(b) VERA: Questo è vero per ogni numero intero n non necessariamente primo. Infatti, se n divide a o/e b, allora n divide ab.

(c) FALSA: Il polinomio $g(X) := (X - \frac{1}{2})(2X^2 + 2)$ non ha radici razionali, ma $g(X) := (2X - 1)(X^2 + 1)$ ha un fattore di primo grado in $\mathbb{Z}[X]$ (vedi l'Esercizio 6).

(d) FALSA: I numeri interi diversi da ± 1 possono essere fattori propri di $f(X)$ in $\mathbb{Z}[X]$, ma sono invertibili in $\mathbb{Q}[X]$. Ad esempio $2X$ è riducibile su $\mathbb{Z}$ ma irriducibile su $\mathbb{Q}$.

(e) VERA: I fattori propri di $f(X)$ in $\mathbb{Q}[X]$ sono polinomi di grado positivo e per il Lemma di Gauss i denominatori si possono sempre cancellare (vedi anche (c)). Ad esempio,

$$6X^2 - 5X + 1 = 6(X - \frac{1}{2})(X - \frac{1}{3}) = (2X - 1)(3X - 1).$$

(f) VERA: Il Lemma di Gauss asserisce che, se $f(X) = g(X)h(X)$ allora $c(f) = c(g)c(h)$. Quindi $c(f) = 1$ se e soltanto se $c(g) = 1 = c(h)$.