**Università degli Studi Roma Tre**
**Corso di Laurea Triennale in Matematica, a.a. 2009/2010**
**AL110 - Algebra 1**
**Soluzioni della seconda prova di valutazione intermedia**
**11 gennaio 2010**

*Cognome*____________________ *Nome*________________________

*Numero di matricola*____________________

**Avvertenza:** Svolgere ogni esercizio nello spazio assegnato, senza consegnare altri fogli e **giustificando tutte le affermazioni fatte**. Non è consentito l'uso di libri, appunti. E' consentito l'uso della calcolatrice.

1. (a) Determinare tutte le eventuali soluzioni distinte della seguente congruenza lineare:

$$234X \equiv 114 \pmod{102}$$

(b) Determinare tutte le eventuali soluzioni distinte del seguente sistema di congruenze lineari:

$$\begin{cases} 3X \equiv 2 & \pmod 5 \\ 81X \equiv 6 & \pmod 7 \\ 11X \equiv 15 & \pmod 8 \\ 6X \equiv 3 & \pmod 9 \end{cases}$$

*Soluzione*

(a) La congruenza data è equivalente alla congruenza $30X \equiv 12 \pmod{102}$; poiché $30 = 2 \cdot 3 \cdot 5$ e $102 = 2 \cdot 3 \cdot 17$, si ha che $\mathrm{MCD}(30, 102) = 6$; essendo 6 un divisore di 12, la congruenza data è risolubile e possiede 6 soluzioni non congruenti mod 102; consideriamo la congruenza $5X \equiv 2 \pmod{17}$; una soluzione è $x = 14$; le soluzioni distinte della congruenza data sono del tipo $14 + k17$ con $0 \leqslant k \leqslant 5$; in conclusione, le soluzioni distinte della congruenza data sono $14,\ 14 + 17 = 31,\ 31 + 17 = 48,\ 48 + 17 = 65,\ 65 + 17 = 82,\ 82 + 17 = 99$.

(b) Il sistema dato è equivalente al sistema:

$$\star \begin{cases} 3X \equiv 2 \pmod 5 \\ 4X \equiv 6 \pmod 7 \\ 3X \equiv 7 \pmod 8 \\ 6X \equiv 3 \pmod 9 \end{cases}$$

Ogni congruenza del sistema $\star$ è risolubile poiché MCD$(5,3) = 1$ =MCD$(7,4) =$

=MCD$(8,3)$ e MCD$(6,9) = 3|3$; per il teorema cinese dei resti il sistema $\star$ ha 3 soluzioni non congruenti modulo $5 \cdot 7 \cdot 8 \cdot 9$.
Consideriamo il sistema

$$\star\star \begin{cases} X \equiv 4 \pmod 5 \\ X \equiv 5 \pmod 7 \\ X \equiv 5 \pmod 8 \\ X \equiv 2 \pmod 3 \end{cases}$$

$N_1 = 7 \cdot 8 \cdot 3 = 168$; $N_1 \equiv 3 \pmod 5$; pertanto un inverso aritmetico di $N_1$ modulo 5 è $x_1 = 2$.
$N_2 = 5 \cdot 8 \cdot 3 = 120$; $N_2 \equiv 1 \pmod 7$; pertanto un inverso aritmetico di $N_2$ modulo 7 è $x_2 = 1$.
$N_3 = 5 \cdot 7 \cdot 3 = 105$; $N_3 \equiv 1 \pmod 8$; pertanto un inverso aritmetico di $N_3$ modulo 8 è $x_3 = 1$.
$N_4 = 5 \cdot 7 \cdot 8 = 280$; $N_4 \equiv 1 \pmod 3$; pertanto un inverso aritmetico di $N_4$ modulo 5 è $x_4 = 1$.
Pertanto:

$$x = 4 \cdot 2 \cdot 168 + 5 \cdot 1 \cdot 120 + 5 \cdot 1 \cdot 105 + 2 \cdot 1 \cdot 280 = 1344 + 600 + 525 + 560 \equiv 509 \pmod{840}$$

è l'unica soluzione mod 840 del sistema $\star\star$
Pertanto

$$\{y \in \mathbb{Z} \mid y \text{ è soluzione del sistema } \star\} = \{z \in \mathbb{Z} \mid z \text{ è soluzione del sistema } \star\star\} =$$
$$= \{509 + k840 \mid k \in \mathbb{Z}\}$$

Quindi le soluzioni del sistema dato non congruenti mod $5 \cdot 7 \cdot 8 \cdot 9 =$ 2520 sono:

$$509, \qquad 509 + 840 = 1349, \qquad 1349 + 840 = 2189$$

2. Nell'insieme $\mathbb{R}^\star = \mathbb{R} - \{0\}$ si consideri la seguente operazione:

$$a \diamond b = |a|b.$$

   (a) Stabilire se $\diamond$ è associativa.
   (b) Stabilire se $\diamond$ è commutativa.
   (c) Stabilire se esiste un elemento neutro rispetto a $\diamond$.
   (d) Provare che:
      i. esiste un elemento neutro sinistro per $\diamond$, cioè esiste $e_s \in \mathbb{R}^\star$ tale che $e_s \diamond x = x$ per ogni $x \in \mathbb{R}^\star$;
      ii. ogni elemento $a \in \mathbb{R}^\star$ possiede un inverso destro rispetto a $e_s$, cioè per ogni $a \in \mathbb{R}^\star$ esiste $\hat{a} \in \mathbb{R}^\star$ tale che $a \diamond \hat{a} = e_s$.

*Soluzione*

   (a) Comunque siano $a, b, c \in \mathbb{R}^\star$ si ha

$$(a \diamond b) \diamond c = (|a|b) \diamond c = ||a|b|c = |ab|c$$

$$a \diamond (b \diamond c) = a \diamond (|b|c) = |a||b|c = |ab|c$$

   quindi $\diamond$ è associativa.

   (b) $\diamond$ non è commutativa: ad esempio

$$(-2) \diamond 5 = 10 \qquad \text{e} \qquad 5 \diamond (-2) = 5(-2) = -10$$

   (c) Supponiamo che esista $u \in \mathbb{R}^\star$ tale che $u \diamond a = a \diamond u = a$ per ogni $a \in \mathbb{R}^\star$; per $a = 1$ si avrebbe $u \diamond 1 = |u| = 1$ da cui $u = 1$ oppure $u = -1$;
   1 non è elemento neutro: $(-2) \diamond 1 = 2 \neq -2$;
   $-1$ non è elemento neutro: $2 \diamond (-1) = -2 \neq 2$.

   (d) 1 è tale che $1 \diamond x = x$ per ogni $x \in \mathbb{R}^\star$; inoltre per ogni $a \in \mathbb{R}^\star$ esiste $\hat{a} \in \mathbb{R}^\star$ tale che $a \diamond \hat{a} = 1$:
   se $a > 0$ si ha $\hat{a} = a^{-1}$: $a \diamond a^{-1} = aa^{-1} = 1$;
   se $a < 0$ si ha $\hat{a} = -a^{-1}$: $a \diamond (-a^{-1}) = |a|(-a^{-1}) = (-a)(-a^{-1}) = 1$.
   Analogamente per $-1$.

3. Sia $\sigma := (234) \circ (456) \circ (561) \circ (2376) \in S_7$.

   (a) Scrivere $\sigma$ come prodotto di cicli disgiunti, determinarne l'ordine e la parità. Calcolare $\sigma^4$.
   (b) Sia $\tau := (3567) \in S_7$. Calcolare $(\tau \circ \sigma)^{-1}$.

*Soluzione*

(a) $\sigma = (1637) \circ (245)$; l'ordine di $\sigma$ è dato dal $\text{mcm}(4,3) = 12$; $\sigma$ è dispari in quanto prodotto di una permutazione dispari e di una permutazione pari.

Essendo (1637) e (245) cicli disgiunti e pertanto permutabili, si ha

$$\sigma^4 = (1637)^4 \circ (245)^4 = (245)$$

(b) $(\tau \circ \sigma) = (3567) \circ (1637) \circ (245) = (17) \circ (2465)$; allora

$$(\tau \circ \sigma)^{-1} = (17) \circ (5642)$$

4. Si considerino i seguenti anelli:

(a) $(\mathbb{Z}_{16}, +, \cdot)$;

(b) $(\mathbb{Z}_{11}, +, \cdot)$;

(c) $(\mathbb{Z}_5[X], +, \cdot)$;

(d) $(\mathbb{C}[X], +, \cdot)$;

(e) $\left(\mathbb{Q}^{\mathbb{Q}} = \{f : \mathbb{Q} \longrightarrow \mathbb{Q} \mid f \text{ applicazione}\}, +, \cdot\right)$, con $+, \cdot$ definiti nel seguente modo:

$$(f+g)(x) = f(x) + g(x), \qquad (f \cdot g)(x) = f(x)g(x)$$

$\forall x \in \mathbb{Q}, \quad \forall f, g \in Q^{\mathbb{Q}}$.

i) Stabilire quali di essi sono domini d'integritá e quali sono campi.

ii) Per ciascuno degli anelli dati, determinare l'insieme (gruppo) degli elementi invertibili.

*Soluzione*

(a) Sappiamo che $(\mathbb{Z}_n, +, \cdot)$ con $n \in \mathbb{Z}$ e $n \geqslant 2$ è un campo se e solo se $n$ è primo. Sappiamo anche che $(\mathbb{Z}_n, +, \cdot)$ con $n \in \mathbb{Z}$ e $n \geqslant 2$ è un campo se e solo se è un dominio d'integritá.

Pertanto $(\mathbb{Z}_{16}, +, \cdot)$ non è un dominio d'integrità e di conseguenza neanche un campo; questo si può stabilire anche direttamente osservando, ad esempio che [4] è uno zero divisore: $[4][4] = [0]$ ( [4] è nilpotente), oppure $[4][8] = [0]$.

$U(\mathbb{Z}_{16}) = \{[a] \in \mathbb{Z}_{16} \mid a \text{ è primo con } 16\} = \{[1], [3], [5], [7], [9], [11], [13], [15]\}$.

(b) Essendo 11 un numero primo, $(\mathbb{Z}_{11}, +, \cdot)$ è un campo e pertanto anche un dominio d'integrità; $U(\mathbb{Z}_{11}) = \mathbb{Z}_{11}^{\star} = \mathbb{Z}_{11} - \{[0]\}$.

(c) Sappiamo che se $D$ è un dominio d'integritá, allora anche $D[X]$ è un dominio d'integritá; pertanto , essendo $\mathbb{Z}_5$ un campo e di conseguenza un dominio di integrità, $(\mathbb{Z}_5[X], +, \cdot)$ è un dominio d'integritá; $\mathbb{Z}_5[X]$ non è un campo, ad esempio $X$ non è invertibile; sappiamo inoltre che $U(\mathbb{Z}_5[X]) = U(Z_5) = Z_5^\star$.

(d) Per quanto osservato nel punto precedente, essendo $\mathbb{C}$ un campo e di conseguenza un dominio di integrità, $(\mathbb{C}[X], +, \cdot)$ è un dominio d'integritá; $\mathbb{C}[X]$ non è un campo, ad esempio $X$ non è invertibile; sappiamo inoltre che $U(\mathbb{C}[X]) = U(\mathbb{C}) = \mathbb{C}^\star$.

(e) $\mathbb{Q}^\mathbb{Q}$ con l'addizione e la moltiplicazione definite puntualmente non è un dominio d'integrità; ad esempio siano $\varphi$ l'applicazione da $\mathbb{Q}$ in $\mathbb{Q}$ definita da

$$x \longmapsto \begin{cases} 0 & \text{se } x \leqslant 0 \\ x & \text{se } x > 0 \end{cases}$$

e $\psi$ l'applicazione da $\mathbb{Q}$ in $\mathbb{Q}$ definita da

$$x \longmapsto \begin{cases} x & \text{se } x \leqslant 0 \\ 0 & \text{se } x > 0 \end{cases}$$

Allora $\varphi$ e $\psi$ sono entrambe diverse dalla applicazione da $\mathbb{Q}$ in $\mathbb{Q}$ identicamente nulla, cioè dallo zero di $\mathbb{Q}^\mathbb{Q}$, ed il loro prodotto è lo zero di $\mathbb{Q}^\mathbb{Q}$.

Essendo l'elemento neutro moltiplicativo di $\mathbb{Q}^\mathbb{Q}$ costituito dalla applicazione da $\mathbb{Q}$ in $\mathbb{Q}$ identicamente uguale ad 1, il gruppo degli elementi invertibili di $\mathbb{Q}^\mathbb{Q}$ è costituito da tutte e sole le applicazioni $f \in \mathbb{Q}^\mathbb{Q}$ tali che $f(x) \neq 0$ per ogni $x \in \mathbb{Q}$.

5. (a) Decomporre il polinomio $12X^5 - 18X^4 + 12X - 18 \in \mathbb{Z}[X]$ in fattori irriducibili in $\mathbb{C}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$ e $\mathbb{Z}[X]$.

   (b) Decomporre il polinomio $X^5 - X^4 + 3X^3 - 3X^2 + 2X - 2 \in \mathbb{Z}_7[X]$ in fattori irriducibili in $\mathbb{Z}_7[X]$ .

   (c) Dimostrare che il polinomio $f(X) = X^4+4X^3+6X^2+4X+3 \in \mathbb{Z}[X]$ è irriducibile in $\mathbb{Q}[X]$, determinando un numero intero $\alpha$ in modo tale che per $f(X - \alpha)$ si possa applicare il criterio di Eisenstein.

*Soluzione*

(a) $12X^5-18X^4+12X-18 = 12X(X^4+1)-18(X^4+1) = 6(X^4+1)(2X-3)$; determiniamo le radici complesse di $X^4 + 1$; la rappresentazione trigonometrica di $-1$ è $\cos\pi + i\sin\pi$; pertanto le radici quarte di $-1$ sono date da $\cos\frac{\pi+2\pi k}{4} + i\sin\frac{\pi+2\pi k}{4}$ con $k = 0, 1, 2, 3$ e precisamente:

$$\text{per } k = 0 \qquad \alpha_0 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$\text{per } k=1 \qquad \alpha_1 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$$

$$\text{per } k=2 \qquad \alpha_2 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$

$$\text{per } k=3 \qquad \alpha_3 = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$$

Si osservi che $\alpha_3 = \overline{\alpha}_0$ e $\alpha_2 = \overline{\alpha}_1$.

Allora la decomposizione del polinomio $12X^5 - 18X^4 + 12X - 18$ in fattori irriducibili in $\mathbb{C}[X]$ è:

$$12\left(X - \frac{3}{2}\right)(X - \alpha_0)(X - \alpha_3)(X - \alpha_1)(X - \alpha_2);$$

la decomposizione del polinomio $12X^5 - 18X^4 + 12X - 18$ in fattori irriducibili in $\mathbb{R}[X]$ è:

$$12\left(X - \frac{3}{2}\right)\left(X^2 - \sqrt{2}X + 1\right)\left(X^2 + \sqrt{2}X + 1\right);$$

la decomposizione del polinomio $12X^5 - 18X^4 + 12X - 18$ in fattori irriducibili in $\mathbb{Q}[X]$ è:

$$12\left(X - \frac{3}{2}\right)\left(X^4 + 1\right);$$

la decomposizione del polinomio $12X^5 - 18X^4 + 12X - 18$ in fattori irriducibili in $\mathbb{Z}[X]$ è:

$$2 \cdot 3(2X - 3)(X^4 + 1).$$

(b) $X^5 - X^4 + 3X^3 - 3X^2 + 2X - 2 = X^4(X-1) + 3X^2(X-1) + 2(X-1) = (X-1)(X^4 + 3X^2 + 2) = (X-1)(X^2+1)(X^2+2)$; $X^2+1$ e $X^2+2$ sono polinomi irriducibili in $\mathbb{Z}_7[X]$ poiché polinomi di 2 grado e privi di radici essendo i quadrati di $\mathbb{Z}_7$ dati da : $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, $6^2 = 1$ e ciascuno di essi diverso da $-1 = 6$ e $-2 = 5$.

(c) Per $\alpha = 1$ si ha che $f(X-1)$ ha come termine noto $1-4+6-4+3 = 2$, ha il coefficiente direttore uguale ad 1 ed i coefficienti di $X$, $X^2$ e $X^3$ pari; pertanto 2 è un numero primo che divide il termine noto di $f(X-1)$ e tutti gli altri suoi coefficienti tranne quello direttore; inoltre 4 non divide il termine noto di $f(X-1)$; si può pertanto applicare il criterio di Eisenstein a $f(X-1)$.