

Esercizi per il corso di Algebra (I modulo) assegnati nell'Anno Accademico 2006-07

Ultima revisione: 13 marzo 2009

1 Insiemi e relazioni

Esercizio 1. Siano A, B, C tre insiemi. Dimostrare che

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C) \quad \text{e} \quad (A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Esercizio 2. Siano A e B due insiemi. Dimostrare che

$$(A \cap B = A) \Leftrightarrow (A \subseteq B) \quad \text{e} \quad (A \cup B = B) \Leftrightarrow (A \subseteq B).$$

Esercizio 3. Si considerino le seguenti applicazioni

1. $f_1 : \mathbb{Q} \rightarrow \mathbb{Q}$, definita da $f_1(x) = x^2 - 2x$.
2. $f_2 : \mathbb{R}^- \rightarrow \mathbb{R}^+$, definita da $f_2(x) = \sqrt{x^2 - x}$.

Dire se f_1 e f_2 sono iniettive, suriettive o biettive.

Esercizio 4. Sia $f : A \rightarrow B$ un'applicazione e siano A_1, A_2 due sottoinsiemi di A . Mostrare che

1. $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$,
2. $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$.

Esercizio 5. Verificare quali tra le seguenti relazioni sono di equivalenza su $T = \{ \text{triangoli di un piano} \}$

1. $x\mathcal{R}y \Leftrightarrow x$ e y hanno lo stesso perimetro;
2. $x\mathcal{R}y \Leftrightarrow x$ e y hanno un angolo congruente;
3. $x\mathcal{R}y \Leftrightarrow x$ e y hanno due angoli congruenti.

Esercizio 6. Verificare quali tra le seguenti relazioni sono di equivalenza su \mathbb{R} :

1. $x\mathcal{R}y \Leftrightarrow |x| = |y|$;
2. $x\mathcal{R}y \Leftrightarrow e^x = e^y$;
3. $x\mathcal{R}y \Leftrightarrow x - y \in \mathbb{N} = \mathbb{Z}^+$

2 Induzione

Esercizio 7. Dimostrare per induzione che

1. $\sum_{k=1}^n k = \frac{n(n+1)}{2}$, per ogni $n \geq 1$;
2. $\sum_{k=0}^n \frac{1}{2^k} = 2 - \frac{1}{2^n}$, per ogni $n \geq 0$;
3. $n! > 2^n$, per ogni $n \geq 4$;
4. 13 divide $4^{2n+1} + 3^{n+2}$, per ogni $n \geq 0$.

3 Gli interi: M.C.D. e congruenze lineari

Esercizio 8. Utilizzando l'algoritmo delle divisioni successive si calcoli il Massimo Comune Divisore delle seguenti coppie:

1. $M.C.D.(72, 120)$;
2. $M.C.D.(300, 497)$;
3. $M.C.D.(5865, 4416)$.

Si esprimano inoltre tali $M.C.D.$ utilizzando l'identità di Bézout.

Esercizio 9. Si risolvano le seguenti congruenze lineari $ax \equiv b \pmod{n}$:

1. $5x \equiv 3 \pmod{6}$;
2. $21x \equiv 14 \pmod{35}$;
3. $21x \equiv 14 \pmod{55}$;
4. $15x \equiv 1 \pmod{9}$;
5. $64x \equiv 24 \pmod{20}$;
6. $21x \equiv -5 \pmod{8}$;
7. $5x \equiv 13 \pmod{21}$;
8. $15x \equiv 13 \pmod{17}$.

In particolare si trovino tutte e sole le soluzioni c tali che $0 \leq c < n$.

4 Gruppi

Esercizio 10. Dimostrare le seguenti proprietà:

1. Se G è un gruppo in cui $(ab)^2 = a^2b^2$ per ogni $a, b \in G$, allora G è abeliano;
2. Se $a^2 = 1_G$ per ogni $a \in G$, allora G è abeliano.
3. Se G è un gruppo finito di ordine pari, allora esiste un elemento $1_G \neq x \in G$ tale che $x^2 = 1_G$.

Esercizio 11. Sia G un gruppo abeliano finito. Allora $\prod_{g \in G} g^2 = 1$.

Esercizio 12. Sia X un insieme e $\mathcal{P}(X)$ l'insieme delle parti di X . Siano $A, B \in \mathcal{P}(X)$ e si definisca $A * B = (A \cup B) \setminus (A \cap B)$. Provare che $(\mathcal{P}, *)$ è un gruppo abeliano.

Esercizio 13. Calcolare l'ordine dei seguenti elementi:

1. $g = 2$ in $(\mathbb{Z}/5\mathbb{Z}, +)$;

2. $g = 2$ in $(\mathbb{Z}/6\mathbb{Z}, +)$;

3. $g = 5$ in $(\mathbb{Z}/8\mathbb{Z}, +)$;

4. $g = 3$ in $(\mathbb{Z}/12\mathbb{Z}, +)$.

Esercizio 14. Sia $H = \{id, (1, 4)(2, 3), (1, 2)(3, 4), (1, 3)(2, 4)\}$ un sottoinsieme di $G = \mathbb{A}_4$. Dimostrare che H è un sottogruppo di G e determinare la tavola di moltiplicazione di H .

Esercizio 15. Sia

$$H = \{id, (1, 3, 2), (1, 2, 3), (4, 5), (1, 3, 2)(4, 5), (1, 2, 3)(4, 5)\}$$

un sottoinsieme di $G = \mathbb{S}_5$.

1. Dimostrare che H è un sottogruppo di G e determinare la tavola di moltiplicazione di H ;
2. Determinare $H \cap \mathbb{A}_5$.

Esercizio 16. Siano σ e τ due permutazioni di \mathbb{S}_{10} così definite:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 4 & 6 & 7 & 5 & 8 & 10 & 9 \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 1 & 4 & 3 & 6 & 7 & 8 & 5 & 10 & 9 \end{pmatrix}.$$

1. Scrivere σ e τ come prodotto di cicli disgiunti;
2. Determinare σ^{-1} , τ^{-1} , $\sigma\tau$ e $\tau\sigma$;
3. Determinare il sottogruppo generato da σ ;
4. Determinare $o(\tau)$.

Esercizio 17. Sia $\sigma \in \mathbb{S}_n$ un ciclo di lunghezza $r \leq n$. Si dimostri che $o(\sigma) = r$.

Esercizio 18. Siano $\sigma, \tau \in \mathbb{S}_n$ due cicli disgiunti di lunghezza r e s , rispettivamente. Si dimostri che $o(\sigma\tau) = m.c.m.(r, s)$.

Esercizio 19. Sia H un sottogruppo di un gruppo G e sia $g \in G$. Si provi che gHg^{-1} è un sottogruppo di G .

Esercizio 20. Sia G un gruppo abeliano. Si provi che ogni sottogruppo di G è normale.

Esercizio 21. Sia G un gruppo e H un sottogruppo di G di indice 2. Si provi che H è normale in G . In particolare, si provi che \mathbb{A}_n è normale in \mathbb{S}_n .

Esercizio 22. Sia $G = \mathbb{S}_3$ e $H = \langle (1, 3) \rangle$. Si dica se H è normale in G .

Esercizio 23. Sia $G = \mathbb{S}_4$, $H = \{id, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\} \subset G$ e $N = \{id, (1, 2)(3, 4)\} \subset G$. Si provi che

1. H è un sottogruppo abeliano di G ;
2. H è un sottogruppo normale di G ;
3. N è un sottogruppo normale di H ;
4. N non è normale in G (ovvero l'essere normale non è una relazione transitiva).

Esercizio 24. Sia $H \trianglelefteq G$ e $K \leq G$ tale che $H \leq K$. Si provi che $H \trianglelefteq K$.

Esercizio 25. Siano H e K sue sottogruppi normali di G . Si provi che $H \cap K$ è un sottogruppo normale di G .

Esercizio 26. Dato un gruppo G , si definisce centro di G il sottoinsieme

$$\mathbf{Z}(G) = \{z \in G \mid zg = gz \forall g \in G\}.$$

Si provi che:

1. $\mathbf{Z}(G)$ è un sottogruppo abeliano di G ;
2. $\mathbf{Z}(G)$ è un sottogruppo normale di G ;
3. se $H \trianglelefteq G$, allora $\mathbf{Z}(H) \trianglelefteq G$.

Esercizio 27. Sia $G = \mathbb{S}_3$. Si determinino tutti i sottogruppi di G . In particolare, si dica quali di essi sono normali.

Esercizio 28. Utilizzando il teorema di Lagrange, dimostrare che se G è un gruppo finito, allora ogni elemento di G ha ordine finito. Dimostrare inoltre che non vale il viceversa, cioè che esistono gruppi infiniti i cui elementi hanno tutti ordine finito.

Suggerimento

1. Si consideri il gruppo $G = \mathbb{Q}/\mathbb{Z}$.
2. Si consideri l'insieme $X = \{\frac{1}{k} : k \in \mathbb{Z}^+\}$. Si dimostri che ogni elemento di X appartiene ad un differente laterale di \mathbb{Z} in \mathbb{Q} e se ne deduca che G è un gruppo infinito.
3. Si dimostri che gli elementi di G hanno ordine finito.

Esercizio 29. Sia G un gruppo tale che $|G| = p$, con p primo. Dimostrare che G è ciclico.

Esercizio 30. Sia $G = \mathbb{S}_6$. Siano $g_1 = (1, 2, 4)$, $g_2 = (1, 5, 6)$, $g_3 = (1, 2)(3, 4)(5, 6)$, $g_4 = (1, 2)(3, 6)$, $g_5 = (1, 2, 3, 4, 5, 6)$, $g_6 = (1, 6)(2, 4)$, $g_7 = (2, 3)(5, 6)(1, 4)$, $g_8 = (1, 3, 4, 5, 6, 2)$ elementi di G .

1. Si determinino quali di questi elementi appartengono a \mathbb{A}_6 ;
2. si determinino quali di questi elementi sono coniugati in G ;
3. se due elementi sono coniugati, si trovi almeno un elemento $g \in G$ che realizza il coniugio, cioè si trovi almeno un $g \in G$ tale $g_i = gg_jg^{-1}$.

Esercizio 31. Sia $G = \mathbb{S}_6$. Si determini quanti sono gli elementi di G coniugati a: $g_1 = (1, 2)$, $g_2 = (1, 2, 3)$, $g_3 = (1, 2)(3, 4)$, $g_4 = (1, 2, 3)(4, 5, 6)$ e $g_5 = (1, 2, 3, 4, 5, 6)$.

Esercizio 32. Si determinino le classi di coniugio di $G = \mathbb{S}_5$, determinandone in particolare l'ordine. (*Suggerimento: sono 7.*)

Esercizio 33. Sia G un gruppo finito tale che 3 non divide $|G|$ e tale che $(ab)^3 = a^3b^3$, per ogni $a, b \in G$. Provare che G è abeliano (*Servono poche conoscenze di algebra e un po' intuito algebrico...*).

5 Omomorfismi di gruppi

Esercizio 34. Sia $\phi : G \rightarrow H$ un omomorfismo di gruppi. Si provi che $\phi(1_G) = 1_H$ e che $\phi(g^{-1}) = \phi(g)^{-1}$, per ogni $g \in G$.

Esercizio 35. Sia $\phi : G \rightarrow H$ un omomorfismo di gruppi. Si provi che $\text{Ker}(\phi)$ è un sottogruppo normale di G e che ϕ è iniettivo se e soltanto se $\text{Ker}(\phi) = \{1_G\}$.

Esercizio 36. Sia $\vartheta : G \rightarrow H$ un omomorfismo di gruppi, ove H è abeliano. Si definisca una mappa $\phi : G \times G \rightarrow H$, ponendo $\phi((g_1, g_2)) = \vartheta(g_1)\vartheta(g_2)^{-1}$. Si provi che ϕ è un omomorfismo di gruppi.

Esercizio 37. Sia $\phi : G \rightarrow H$ un omomorfismo di gruppi. Si provi per induzione che, per ogni intero positivo k e per ogni $g \in G$, si ha $\phi(g^k) = \phi(g)^k$. Se ne deduca che se $o(g) = k$ finito, allora $o(\phi(g))$ divide k . Inoltre, se ϕ è iniettivo, allora $o(\phi(g)) = k$.

Esercizio 38. Sia $f : G \rightarrow H$ un morfismo di gruppi. Si dimostri che

1. se f è suriettivo e G è abeliano, allora anche H è abeliano;

2. se f è iniettivo e H è abeliano, allora anche G è abeliano;
3. se f è biiettivo, allora G è abeliano se e solo se H è abeliano.

6 Teoremi di Sylow

Esercizio 39. Sia $G = \mathbb{S}_4$. Trovare almeno un 2-sottogruppo di Sylow di G e un 3-sottogruppo di Sylow di G .

Esercizio 40. Cosa (se possibile) si può dedurre riguardo al numero dei p -sottogruppi di Sylow di G se:

1. $p = 7$ e $|G| = 28$;
2. $p = 2$ e $|G| = 48$;
3. $p = 2$ e $|G| = 32$;
4. $p = 2$ e $|G| = 12$;
5. $p = 3$ e $|G| = 12$.

Esercizio 41. Dimostrare che un gruppo G non è semplice se

1. $|G| = 56$;
2. $|G| = 148$;
3. $|G| = 385$.

Esercizio 42. Sapendo che ogni gruppo di ordine p^2 (con p primo) è abeliano, provare che G è abeliano se

1. $|G| = 99$;
2. $|G| = 153$.

Esercizio 43. Dato l'insieme $G = GL(2, F)$ delle matrici 2×2 invertibili con entrate in $F = \mathbb{Z}/p\mathbb{Z}$, p primo (G è un gruppo rispetto all'usuale operazione di prodotto tra matrici), si considerino i seguenti sottoinsiemi di G :

$$T = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in F, ad \neq 0 \right\} \quad P = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F \right\}.$$

1. Si provi che T è un sottogruppo di G e P un sottogruppo di T .
2. Si dimostri che $|G| = p(p^2 - 1)(p - 1)$.
3. Si dimostri che $P \in Syl_p(G)$ e $P \in Syl_p(T)$.
4. Si dimostri che $|Syl_p(T)| = 1$ e che $|Syl_p(G)| > 1$.

Esercizio 44. Sia G un gruppo tale che $|G| = pq$, con p e q primi distinti. Si dimostri che G non è semplice.

7 Anelli

Esercizio 45. Sia A un anello e siano $a, b \in A$. Dimostrare che

1. $0 \cdot a = a \cdot 0 = 0$;
2. $(-a)b = a(-b) = -(ab)$.

Esercizio 46. Nella definizione di anello (con 1_A), si richiede che $(A, +)$ sia commutativo. Dimostrare che in realtà la commutatività di $(A, +)$ segue dagli altri assiomi di anello.

Esercizio 47. Sia A un anello. Dimostrare che l'insieme degli elementi unitari di A forma un gruppo.

Esercizio 48. Determinare esplicitamente gli elementi unitari dell'anello $\frac{\mathbb{Z}}{n\mathbb{Z}}$, nel caso $n = 7, 8, 12$.

Esercizio 49. Sia K un campo e sia $A = \text{Mat}(n, K)$ ($n \geq 2$) l'anello delle matrici quadrate di ordine n su K . Determinare gli elementi unitari e i divisori dello zero di A .

Esercizio 50. Sia $A = \text{Mat}(2, \mathbb{R})$. Sia B il sottoinsieme di A costituito dalle matrici della forma

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}.$$

1. Provare che B è un sottoanello di A ;
2. determinare gli elementi invertibili di B ;
3. determinare i divisori dello zero di B .

Esercizio 51. Sia $A = \{ax + by + c \mid a, b, c \in \frac{\mathbb{Z}}{2\mathbb{Z}}\}$. Definiamo su A le seguenti operazioni:

- somma: l'usuale somma di polinomi;
- prodotto: $(ax + by + c)(a_1x + b_1y + c_1) = (ac_1 + a_1c)x + (bc_1 + b_1c) + (cc_1)$.

1. Provare che A con tali operazioni è un anello commutativo;
2. determinare gli elementi invertibili di A ;
3. determinare i divisori dello zero di A .

Esercizio 52. Sia A un anello tale che $a^2 = a$ per ogni $a \in A$. Dimostrare che A è commutativo.

Esercizio 53. Sia A un anello commutativo e sia $R = \text{Mat}(2, A)$ l'anello delle matrici quadrate di ordine 2 ad elementi in A . Sia B_n il seguente sottoinsieme di R :

$$B_n = \left\{ \begin{pmatrix} 0 & n \cdot a \\ 0 & a \end{pmatrix} \mid a \in A \right\},$$

ove per ogni $n \in \mathbb{Z}$, $n \cdot a$ denota l' n -esimo multiplo di A . Si provi che per ogni fissato $n \in \mathbb{Z}$, B_n è un anello, ma non un sottoanello di A . In particolare, si determini l'unità di B_n .

Esercizio 54. Sia $A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$.

1. Provare che A è un sottoanello di $Mat(2, \mathbb{Z})$.
2. Determinare gli elementi invertibili di A .
3. Provare che $I = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid b \in 2\mathbb{Z} \right\}$ è un sottoanello di A , ma non un suo ideale.
4. Provare che $J = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in 2\mathbb{Z} \right\}$ è un ideale di A .

Esercizio 55. Sia $R = Mat(2, \mathbb{Z})$ e su consideri il suo sottoinsieme $A = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{Z} \right\}$.

1. Provare che A è un sottoanello di R .
2. Trovare i divisori dello zero e gli elementi invertibili di A .
3. Dimostrare che $I = \left\{ \begin{pmatrix} 3h & 0 \\ 0 & 7k \end{pmatrix} \mid h, k \in \mathbb{Z} \right\}$ è un ideale di A .
4. Provare che I non è primo.
5. Per ogni $n \in \mathbb{N}$, provare che $I_n = \left\{ \begin{pmatrix} a & 0 \\ 0 & nk \end{pmatrix} \mid a, k \in \mathbb{Z} \right\}$ è un ideale di A .
6. Per quali valori di n I_n è massimale?

Esercizio 56. Si determinino tutti gli omomorfismi di anello tra $\mathbb{Z}/6\mathbb{Z}$ e $\mathbb{Z}/3\mathbb{Z}$.

Esercizio 57. Si consideri l'insieme A_k delle matrici quadrate di ordine 2 ad elementi reali della forma:

$$\begin{pmatrix} x & ky \\ y & x \end{pmatrix}, \quad x, y, \in \mathbb{R},$$

ove k è un fissato elemento reale.

1. Si mostri che A_k è un anello commutativo per ogni valore di k , rispetto alle usuali operazioni di somma e prodotto tra matrici.
2. Si determinino per quali valori di k l'insieme A_k è un campo.

8 Teorema di Eulero-Fermat

Esercizio 58. Sia ϕ la funzione di Eulero. Determinare $\phi(n)$, nel caso $n = 7, 8, 12, 15$.

Esercizio 59. Determinare il minimo intero positivo n tale che

- $\phi(n) = 4$;
- $\phi(n) = 6$;
- $\phi(n) = 10$.

Esercizio 60. Determinare quali delle seguenti equazioni possono essere risolte utilizzando il teorema di Eulero-Fermat:

1. $5^6 \equiv x \pmod{7}$;
2. $3^2 \equiv x \pmod{6}$;
3. $5^2 \equiv x \pmod{6}$;
4. $6^4 \equiv x \pmod{8}$.

Esercizio 61. Dimostrare che per ogni intero $n \geq 3$, $\phi(n)$ è pari.

9 Polinomi

Esercizio 62. Dati i seguenti polinomi $a(x), b(x) \in \mathbb{Q}[x]$, calcolare quoziente e resto della divisione $a(x) : b(x)$:

1. $a(x) = x^3 + 2x + 5$ e $b(x) = x^2 - 1$;
2. $a(x) = x^4 + x^2 - 1$ e $b(x) = 2x^2 + x - 1$;
3. $a(x) = x^5 + \frac{1}{2}x + 1$ e $b(x) = x^2 + x - 1$;
4. $a(x) = x^4 - 3x^2 + 1$ e $b(x) = x^2 + x - 1$.

Esercizio 63. Dati i seguenti polinomi $a(x), b(x) \in A[x]$, calcolare quoziente e resto della divisione $a(x) : b(x)$:

1. $a(x) = x^4 + x^2 + 1$, $b(x) = x^2 + x + 1$ e $A = \frac{\mathbb{Z}}{2\mathbb{Z}}$;
2. $a(x) = x^4 + x^3 + 1$, $b(x) = x^2 + x + 1$ e $A = \frac{\mathbb{Z}}{2\mathbb{Z}}$;
3. $a(x) = x^4 + x^3 + 1$, $b(x) = x^3 + x + 1$ e $A = \frac{\mathbb{Z}}{2\mathbb{Z}}$;
4. $a(x) = x^4 + x^2 + 1$, $b(x) = x^2 + x + 1$ e $A = \frac{\mathbb{Z}}{3\mathbb{Z}}$;
5. $a(x) = x^4 + x^3 + 2x + 1$, $b(x) = x^3 + x + 1$ e $A = \frac{\mathbb{Z}}{3\mathbb{Z}}$;
6. $a(x) = x^4 + 2x^3 + 1$, $b(x) = 2x^3 + x + 1$ e $A = \frac{\mathbb{Z}}{3\mathbb{Z}}$;
7. $a(x) = x^4 + 5x^3 + 2x + 1$, $b(x) = x^3 + 3x + 1$ e $A = \frac{\mathbb{Z}}{7\mathbb{Z}}$;
8. $a(x) = 6x^4 + 2x + 1$, $b(x) = 2x^3 + 3x + 1$ e $A = \frac{\mathbb{Z}}{7\mathbb{Z}}$;
9. $a(x) = 2x^4 + 3x^3 + x + 1$, $b(x) = 2x^2 + 2x + 3$ e $A = \frac{\mathbb{Z}}{7\mathbb{Z}}$.

Esercizio 64. Dati i seguenti polinomi $a(x), b(x) \in \mathbb{Z}[x]$, dire quando è possibile dividere $a(x)$ per $b(x)$. In caso affermativo, calcolare quoziente e resto della divisione $a(x) : b(x)$:

1. $a(x) = x^3 + x + 1$ e $b(x) = x^2 + x + 1$;
2. $a(x) = x^3 + 5x - 3$ e $b(x) = 2x^2 + x + 1$;

3. $a(x) = x^5 + x^4 + x^2 - x + 1$ e $b(x) = -x^3 + x + 1$.

Esercizio 65. Dati i seguenti polinomi $a(x), b(x) \in A[x]$, dire quando è possibile dividere $a(x)$ per $b(x)$. In caso affermativo, calcolare quoziente e resto della divisione $a(x) : b(x)$:

1. $a(x) = x^4 + x^2 + 1$, $b(x) = 2x^2 + x + 1$ e $A = \frac{\mathbb{Z}}{4\mathbb{Z}}$;

2. $a(x) = x^4 + 3x + 1$, $b(x) = 3x^2 + x + 1$ e $A = \frac{\mathbb{Z}}{4\mathbb{Z}}$;

3. $a(x) = 3x^4 + 2x^2 + 1$, $b(x) = 4x^2 + 4x + 4$ e $A = \frac{\mathbb{Z}}{4\mathbb{Z}}$;

4. $a(x) = x^3 + 7x^2 + 5$, $b(x) = 3x^2 + x + 1$ e $A = \frac{\mathbb{Z}}{12\mathbb{Z}}$;

5. $a(x) = 5x^4 + x^2 + 1$, $b(x) = 7x^2 + x + 1$ e $A = \frac{\mathbb{Z}}{12\mathbb{Z}}$;

6. $a(x) = x^3 + x^2 + 1$, $b(x) = 9x^2 + 7x + 1$ e $A = \frac{\mathbb{Z}}{12\mathbb{Z}}$.

Esercizio 66. Si determini in $\mathbb{Q}[x]$ un M.C.D. tra le seguenti coppie di polinomi:

1. $f(x) = x^4 - 4x^3 + 4x^2 - 4x + 3$ e $g(x) = x^3 + x^2 + x + 1$;

2. $f(x) = x^3 + x^2 + x$ e $g(x) = x^6 - x^5 + x$;

3. $f(x) = x^3 + x^2 + x - 1$ e $g(x) = x^4 + x - 1$;

4. $f(x) = x^4 + x^3 + x + 1$ e $g(x) = x^2 + 2x + 1$.

Esercizio 67. Si determini in $F[x]$ un M.C.D. tra le seguenti coppie di polinomi:

1. $f(x) = x^4 + x^3 + x + 1$, $g(x) = x^2 + 2x + 1$ e $F = \mathbb{Z}/2\mathbb{Z}$;

2. $f(x) = x^3 + x - 1$, $g(x) = x^4 + x - 1$ e $F = \mathbb{Z}/2\mathbb{Z}$;

3. $f(x) = x^4 + x^3 + x + 1$, $g(x) = x^2 + x - 1$ e $F = \mathbb{Z}/3\mathbb{Z}$;

4. $f(x) = x^4 + 2x^3 - x + 1$, $g(x) = x^2 - x - 1$ e $F = \mathbb{Z}/3\mathbb{Z}$;

5. $f(x) = x^3 + 3x^2 - 2x - 1$, $g(x) = x^5 - x^4 + x + 2$ e $F = \mathbb{Z}/5\mathbb{Z}$.

Esercizio 68. Si decomponga in fattori irriducibili i seguenti polinomi di $\mathbb{Q}[x]$:

1. $x^3 - 7x - 6$;
2. $x^4 + 2x^3 - x - 2$;
3. $x^4 + 5x^2 + 4$;
4. $x^4 - 4x^3 + 4x^2 - 4x + 3$.

Esercizio 69. Si determinino i polinomi monici irriducibili di grado 2 di $\mathbb{Z}/3\mathbb{Z}[x]$.

Esercizio 70. Si decomponga in fattori irriducibili i seguenti polinomi di $\mathbb{Z}/p\mathbb{Z}[x]$:

1. $x^4 + 2x^3 - x - 2$, $p = 3$;
2. $x^4 + 5x^2 + 4$, $p = 7$;
3. $x^4 + 5x^2 + 4$, $p = 5$;
4. $x^4 + 4x^3 + 4x^2 - 4x + 3$, $p = 5$;
5. $x^4 + 4x^3 + 4x^2 - 4x + 3$, $p = 3$;
6. $x^4 + 4x^3 + 4x^2 - 4x + 3$, $p = 11$.

10 Interi di Gauss

Esercizio 71. Sia $R = \mathbb{Z}[i]$ l'anello degli interi di Gauss. Si calcolino in R le seguenti divisioni, trovando quoziente e resto:

1. $(2 + i) : (3 - i)$.
2. $(5 + i) : i$.
3. $(-5 + 2i) : (-1 + 2i)$.

4. $(-2 - 3i) : 3$.

5. $2 : (i + 1)$.

6. $(2 + 5i) : (1 + i)$.

Esercizio 72. Si determini in $\mathbb{Z}[i]$ un M.C.D. tra le seguenti coppie di numeri:

1. $a = 7 + 3i$ e $b = 1 - 7i$;

2. $a = 1 + 7i$ e $b = 7 + i$;

3. $a = 7i$ e $b = 7 + 2i$;

4. $a = 3 + 4i$ e $b = 4 - 3i$;

5. $a = 11 + 7i$ e $b = 3 + 7i$;

6. $a = 8i$ e $b = 7 + 3i$.

11 Sistemi di congruenze: teorema cinese del resto

Esercizio 73. Si risolvano in \mathbb{Z} i seguenti sistemi di congruenze:

$$1. \begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{2} \end{cases}; \quad 2. \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{4} \\ x \equiv 3 \pmod{5} \end{cases};$$

$$3. \begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 1 \pmod{5} \\ x \equiv 7 \pmod{4} \end{cases}; \quad 4. \begin{cases} x \equiv 2 \pmod{13} \\ x \equiv 3 \pmod{8} \\ x \equiv 7 \pmod{15} \end{cases}.$$

Esercizio 74. Si risolva nell'anello \mathbb{Z} il seguente sistema di congruenze:

$$\begin{cases} x \equiv 2 \pmod{10} \\ x \equiv 4 \pmod{9} \\ x \equiv 11 \pmod{13} \end{cases}$$

Esercizio 75. Si risolvano in \mathbb{Z} i seguenti sistemi di congruenze:

$$1. \begin{cases} 2x \equiv 1 \pmod{3} \\ 3x \equiv 1 \pmod{4} \\ 2x \equiv 3 \pmod{5} \end{cases} ; \quad 2. \begin{cases} 5x \equiv 2 \pmod{9} \\ 7x \equiv 1 \pmod{11} \\ 4x \equiv 3 \pmod{13} \end{cases} .$$

Esercizio 76. Si risolvano in \mathbb{Z} i seguenti sistemi di congruenze:

$$1. \begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 1 \pmod{6} \\ x \equiv 3 \pmod{7} \end{cases} ; \quad 2. \begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 5 \pmod{12} \\ x \equiv 8 \pmod{15} \end{cases} .$$

Esercizio 77. Si risolva in $\mathbb{Q}[x]$ il seguente sistema di congruenze:

$$\begin{cases} f(x) \equiv x + 5 \pmod{x^2 + 3} \\ f(x) \equiv x \pmod{x + 2} \\ f(x) \equiv x + 3 \pmod{x^2 + 1} \end{cases}$$