Esercizi per il Corso di Matematica Discreta

Andrea Mori
Dipartimento di Matematica
Università di Torino

(versione Luglio 2003)

Nota: In tutto il testo i simboli $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ indicheranno, rispettivamente, i numeri naturali, i numeri interi relativi, i numeri razionali, i numeri reali ed i numeri complessi. Altri simboli speciali verranno spiegati di volta in volta.

1 Insiemistica

Nota: Nei seguenti problemi A, B, C, ... denotano sottoinsiemi arbitrari di un insieme X fissato. Il complementare di A (in X) è denotato A^c.

1. Siano $A = \{x \in \mathbb{R} \,|\, x^2 + x - 2 = 0\}$, $B = \{1, -1, 2\}$ e $C = \{1, \{2, 3\}\}$.

1. Determinare l'insieme delle parti di B e l'insieme delle parti di C.
2. Dire quali delle seguenti affermazioni sono vere e quali false:

$$\begin{array}{cccccc} \{1\} \not\subseteq A & 1 \in C & \{1\} \in A & 2 \in C & 1 \subseteq A & 3 \in C \\ 1 \in A & \{1\} \in C & A \subseteq B & \{2,3\} \in C & B \subseteq A & \{2\} \in C \end{array}$$

2. Siano $A = \{x \in \mathbb{N} \,|\, x < 20\}$ e $B = \{x \in \mathbb{N} \,|\, x \geq 10\}$. Calcolare:

$$A \cap B, \quad A \cup B, \quad A - B, \quad B - A, \quad A^c, \quad B^c.$$

3. Siano $Y = \{x \in \mathbb{R} \,|\, x \leq 3\}$ e $Z = \{x \in \mathbb{R} \,|\, 5 \leq x < 21\}$. Determinare $(Y \cup Z)^c$, Y^c, Z^c e verificare che $(Y \cup Z)^c = Y^c \cap Z^c$.

4. Dimostrare le *Leggi di De Morgan*:

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C) \qquad e \qquad (A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

5. Verificare le uguaglianze $(A \cup B)^c = A^c \cap B^c$ e $(A \cap B)^c = A^c \cup B^c$.

6. Dimostrare che le relazioni del problema precedente rimangono valide per una famiglia arbitraria $\{A_i\}_{i \in \mathcal{I}}$ di insiemi:

$$\left(\bigcup_{i \in \mathcal{I}} A_i \right)^c = \bigcap_{i \in \mathcal{I}} {A_i}^c \qquad e \qquad \left(\bigcap_{i \in \mathcal{I}} A_i \right)^c = \bigcup_{i \in \mathcal{I}} {A_i}^c.$$

7. Siano $Y = \{x \in \mathbb{R} \,|\, x \leq a\}$ e $Z = \{x \in \mathbb{R} \,|\, b \leq x < c\}$, dove a, b, c sono numeri reali qualsiasi, non necessariamente distinti e con $b < c$. Distinguendo i vari casi, determinare $(Y \cup Z)^c$ come unione di sottoinsiemi disgiunti di $\mathbb{R}$.

8. Per ogni $n \in \mathbb{N}$, sia $A_n = \{x \in \mathbb{N} \,|\, x \neq n+1\}$. Calcolare $\bigcup_{n\in\mathbb{N}} A_n$ e $\bigcap_{n\in\mathbb{N}} A_n$.

9. Per ogni $n \in \mathbb{N}$ poniamo $I_n = (0, 1/n)$, intervallo aperto di $\mathbb{R}$. Dimostrare che $\bigcap_{n\in\mathbb{N}} I_n = \emptyset$. Chi è $\bigcup_{n\in\mathbb{N}} I_n$?

10. Per ogni $n \in \mathbb{N}$ poniamo $I_n = (-1/n, 1/n)$. Dimostrare che $\bigcap_{n\in\mathbb{N}} I_n = \{0\}$.

11. Dimostrare le uguaglianze $A \cap B^c = A - B$ e $A \cup B^c = (B - A)^c$.

12. Dimostrare la seguente affermazione: $A \cap B = \emptyset$ se e solo se $A^c \cup B^c = X$.

Una famiglia di insiemi non vuoti $\{A_i\}_{i\in\mathcal{I}}$ è detta una **partizione** di X se $\bigcup_{i\in\mathcal{I}} A_i = X$ e se, per ogni i,j si ha $A_i \cap A_j = \emptyset$ oppure $A_i = A_j$.

13. Siano D e P i sottoinsiemi dei numeri dispari e pari, rispettivamente. Dimostrare che $\{D, P\}$ è una partizione di $\mathbf{N}$.

14. Si fissi $d \in \mathbb{N}$ con $d > 1$. Per ogni $r \in \{0, 1, \ldots, d-1\}$ si definisca A_r come il sottoinsieme dei numeri naturali la cui divisione per d dà resto r. Dimostrare che la famiglia $\{A_r\}$ definisce una partizione di $\mathbb{N}$. In che senso questa costruzione generalizza la situazione del problema precedente?

15. Sia X l'insieme di tutti i numeri naturali multipli di 3. Scrivere una partizione di X costituita da 2 sottoinsiemi. Scrivere una partizione di X costituita da infiniti sottoinsiemi.

16. Sia $A_n = [n-1, n]$, per ogni $n \in \mathbb{Z}$, l'intervallo chiuso in X con estremi $n-1$ e n. Calcolare $\bigcup_{n\in\mathbb{Z}} A_n$ e $\bigcap_{n\in\mathbb{Z}} A_n$. Gli insiemi A_n costituiscono una partizione di $\mathbb{R}$?

17. È vero che per ogni coppia di insiemi $A, B \subset X$, la famiglia $\{A \cap B, A - B, B - A, (A \cup B)^c\}$ è una partizione di X?

18. È vero che $B \subseteq A$ se e soltanto se $\{B, A - B, A^c\}$ è una partizione di X?

19. Dimostrare l'affermazione seguente. Sia $\{A_i\}_{i\in\mathcal{I}}$ una partizione di X e sia $B \subseteq X$. Allora B non contiene alcun A_i se e solo se la famiglia $\{A_i - B\}_{i\in\mathcal{I}}$ è una partizione di B^c.

20. Sia $\mathcal{A} = \{A_i\}_{i\in\mathcal{I}}$ una partizione di X e sia $B \subset X$. Costruire, a partire da $\mathcal{A}$, una partizione di B.

21. Data una funzione $f(x)$ sia $Z(f) = \{x \,|\, f(x) = 0\}$. Dimostrare che se $f(x)$ e $g(x)$ sono due funzioni qualunque, allora $Z(fg) = Z(f) \cup Z(g)$.

22. Con la notazione dell'esercizio precedente, determinare una coppia di funzioni f e g in modo che gli insiemi $Z(f)$ e $Z(g)$ costituiscano una partizione di $\mathbb{R}$.

23. Sia ora $p(x)$ un polinomio e $p'(x)$ la sua derivata. Dimostrare che $a \in Z(p) \cap Z(p')$ se e soltanto se $(x-a)^2$ divide $p(x)$.

24. Esprimere l'insieme delle soluzioni della disequazione $\frac{x+2}{x+1} > 2$ in termini dei sottoinsiemi $A = \{x \in \mathbb{R} \,|\, x < 0\}$, $B = \{x \in \mathbb{R} \,|\, x > -1\}$.

25. Esprimere l'insieme delle soluzioni della disequazione $\sqrt{x^2 - 1} > x - 2$ in termini dei sottoinsiemi $A = (-1, 1)$, $B = \{x \in \mathbb{R} \,|\, x > 5/4\}$ e $C = \{x \in \mathbb{R} \,|\, x < 2\}$.

26. Si generalizzi la discussione del problema precedente esprimendo l'insieme delle soluzioni della disequazione $\sqrt{P(x)} > Q(x)$ in termini degli insiemi $A = \{x \in \mathbb{R} \,|\, P(x) \geq 0\}$, $B = \{x \in \mathbb{R} \,|\, P(x) \geq Q(x)^2\}$ e $C = \{x \in \mathbb{R} \,|\, Q(x) < 0\}$

Nei prossimi problemi π è l'insieme dei punti del piano (euclideo). Denotiamo $C(P, r)$ il cerchio di centro P e raggio r, cioè l'insieme dei punti di π aventi distanza $\leq r$ da P.

27. Supponiamo assegnato in π un riferimento cartesiano ortogonale Oxy. Siano $A = \{(x,y) \in \pi \,|\, x+y-2>0\}$, $B = \{(x,y) \in \pi \,|\, x-2y+4<0\}$ e $C = A \cap B$. Qual è il valore massimo di r per cui $C \cap C(0,r) = \emptyset$?

28. Siano P_1 e $P_2 \in \pi$ arbitrari. Si enunci una condizione in termini della distanza tra P_1 e P_2 e sui valori r_1 e r_2 che risulti necessaria e sufficiente affinchè $C(P_1,r_1) \cap C(P_2,r_2) = \emptyset$.

Nei problemi seguenti si richiede di usare il procedimento di INDUZIONE.

29. Provare mediante l'induzione che le seguenti formule valgono per ogni $n \in \mathbf{N}$:

1. $1+2+...+n = \frac{1}{2}(n(n+1)$.
2. $1^2+2^2+...+n^2 = \frac{1}{6}(n(n+1)(2n+1)$.
3. $1^3+2^3+...+n^3 = \left(\frac{1}{6}n(n+1)(2n+1)\right)^2$.
4. $(1+x)^n \geq 1+nx$, per ogni $x \in \mathbf{R}$ tale che $x>1$.
5. $\left(\frac{1}{2}\right)^0 + \left(\frac{1}{2}\right)^1 + \cdots + \left(\frac{1}{2}\right)^n = \frac{2^{n+1}-1}{2^n}$.
6. $\left(\frac{1}{3}\right)^0 + \left(\frac{1}{3}\right)^1 + \cdots + \left(\frac{1}{3}\right)^n = \frac{3^{n+1}-1}{2\cdot 3^n}$.
7. $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.
8. $1+2q+3q^2+\cdots+nq^{n-1} = \frac{1-(n+1)q^n+nq^{n+1}}{(1-q)^2}$.
9. $(1+q)(1+q^2)(1+q^4)\cdots(1+q^{2^n}) = \frac{1-q^{2^{n+1}}}{1-q}$.

30. Sia $A = \{n \in \mathbf{N} \,|\, 1+2+\cdots+n = (n+3)(n-2)/2\}$. Provare che se n appartiene ad A allora anche $n+1$ appartiene ad A. È vero che $A = \mathbb{N}$?

31. Provare che per ogni numero naturale $k \geq 7$ si ha $(k-5)^4 > k$. Determinare $\{k \in \mathbf{N} \,|\, (k-5)^4 > k\}$.

32. Provare che si ha $p^q + q^p \leq 2^{pq}$, per ogni coppia di numeri naturali (p,q) entrambi maggiori di 0. (Suggerimento: Dimostrare dapprima mediante l'induzione che la formula vale per ogni coppia del tipo $(1,q)$, cioè ponendo $p=1$; dimostrare quindi che se la formula vale per una coppia (p,q) allora vale anche per la coppia $(p+1,q)$. Spiegare perché queste due affermazioni permettono di concludere.)

33. Provare mediante l'induzione la divisione euclidea: per ogni coppia $(a,b) \in \mathbb{N} \times \mathbb{N}$ con $b>0$, esiste una unica coppia $(q,r) \in \mathbb{N} \times \mathbb{N}$ con $0 \leq r < b$ tale che $a = bq + r$. (Suggerimento: usare l'induzione su a.)

2 Relazioni

Nei seguenti problemi viene definita una relazione ϱ su un insieme X specificato di volta in volta. In ciascun caso si dovrà stabilire se la relazione ϱ soddisfa o meno le proprietà riflessiva, simmetrica, antisimmetrica e transitiva. Qualora la relazione ϱ risulti essere un'equivalenza, si dovranno descrivere la partizione di X da essa definita e l'insieme quoziente associato.

Nei prossimi problemi X è l'insieme delle lettere dell'alfabeto latino.

34. $x \varrho y \iff x$ precede y nell'ordine alfabetico.

35. $x \varrho y \iff$ almeno una tra x e y è una consonante.

36. $x \varrho y \iff$ la sequenza xy appare in questo elenco di problemi.

Nei prossimi problemi $X = \{0, 1, \ldots, 9\}$.

37. $x \varrho y \iff 10x + y$ è un numero primo.

38. $x \varrho y \iff 10x + y$ è divisibile per 3.

39. $x \varrho y \iff x + 10y + 100x$ è divisibile per 3.

Nei prossimi problemi $X = \mathbb{N}$ è l'insieme dei numeri naturali.

40. $x \varrho y \iff x$ divide y.

41. $x \varrho y \iff y = xn^2$ per qualche $n \in \mathbb{N}$.

42. $x \varrho y \iff x = y \pm n^2$ per qualche $n \in \mathbb{N} \cup \{0\}$.

43. $x \varrho y \iff x + y$ è un numero composto (cioè non primo).

Nei prossimi problemi $X = \mathbb{Z}$ è l'insieme dei numeri interi.

44. $x \varrho y \iff x$ divide y.

45. $x \varrho y \iff y = xn^2$ per qualche $n \in \mathbb{Z}$.

46. $x \varrho y \iff |x - y| = 0$ oppure è un numero primo.

Nei prossimi problemi $X = \mathbb{R}$ è l'insieme dei numeri reali.

47. $x \varrho y \iff |x - y| \leq 1$.

48. $x \varrho y \iff xy \geq x + y$.

49. $x \varrho y \iff x - y \in \mathbb{Z}$.

50. $x \varrho y \iff x + y \in \mathbb{Z}$.

51. $x \varrho y \iff x^2 = y^2$

52. $x \varrho y \iff \cos^2(x) + \sin^2(y) = 1$.

Nei prossimi problemi $X = \mathbb{R} - \{0\}$ è l'insieme dei numeri reali non nulli.

53. $x \varrho y \iff xy > 0$.

54. $x \varrho y \iff x/y \in \mathbb{Z}$.

55. $x \varrho y \iff x/y \in \mathbb{Q}$.

56. $x \varrho y \iff \frac{1}{x} - \frac{1}{y} \in \mathbb{Q}$.

Nei prossimi problemi X è l'insieme dei punti del piano, che pensiamo dotato di un sistema di coordinate Oxy. Denotiamo $P, Q, R, \ldots$ gli elementi di X (punti). Dato $P \in X$ denotiamo $x(P)$ e $y(P)$ le sue coordinate.

57. $P \varrho Q \iff x(P) = x(Q)$.

58. $P \varrho Q \iff x(P) = y(Q)$.

59. $P \varrho Q \iff x(P) \cdot y(Q) \geq 0$.

60. $P \varrho Q \iff P = Q$ oppure il segmento PQ interseca uno degli assi coordinati.

Nei prossimi problemi l'insieme X verrà specificato di volta in volta.

61. Sia X l'insieme dei punti del piano meno l'origine O. Definiamo $P \varrho Q \iff P = Q$ oppure se la retta per P e Q passa per O.

62. Sia X l'insieme dei cerchi del piano. Definiamo $x \varrho y \iff x$ e y sono cerchi concentrici.

63. Sia X l'insieme delle rette del piano. Definiamo $x \varrho y \iff x$ e y sono parallele oppure se sono perpendicolari fra di loro (dichiariamo convenzionalmente che ogni retta è parallela a sè stessa).

64. Sia X l'insieme dei punti della superficie di una sfera. Definiamo $x \varrho y \iff x = y$ oppure il segmento xy è un diametro.

65. Siano $r_1, \ldots, r_n$ rette dello spazio $\mathbf{R}^3$ due a due disgiunte (cioè $r_i \cap r_j = \emptyset$ se $i \neq j$) e sia $X = \bigcup_{i=1}^{n} r_i$. Poniamo $P \varrho Q \iff P$ e Q appartengono alla stessa retta.

66. Cosa cambia nel problema precedente se si elimina l'ipotesi che le rette siano a due a due disgiunte?

Nei prossimi problemi prendiamo come insieme X l'insieme $\mathcal{P}(S)$ delle parti di un insieme non vuoto S. Dunque X è l'insieme dei sottoinsiemi di S, e denotiamo $A, B, \cdots$ i suoi elementi.

67. $A \varrho B \iff A \cap B \neq \emptyset$.

68. $A \varrho B \iff A = B$ oppure A e B formano una partizione di S.

69. $A \varrho B \iff A = B$ oppure $A \cup B = S$.

70. $A \varrho B \iff A \subseteq B$.

71. Nell'ipotesi ulteriore in cui S è un insieme finito, $A \varrho B \iff A$ e B possiedono lo stesso numero di elementi.

3 Applicazioni ed Operazioni

72. Determinare esplicitamente tutte le applicazioni $f : A \to B$ dove $A = \{1, 2, 3\}$ e $B = \{\alpha, \beta\}$. Quante sono quelle suriettive? Quante sono quelle iniettive?

73. Esiste una applicazione $f : \mathbb{R} \to \mathbb{R}$ tale che $f(\{1, 2\}) = \{1, \sqrt{2}, \pi\}$? Esiste una applicazione $g : \mathbb{R} \to \mathbb{R}$ tale che $g(\{1, \sqrt{2}, \pi\}) = \{1, 2\}$?

74. Dare un esempio di due applicazioni differenti di $\mathbb{N}$ in $\mathbb{N}$ aventi la stessa immagine. È possibile costruire infinite applicazioni di $\mathbb{N}$ in $\mathbb{N}$ aventi la stessa immagine?

75. Dare un esempio di applicazione $\phi : \mathbb{N} \to \mathbb{N}$ suriettiva ma non iniettiva. È possibile costruire una tale ϕ in modo che per ogni $n \in \mathbb{N}$ l'insieme $\phi^{-1}(n)$ sia infinito?

76. Sia $f : \mathbb{Z} \to \mathbb{Z}$ data da $f(n) = n^2 - 3n + 5$. Determinare $f(0)$, $f^{-1}(5)$ e $f^{-1}(0)$. Si tratta di una applicazione iniettiva? Si tratta di una applicazione suriettiva? Rispondere alle stesse domande per la funzione $g(n) = 2n^2 - 3n + 5$.

77. Decidere quali delle seguenti funzioni $\varphi : \mathbb{R} \to \mathbb{R}$ sono iniettive, e quali sono suriettive determinando esplicitamente l'insieme immagine. Nel caso una funzione φ risulti biettiva, si determini l'inversa φ^{-1}.

$$\varphi_1(x) = x^2 - 4. \quad \varphi_2(x) = 10 - 7x. \quad \varphi_3(x) = x^5 + 2.$$
$$\varphi_4(x) = 2^x. \quad \varphi_5(x) = \cos(\pi x). \quad \varphi_6(x) = 1/2.$$

78. Decidere quali delle funzioni φ del problema precedente inducono una funzione $X \to X$ dove X è, di volta in volta, $\mathbb{N}$ o $\mathbb{Z}$ o $\mathbb{Q}$. In caso affermativo, dire se l'applicazione così ottenuta è iniettiva e/o suriettiva e, se possibile, determinare l'inversa.

79. Determinare l'insieme immagine della funzione $\phi : X \to Y$ in ciascuno dei casi seguenti:

1. $X = \mathbb{N} \times \mathbb{N}$, $Y = \mathbb{N}$ e $\phi(m,n) = mn$.

2. X è il piano euclideo, $Y = \mathbb{R}$ e $\phi(P) =$ distanza del punto P dall'origine O.

3. X è l'insieme dei triangoli rettangoli aventi cateti di lunghezza intera, $Y = \mathbb{R}$ e $\phi(T) =$ area del triangolo T.

4. $X = Y = \mathbb{N}$, $\varphi(n) =$ numero di case raggiungibili in almeno n mosse nel gioco degli scacchi da una torre situata in una casa d'angolo con la scacchiera vuota[1]. La risposta cambia se la torre non è inizialmente in una casa d'angolo?

5. $X = Y = \mathbb{R} \times \mathbb{R}$ e $\phi(x,y) = (x+y, x-y)$.

6. X insieme dei possibili esiti del lancio di 2 dadi, $Y = \mathbb{N}$ e $\varphi(\ell) =$ totale ottenuto con il lancio ℓ. Generalizzare il problema ad un lancio di un numero arbitrario, ma fisso, n di dadi.

7. X insieme dei possibili esiti di 3 lanci consecutivi di una moneta, $Y = [0,1]$, $\phi(s) =$ probabilità che esca "testa" al quarto lancio dopo la successione s.

8. Sia S un insieme arbitrario non vuoto, e sia X l'insieme i cui elementi sono le applicazioni $f\colon S \to S$. Sia $Y = \mathcal{P}(S)$ (l'insieme delle parti di S) e $\varphi(f) =$ immagine di f.

80. Siano X, Y e Z insiemi e $f\colon X \to Y$, $g\colon Y \to Z$ delle applicazioni. Si determini la composizione $g \circ f\colon X \to Z$ in ciascuno dei casi seguenti:

1. $X = Y = Z = \mathbb{R}$, $f(x) = x^2 + 1$ e $g(x) = (x-1)^2$.

2. $X = Z = \mathbb{R}$, $Y = \{x \in \mathbb{R} \mid x > 0\}$, $f(x) = x^2$, $g(x) = \sqrt{x}$.

3. $X = \mathbb{R} - \{0\}$, $Y = \mathbb{R}$, $Z = \mathbb{Z}$, $f(x) = x/|x|$ e $g(x) =$ il più piccolo numero pari $\geq x$.

4. $X = \{x \in \mathbb{R} \mid x > 0\} \times \mathbb{N}$, $Y = Z = \mathbb{R}$, $f(x,n) = x^n$, $g(x) = \log(x)$.

81. Sia X un insieme contenente almeno 2 elementi e siano $f, g\colon X \to X$ due applicazioni tali che la composizione $g \circ f$ è costante (cioè $g \circ f(x)$ è un elemento costante che non dipende da x). È vero che almeno una tra f e g è necessariamente un'applicazione costante?

82. Sia $f : \mathbb{N} \to \mathbb{N}$ l'applicazione definita da $f(n) = n^2$. Provare che non esiste una applicazione $g : \mathbb{N} \to \mathbb{N}$ tale che $f \circ g = id_{\mathbb{N}}$. Costruire due diverse applicazioni $h : \mathbb{N} \to \mathbb{N}$ tali che $h \circ f = id_{\mathbb{N}}$.

83. Sia $f : \mathbb{Z} \to \mathbb{N}$ l'applicazione definita da $f(n) = n^2 - n$ se $n \geq 0$ e $f(n) = -n + 1$ se $n < 0$. Provare che non esiste una applicazione $g : \mathbb{N} \to \mathbb{Z}$ tale che $g \circ f = id_{\mathbb{Z}}$. Costruire due diverse applicazioni $h : \mathbb{N} \to \mathbb{Z}$ tali che $f \circ h = id_{\mathbb{N}}$.

84. Sia X un insieme non vuoto qualunqe. Definiamo le applicazioni $p_1\colon X \times X \to X$ come $p_1(x,y) = x$, e $p_2\colon X \times X \to X$ come $p_2(x,y) = y$ (p_1 e p_2 sono chiamate la *prima* e la *seconda proiezione* rispettivamente).

1. Dimostrare che p_1 e p_2 sono suriettive. Esistono degli insiemi X particolari per cui p_1 e p_2 sono anche iniettive?

[1] La scacchiera è un quadrato di 8×8 case. Una torre si muove di un numero arbitrario di case in orizzontale o in verticale.

2. Si consideri l'applicazione $s\colon X \times X \to X \times X$, $s(x,y) = (y,x)$. Dimostrare che $p_1 \circ s = p_2$ e $p_2 \circ s = p_1$.

3. Si consideri l'applicazione $d\colon X \to X \times X$, $d(x) = (x,x)$. Calcolare $d \circ p_1$, $d \circ p_2$, $p_1 \circ d$ e $p_2 \circ d$. Calcolare anche $s \circ d$. Che possiamo dire di $d \circ s$?

4. Supponiamo assegnate due applicazioni f e $g\colon X \to X$. Definiamo un applicazione $f \times g\colon X \times X \to X \times X$ ponendo $f \times g(x,y) = (f(x), g(y))$. Calcolare $p_1 \circ (f \times g) \circ d$ e $p_1 \circ (f \times g) \circ d$. Calcolare anche $p_1 \circ s \circ (f \times g) \circ d$ e $p_1 \circ s \circ (f \times g) \circ d$.

85. Siano X e Y insiemi arbitrari (non vuoti) e $f\colon X \to Y$ una data funzione. Definiamo in X una relazione ϱ secondo la regola: $x \varrho x' \iff f(x) = f(x')$. Dimostrare che ϱ è una relazione di equivalenza e che la funzione $\varphi([x]) = f(x)$ definisce una biezione tra l'insieme quoziente X/ϱ e l'immagine di f.

86. Si verifichi che in $\mathbb{R}$ la relazione $x \varrho y \iff x - y \in \mathbb{Z}$ è un'equivalenza. Denotato X l'insieme quoziente e $[x] \in X$ la classe di equivalenza di $x \in \mathbb{R}$, dire se le seguenti operazioni in X sono ben definite:

$$[x] * [y] = [x + y] \quad [x] * [y] = [xy] \qquad [x] * [y] = [x - y]$$

$$[x] * [y] = [2x - y] \quad [x] * [y] = [x^2] \quad [x] * [y] = [\max\{x, y\}]$$

87. Sia X l'insieme quoziente definito nel problema precedente. Si dimostri che la funzione $f\colon X \to \mathbb{R}^2$ definita da $f([t]) = (\cos(2\pi t), \sin(2\pi t))$ è una biezione tra X e la circonferenza di centro l'origine 0 e raggio 1.

88. Si verifichi che in $\mathbb{Z}$ la relazione $n \rho m \iff n - m$ é pari è un'equivalenza. Denotato $\mathbb{Z}_2$ l'insieme quoziente e $[n] \in \mathbb{Z}_2$ la classe di equivalenza di $n \in \mathbb{Z}$, dire se le seguenti operazioni in $\mathbb{Z}_2$ sono ben definite:

$$[n] * [m] = [n + m^2] \qquad [n] * [m] = [nm] \qquad [n] * [m] = [n]$$

$$[n] * [m] = [n!m!] \quad [n] * [m] = [\min\{n, m\}] \quad [n] * [m] = [n + m]$$

89. Sia $\mathbb{Z}_2$ come nell'esercizio precedente. Si consideri il sottoinsieme di $\mathbb{Z}_2 \times \mathbb{Z}$ costituito dalle coppie della forma $([n], n)$ per ogni $n \in \mathbb{Z}$. È il grafico di una funzione $\mathbb{Z}_2 \to \mathbb{Z}$? La relazione inversa (ottenuta scambiando l'ordine degli elementi delle coppie) è il grafico di una funzione $\mathbb{Z} \to \mathbb{Z}_2$?

90. Sia $\mathbb{Z}_2$ come negli esercizi precedenti. Perché $f([n]) = 3n+1$ non definisce una funzione $f : \mathbb{Z}_2 \to \mathbb{Z}$? È vero che $g([n]) = [3n + 1]$ definisce una funzione di $\mathbb{Z}_2$ in se stesso?

91. Sia $\mathbb{Z}_2$ come negli esercizi precedenti. Verificare che $f(n) = [3n + 1]$ definisce una funzione $f : \mathbb{Z} \to \mathbb{Z}_2$. Determinare

$$f(7),\ f(8),\ f(\{-2,-1,0,1\}),\ \mathrm{Im}(f),\ f^{-1}([7]),\ f^{-1}(\{[-1],[7]\}).$$

4 Calcolo Combinatorio

92. Per *anagramma* di una certa parola, si intende un qualunque riordinamento delle lettere che costituiscono quella parola. Contrariamente a quanto succede in enigmistica, in

matematica NON si richiede che il nuovo riordinamento delle lettere formi una parola di senso compiuto. Calcolare quanti sono gli anagrammi delle parole seguenti:

$$SE,\ ICS,\ NONO,\ SOMMA,\ INSIEME,\ ANAGRAMMA.$$

93. In quanti modi si possono disporre 8 torri su di una scacchiera[2] vuota in modo che nessuna torre ne attacchi un'altra?

94. Sia A un numero intero avente due soli divisori primi (cioè A è della forma $A = p^\alpha q^\beta$ con p e q primi). Quanti sono i rettangoli aventi base ed altezza di lunghezza intera e area uguale ad A?

95. Sia $V = p^n$ un numero intero potenza di un primo p. Quanti sono i parallelepipedi aventi lati di lunghezza intera e volume V? (Per semplicità, si pensino i lati assegnati in un certo ordine, come larghezza, profondità, altezza)

96. Dati 5 punti del piano, a 3 a 3 non allineati, quante sono le rette che per passano per 2 di tali punti? Cambia la risposta se anzichè nel piano i 5 punti sono scelti nello spazio? Qual'è la risposta nel caso generale di $n \geq 2$ punti, con la medesima condizione che siano a 3 a 3 non allineati?

97. Una gelateria vende gelato di 15 gusti differenti. È possibile comprare coni di 1, 2, 3 o 4 gusti. Quanti gelati differenti si possono acquistare in quella gelateria?

98. Un gruppo di 5 bambini e 5 bambine gioca a girotondo. In quanti modi si possono disporre? In quante di queste disposizioni ogni bambino è sempre fra due bambine e ogni bambina fra due bambini?

99. Si hanno a disposizione 6 vernici di colori diversi, con cui si vogliono dipingere le 4 pareti di una stanza, usando un solo colore per parete.

1. In quanti modi si possono dipingere le pareti se si decide di non usare più volte uno stesso colore?
2. In quanti modi se si decide che è possibile usare più volte uno stesso colore?
3. In quanti modi se si decide che è possibile usare più volte uno stesso colore, purchè non su pareti adiacenti?

100. Alla finale olimpica dei 100 metri piani sono ammessi otto atleti. Quante sono le possibili graduatorie dei tre vincitori di medaglia?

101. Quante sono le partite disputate nel girone di andata di un torneo di calcio a 20 squadre?

102. Prima di una partita di calcio i giocatori le due squadre (11 giocatori ciascuna) si scambiano una stretta di mano in segno d'amicizia, e anche ogni giocatore con ciascuno dei tre arbitri. Quante sono in totale le strette di mano?

103. Siano $A = \{1, 2, 3, 4, 5\}$, $B = \{1, 2, 6, 4\}$, $C = \{1, 2\}$.

1. Determinare il numero di applicazioni $\phi : A \to B$ tali che $\phi(C) \subseteq C$.
2. Sia $f : A \to B$ una fissata applicazione suriettiva. Quante sono le applicazioni $g : B \to A$ tali che $f \circ g = \mathrm{id}_B$?

[2]Nel gioco degli scacchi la torre si muove di un numero arbitrario di case su di una fila orizzontale o verticale. La scacchiera è costituita da 64 case disposte in un quadrato di 8 file di 8 case.

3. Sia $h : B \to A$ una fissata applicazione iniettiva. Quante sono le applicazioni $k : A \to B$ tali che $k \circ h = \mathrm{id}_B$?

104. Nel Gioco del Lotto vengono estratti 5 numeri su un totale di 90. Nei problemi seguenti si richiede di calcolare il numero delle estrazioni possibili che verificano certe condizioni stabilite di volta in volta. Per semplicità si ignori il fatto che nel gioco reale avvengono 10 estrazioni simultanee su altrettante "ruote", cioè si effettuino i conti sulle estrazioni di una singola ruota.

1. Calcolare il numero di tutte le possibili estrazioni.
2. Calcolare il numero delle estrazioni composte da 4 numeri dispari ed un numero pari. In quante di queste il numero pari è consecutivo di uno dei dispari?
3. Data un'estrazione, qual è il numero degli ambi e dei terni vincenti? Giocando un ambo solo, od un terno solo, qual'è la probabilità[3] di vincere?
4. Quante sono le estrazioni in cui compare esattamente un numero ad una cifra? Quante quelle in cui compare almeno un numero ad una cifra?
5. Quante sono le estrazioni i cui numeri divisi per 5 danno sempre lo stesso resto?
6. Quante sono le estrazioni costituite da numeri primi?

5 Numeri

105. Scelto un numero intero a con $2 \leq a \leq 9$, scrivere in base a i seguenti numeri in base 10:

$$11, \quad -32, \quad 107, \quad 229, \quad -513, \quad 1403, \quad 3260, \quad -7771, \quad 10055.$$

106. I seguenti numeri sono scritti in base 12 con $A = 10$ e $B = 11$. Trascriverli prima in base 10 e poi in base 8.

$$2A, \quad AB, \quad 2B0, \quad 709, \quad 2661, \quad A0A1, \quad BA3B, \quad 3ABA3, \quad B1AAA.$$

107. Scrivere in forma decimale le seguenti frazioni (elementi di $\mathbb{Q}$):

$$1/17, \quad 11/18, \quad -23/7, \quad -35/121, \quad 101/313, \quad 2004/713, \quad 2005/33.$$

108. Scrivere i seguenti numeri razionali in forma di frazione:

$$0,58 \qquad 0,5\overline{8} \qquad 0,\overline{58} \qquad 1,0\overline{01} \qquad 1,\overline{001}$$

$$1,27\overline{31} \quad 1,273\overline{1} \quad -2,\overline{117} \quad -2,1\overline{17} \quad -2,11\overline{7}$$

109. Fattorizzare i seguenti numeri interi come prodotto di numeri primi

$$927, \quad -1800, \quad 3575, \quad -14365, \quad -1936, \quad 3589, \quad 11011, \quad 48841.$$

110. Sia n un numero intero non primo, $n > 1$. Dimostrare che esiste un fattore primo p di n con $p \leq \sqrt{n}$.

[3] dato un insieme finito A ed un suo sottoinsieme B, la probabilità che un elemento di A appartenga a B è, *per definizione*, il rapporto $|B|/|A|$.

111. Sia p un numero primo e $j \in \{1, \ldots, p-1\}$. Dimostrare che p divide il coefficiente binomiale $\binom{p}{j}$.

112. Sia n un intero positivo, e sia p un numero primo. Poniamo $\alpha = [n/p]$ dove $[x]$ denota la parte intera di x. Dimostrare che p^α divide $n!$. Nella fattorizzazione di $n!$, il primo p compare sempre esattamente con esponente α?

113. Per ciascuna delle coppie di numeri interi seguenti, usare la fattorizzazione in primi per determinare un massimo comun divisore dei due numeri.

$$(28, 35) \quad (1, -1) \quad (-8, 44) \quad (10, 75) \quad (81, 693)$$

$$(87, 187) \quad (120, 133) \quad (-159, -185) \quad (-192, 243) \quad (143, -187)$$

114. Risolvere da capo l'esercizio precedente usando l'algoritmo di divisione euclidea. Inoltre, per ciascuna coppia (a, b) con massimo comun divisore d, determinare interi x ed y tali che $d = ax + by$.

115. Si fissi un intero $d \in \mathbb{Z}$. Consideriamo $d\mathbb{Z} = \{n = dm \,|\, m \in \mathbb{Z}\}$ (cioè, l'insieme dei multipli di d in $\mathbb{Z}$). Mostrare che per ogni $a, b \in d\mathbb{Z}$ e per ogni $m \in \mathbb{Z}$, gli interi $a + b$, ab e na sono in $d\mathbb{Z}$. Per quali valori di d si ha $d\mathbb{Z} = \mathbb{Z}$?

116. Si fissi un intero $d \in \mathbb{Z}$. Denotiamo $\frac{1}{d}\mathbb{Z}$ il sottoinsieme dei numeri razionali che si possono scrivere nella forma n/d con $n \in \mathbb{Z}$ (frazione NON necessariamente ridotta ai minimi termini). Mostrare che:

1. $\mathbb{Z} \subseteq \frac{1}{d}\mathbb{Z}$. Per quali valori di d si ha $\frac{1}{d}\mathbb{Z} = \mathbb{Z}$? Esistono valori di d per cui $\frac{1}{d}\mathbb{Z} = \mathbb{Q}$?

2. È vero che per ogni $a, b \in \frac{1}{d}\mathbb{Z}$ e per ogni $n \in \mathbb{Z}$ si ha $a + b, ab$ e $na \in \frac{1}{d}\mathbb{Z}$?

117. Trovare, quando possibile, una soluzione in $\mathbb{Z}^2$ delle seguenti equazioni

$$2x - 5y = 8, \quad 12x + 9y = 6, \quad 6x - 15y = 8, \quad 20x + 14y = -10, \quad 7x - 8y = 4.$$

118. In $\mathbb{Q}$ ed in $\mathbb{R}$ si consideri la relazione $x \varrho y$ se e soltanto se $x - y \in \mathbb{Z}$. In entrambi i casi la relazione è un'equivalenza. Si denotino $\mathbb{Q}/\mathbb{Z}$ e $\mathbb{R}/\mathbb{Z}$ i rispettivi insiemi quozienti, $[x]$ la classe di $x \in \mathbb{Q}$ in $\mathbb{Q}/\mathbb{Z}$ e $\{x\}$ la classe di $x \in \mathbb{R}$ in $\mathbb{R}/\mathbb{Z}$.

1. Siccome $\mathbb{Q} \subset \mathbb{R}$ possiamo definire una funzione $\iota : \mathbb{Q}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ ponendo $\iota([q]) = \{q\}$. Si dimostri che la funzione ι è ben definita, iniettiva ma non suriettiva.

2. Dimostrare che in $\mathbb{Q}/\mathbb{Z}$ l'operazione $[x] + [y] = [x + y]$ è ben definita. Spiegare perchè l'operazione $[x][y] = [xy]$ non è ben definita. Fare la stessa cosa (con l'ovvio cambio di notazione per le classi) in $\mathbb{R}/\mathbb{Z}$.

3. Sia $n > 0$ un numero intero. Per il punto precedente possiamo porre $n[x] = [x] + \cdots + [x]$ (n volte) in $\mathbb{Q}/\mathbb{Z}$ e $n\{x\} = \{x\} + \cdots + \{x\}$ (n volte) in $\mathbb{R}/\mathbb{Z}$. Mostrare che $n[x] = [nx]$ e $n\{x\} = \{nx\}$.

4. Mostrare che per ogni $[x] \in \mathbb{Q}/\mathbb{Z}$ è possibile trovare un $n > 0$ tale che $n[x] = 0$. Mostrare che in $\mathbb{R}/\mathbb{Z}$ esistono elementi $\{x\}$ tali che $n\{x\} \neq 0$ per ogni intero positivo n.

5. Sia X l'immagine della mappa ι definita sopra. Mostrare che X coincide con l'insieme delle classi $\{x\} \in \mathbb{R}/\mathbb{Z}$ tali che $n\{x\} = 0$ per qualche intero positivo n.

119. Sia $q \in \mathbb{Q}$, $q \neq 0$. Dimostrare che q si può scrivere in modo unico nella forma $q = 5^n \cdot (a/b)$ dove $n \in \mathbb{Z}$ ed a, b interi relativi coprimi,nessuno dei quali divisibile per 5. L'esponente n nella scrittura di q sopra è detto *ordine di q in 5* e denotato $\mathrm{ord}_5(q)$. Posto convenzionalmente $\mathrm{ord}_5(0) = +\infty$, mostrare che la funzione ord_5 soddisfa le seguenti regole

$$\mathrm{ord}_5(qq') = \mathrm{ord}_5(q) + \mathrm{ord}_5(q'), \qquad \mathrm{ord}_5(q+q') \geq \min\{q, q'\}, \qquad \forall q, q' \in \mathbb{Q}.$$

Cosa cambia se al posto di 5 si usa un qualunque altro primo p?

120. Verificare che i seguenti numeri sono algebrici trovando per ciascuno di essi un polinomio esplicito a coefficienti razionali che li ammette come radice :

$$\sqrt[3]{2} - 1, \quad \sqrt{2} + \sqrt{7}, \quad \sqrt{2} + \sqrt[5]{3}, \quad \sqrt{2} + \sqrt{3} + \sqrt{5}.$$

121. Calcolare la parte reale e la parte immaginaria dei seguenti numeri complessi:

$$(1+i)^5, \quad (2-i)^3 - (1-3i)^2, \quad \frac{6+5i}{3-i}, \quad \frac{(2+i)^3}{5i^{15}}, \quad \frac{3-2i}{1+5i} + \frac{2-3i}{2-i}.$$

122. Disegnare nel piano complesso i seguenti sottoinsiemi:

1. $A = \{z \in \mathbb{C} \,|\, \mathrm{Re}(z) > \mathrm{Im}(z)\}$;
2. $B = \{z \in \mathbb{C} \,|\, z + \overline{z} = i\}$;
3. $C = \{z \in \mathbb{C} \,|\, ||z-2|| \geq 2\}$;
4. $D = \{z \in \mathbb{C} \,|\, ||z+i|| < ||z-3||\}$;
5. $E = \{z \in \mathbb{C} \,|\, z - \overline{z} \in \mathbb{R}\}$;
6. $F = \{z \in \mathbb{C} \,|\, \mathrm{Re}(z^4) = 0\}$.

123. Verificare che i seguenti numeri complessi sono radice di un polinomio a coefficienti razionali :

$$2 + \cos\left(\frac{2\pi}{5}\right) + i \sin\left(\frac{2\pi}{5}\right), \quad 3 + i\sqrt{11}, \quad \sqrt[4]{2-i}, \quad \sqrt[3]{5} + i\sqrt{3}.$$

124. Sia $n > 1$ un un numero intero. Consideriamo gli n numeri complessi

$$\zeta_k = \cos\frac{2k\pi}{n} + i \sin\frac{2k\pi}{n}, \qquad k = 0, 1, \ldots, n-1.$$

Mostrare che:

1. $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ sono tutti distinti e $||\zeta_k|| = 1$ per ogni k;
2. per ogni intero m si ha $\zeta_1^m = \zeta_r$, dove r è il resto della divisione di m per n;
3. $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ sono le n soluzioni complesse dell'equazione $X^n - 1 = 0$ (per questo motivo tali numeri sono detti *radici n-esime dell'unità*).

125. Sia a un numero complesso non nullo, e sia $\alpha \in \mathbb{C}$ tale che $\alpha^n = 1$. Siano $\zeta_0, \zeta_1, \ldots, \zeta_{n-1}$ le radici n-esime dell'unità (vedi esercizio precedente). Mostrare che i numeri complessi $\alpha_k = \alpha\zeta_k$, $k = 0, 1, \ldots, n-1$ sono soluzioni dell'equazione $X^n - a = 0$. Dedurre che detta equazione possiede n radici distinte e che $\alpha_0 + \alpha_1 + \cdots + \alpha_{n-1} = 0$.

126. Per quali numeri $a \in \mathbb{C}$ l'equazione $X^6 - a = 0$ possiede almeno una radice immaginaria?

127. Per $z = a + bi \in \mathbb{C}$ poniamo $t(z) = z + \overline{z}$ e $N(z) = z\overline{z}$. Si verifichi che $t(z)$, $N(z) \in \mathbb{R}$ e che z è sempre una radice del polinomio di 2^o grado $x^2 - t(z)x + N(z)$. Chi è, dunque, l'altra radice di questo polinomio? Dimostrare che per ogni w, $z \in \mathbb{C}$ valgono le relazioni $t(w+z) = t(w) + t(z)$ e $N(wz) = N(w)N(z)$. Dedurre, in particolare, che se $\zeta \in \mathbb{C}$ è tale che $\zeta^n = 1$ per qualche $n \in \mathbb{N}$ (un tale ζ è detto *radice dell'unità*), allora $N(\zeta) = 1$.

128. Sia $\mathcal{F}$ l'insieme di tutti i numeri reali della forma $a + b\sqrt{2}$ dove a, $b \in \mathbb{Q}$. È vero che $\mathcal{F} = \mathbb{R}$? Mostrare che se x, $y \in \mathcal{F}$ allora $x + y$, $xy \in \mathcal{F}$, e che se inoltre $x \neq 0$ allora $1/x \in \mathcal{F}$. Quali di queste affermazioni rimarrebbe vera se richiedissimo che a, $b \in \mathbb{Z}$ nella definizione di $\mathcal{F}$? Definiamo un'applicazione

$$\sigma : \mathcal{F} \longrightarrow \mathcal{F}, \qquad \sigma(a + b\sqrt{2}) = a - b\sqrt{2}.$$

Si verifichi che σ è una biezione. Per $z \in \mathcal{F}$ poniamo $\tau(z) = z + \sigma(z)$ e $\nu(z) = z\sigma(z)$. Si dimostri che $\tau(z)$ e $\nu(z) \in \mathbb{Q}$ e che z è una radice del polinomio di secondo grado $x^2 - \tau(z)x + \nu(z)$. Chi è l'altra radice?

129. Sia $\mathcal{G}$ l'insieme di tutti i numeri complessi del tipo $z = a + bi$ con a, $b \in \mathbb{Q}$. Mostrare che se x, $y \in \mathcal{G}$ allora $x + y$, $xy \in \mathcal{G}$, e che se inoltre $x \neq 0$ allora $1/x \in \mathcal{G}$. Posto $G = \{z = a + bi \in \mathcal{G} \mid a, b \in \mathbb{Z}\}$, quali delle proprietà precedenti resta valida in G? Determinare esplicitamente l'insieme dei $z \in G$ tali che $1/z \in G$.

130. Di ciascuno dei seguenti sottoinsiemi di $\mathbb{C}$ si dica se, rispetto alle operazioni usuali di somma e di prodotto, si tratta di anelli, se si tratta di campi, quali dei loro elementi sono algebrici, quali trascendenti, quali hanno inverso appartenente all'insieme stesso:

1. $A = \{a + b\sqrt{2} + c\sqrt{3} \mid a, b, c \in \mathbb{Z}\}$;
2. $B = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$;
3. $C = \{a + \pi b \mid a, b \in \mathbb{Z}\}$;
4. $C = \{ai + \sqrt{6}b \mid a, b \in \mathbb{R}\}$.

6 Aritmetica modulare

Nota: Indichiamo con $\mathbb{Z}_n$ l'insieme delle classi resto modulo n. Dato $a \in \mathbb{Z}$, la classe di a in $\mathbb{Z}_n$ sarà indicata $\overline{a}$ se il modulo n è chiaro dal contesto, altrimenti useremo la notazione $[a]_n$.

131. Calcolare le seguenti espressioni in $\mathbb{Z}_n$, dove n è specificato di volta in volta.

$$[2]_3[5]_3 + [4]_3, \quad [2]_4 + [3]_4 + [7]_4, \quad [10]_5[4]_5 - [9]_5, \quad [7]_{11}[4]_{11}[2]_{11},$$

$$[3]_6{}^2 - [2]_6{}^3, \quad [2]_8 + [3]_8{}^2, \quad [6]_{10}[12]_{10}{}^2, \quad [9]_{12} - [3]_{12}{}^2[4]_{12}{}^2.$$

132. Calcolare $[a]_n$ per i seguenti valori di a ed n :

$$a = 10^{13}, n = 3; \quad a = 7^{51}, n = 8; \quad a = 4^{125}, n = 5; \quad a = 5^{107}, n = 8;$$

$$a = 9^{77}, n = 13; \quad a = 3^{84}, n = 10; \quad a = 6^{101}, n = 11; \quad a = 2^{233}, n = 7.$$

133. Consideriamo $\mathbb{Z}_{54}$, l'anello delle classi di equivalenza modulo 54.

1. Trovare un intero n, $0 \leq n < 54$, tale che $\overline{n} = \overline{125}$. Ne esiste piú d'uno?
2. Esiste un intero pari nella classe di 125?
3. Esiste un intero multiplo di 3 nella classe di 125?
4. Sia m un intero fissato. Provare che esiste almeno un intero s, con $100 \leq s \leq 200$, tale che $\overline{m} = \overline{s}$.

134. Determinare la cifra finale dei seguenti numeri

$$17^{307} - 8^{75}, \quad 7^{7^7} - 5^{5^5}, \quad 3^{456009874772}$$

135. Scrivere esplicitamente la tabellina moltiplicativa di $\mathbb{Z}_{10}$ e trovare tutte le classi $\overline{a}$ per cui esiste una classe $\overline{b}$ con $\overline{a}\overline{b} = 1$.

136. Trovare tutte le coppie $(\overline{a}, \overline{b}) \in \mathbb{Z}_{12} \times \mathbb{Z}_{12}$ tali che $\overline{a}\overline{b} = \overline{0}$.

137. In $\mathbb{Z}_{24}$:

1. determinare tutti i divisori dello zero;
2. trovare tutti gli elementi $\overline{b}$ tali che $\overline{b} \cdot \overline{16} = 0$.
3. Provare che $\overline{5^k}$ è invertibile in $\mathbb{Z}_{24}$ per ogni $k \in \mathbb{N}$. Possiamo allora dire che gli elementi invertibili di $\mathbb{Z}_{24}$ sono infiniti?
4. determinare tutti gli elementi invertibile e le loro classi;

138. Diciamo che $\overline{a} \in \mathbb{Z}_n$ è un *quadrato* se esiste $\overline{b} \in \mathbb{Z}_n$ tale che $\overline{b}^2 = \overline{a}$. Trovare esplicitamente tutti i quadrati in $\mathbb{Z}_n$ per $n = 2, 3, \ldots, 10$. In particolare, trovare per quali di questi n esistono classi $\overline{a} \neq \overline{0}$ tali che $\overline{a}^2 = \overline{0}$.

139. Determinare esplicitamente l'insieme delle potenze della classe di 2 in $\mathbb{Z}_{14}$, $\mathbb{Z}_{15}$ e $\mathbb{Z}_{16}$.

140. Risolvere (se possibile) le congruenze:

$$3x \equiv 7 \bmod 11, \quad 8x \equiv 18 \bmod 30 \quad 9x \equiv 12 \bmod 20$$

$$2x \equiv 11 \bmod 13 \quad 8x \equiv 4 \bmod 10 \quad 4x \equiv 7 \bmod 15$$

$$x^2 \equiv 3 \bmod 7 \quad 4x^2 \equiv 1 \bmod 9 \quad x^3 \equiv 7 \bmod 10$$

141. Esiste un intero a tale che la sua classe sia l'inversa della classe di 3 sia in $\mathbb{Z}_{16}$, sia in $\mathbb{Z}_{35}$?

142. Delle seguenti applicazioni $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ (il valore di n verrà specificato di volta in volta), disegnare il grafico e dire se sono iniettive e suriettive.

$$n = 3, f(\overline{a}) = \overline{a}^3 \qquad n = 3, f(\overline{a}) = \overline{1} + \overline{2}\overline{a}$$

$$n = 4, f(\overline{a}) = \overline{a} + \overline{a}^2 \qquad n = 4, f(\overline{a}) = \overline{2}\overline{a} - \overline{a}^3$$

$$n = 5, f(\overline{a}) = \overline{3}\overline{a} + \overline{2}\overline{a}^3 \qquad n = 6, f(\overline{a}) = \overline{3}\overline{a}^2 + \overline{a} + \overline{1}.$$

143. Dire se le seguenti applicazioni sono ben definite. In caso di risposta affermative dire se sono iniettive, suriettive, e disegnare il grafico

$$\mathbb{Z}_4 \to \mathbb{Z}_2, [a]_4 \mapsto [3a]_2 \qquad \mathbb{Z}_9 \to \mathbb{Z}_7, [a]_9 \mapsto [a]_7$$

$$\mathbb{Z}_{10} \to \mathbb{Z}_5, [a]_{10} \mapsto [2a]_5 \qquad \mathbb{Z}_6 \to \mathbb{Z}_4, [a]_6 \mapsto [1+a]_4$$

$$\mathbb{Z}_5 \to \mathbb{Z}_2, [a]_5 \mapsto [2a+1]_2 \qquad \mathbb{Z}_{12} \to \mathbb{Z}_4, [a]_{12} \mapsto [a^3 - 1]_4.$$

7 $\mathbb{Z}$ e $\mathbb{Z}_n$ come Anelli

144. Determinare un generatore dell'ideale $I = \{16h + 18k \mid h, k \in \mathbb{Z}\}$ di $\mathbb{Z}$.

145. Siano $n_1, \ldots, n_r$ numeri interi non nulli. Definire il loro MCD e provare che esiste. Generalizzare l'algoritmo euclideo e l'identità di Bézout al caso di r numeri interi.

146. Determinare il MCD di 6120, 720 e 880.

147. Sia I l'insieme dei multipli di $\overline{4}$ in $\mathbb{Z}_{18}$.

1. Determinare esplicitamente I e provare che si tratta di un ideale.
2. Considerare la relazione di equivalenza in $\mathbb{Z}_{18}$: $\overline{a} \sim \overline{b}$ se $\overline{a} - \overline{b} \in I$. Quante sono le classi di equivqlenza?
3. Determinare esplicitamente l'insieme dei multipli di $\overline{10}$ in $\mathbb{Z}_{18}$.
4. Verificare che $\overline{10} \cdot \overline{13} = \overline{10} \cdot \overline{4}$ in $\mathbb{Z}_{18}$. È vero che $\overline{13} = \overline{4}$?

148. Provare che in $\mathbb{Z}_6$ l'elemento$\overline{2}$ è primo. Verificare l'uguaglianza $\overline{2} = (\overline{-2}) \cdot \overline{2}$. È vero che $\overline{2}$ in quanto elemento primo è anche irriducibile?

149. Nell'anello $\mathbb{Z}_{24}$:

1. determinare tutti gli elementi invertibile e le loro classi;
2. determinare tutti gli zero divisori;
3. trovare tutti gli elementi $\overline{b}$ tali che $\overline{b} \cdot \overline{16} = 0$.
4. Provare che $\overline{5^k}$ è invertibile in $\mathbb{Z}_{24}$ per ogni $k \in \mathbb{N}$. Possiamo allora dire che gli elementi invertibili di $\mathbb{Z}_{24}$ sono infiniti?

150. Dire se le seguenti equazioni hanno soluzioni intere:

$$35x + 84y = 6 \qquad 35x + 84y + 12z + 1975 \quad 49x + 168y = 14.$$

151. L'equazione $\overline{3522} \cdot \overline{x} = \overline{1}$ ha soluzioni in $\mathbb{Z}_{500}$?

152. Trovare un intero n tale che $([n]_4, [n]_9) = ([3]_4, [7]_9)$ in $\mathbb{Z}_4 \times \mathbb{Z}_9$. Ne esiste piú d'uno?

153. Nell'anello $A = \mathbb{Z}_4 \times \mathbb{Z}_6$ verificare dapprima che $([1]_4, [2]_6)$ è uno zero-divisore e che $([1]_4, [3]_6)$ è una unitá. Poi, determinare l'insieme dei multipli di $[2]_4, [2]_6)$.

154. Risolvere le congruenze:

$$3x \equiv 7 \bmod 11, \quad 8x \equiv 18 \bmod 30 \quad 9x \equiv 12 \bmod 20$$

$$2x \equiv 11 \bmod 13 \quad 8x \equiv 4 \bmod 10 \quad 4x \equiv 7 \bmod 15$$

155. Provare che l'applicazione $f : \mathbb{Z}_{18} \to \mathbb{Z}_6$ definita come $f([n]_{18}) = [n]_6$ è un omomorfismo di anelli. Determinare $f^{-1}([0]_6)$ e $f^{-1}([1]_6)$.

156. Calcolare $\phi(36)$, $\phi(528)$ e $\phi(121)$, dove ϕ è la funzione di Eulero.

157. Determinare tutti gli elementi invertibili e tutti gli zero-divisori dell'anello $\mathbb{Z} \times \mathbb{Z}_6$.

158. Esiste un intero a tale che la sua classe sia l'inversa della classe di 3 sia in $\mathbb{Z}_{16}$, sia in $\mathbb{Z}_{35}$?

159. Verificare che $\phi : \mathbb{Z} \to \mathbb{Z}_n$ definita da $\phi(a) = \overline{a}$ è un omomorfismo di anelli (detto omomorfismo canonico) e provare che $\phi^{-1}(\overline{a}) = a + n\mathbb{Z} = \{a + nk \,|\, k \in \mathbb{Z}\}$.

160. Verificare che $I = \{n \in \mathbb{Z} \,|\, n$ è multiplo di 18 e di $24\}$ è un ideale di $\mathbb{Z}$ e trovare un suo generatore.

161. Descrivere gli ideali di $\mathbb{Z}$ che contengono $12\mathbb{Z}$ e quelli contenuti in $12\mathbb{Z}$.

162. Provare che in $\mathbb{Z}_4 \times \mathbb{Z}_2$ ogni elemento è unità oppure zero-divisore.

163. Siano n ed m due interi non nulli. Generalizzando l'esercizio precedente, provare che in $\mathbb{Z}_m \times \mathbb{Z}_n$ ogni elemento è unità oppure zero-divisore.