Corso "Matematica Discreta e Algebra Linerare"
Anno accademico 2015-2016

LISTA DOMANDE PER L'ORALE BREVE.
MODULO DI MATEMATICA DISCRETA.

1. Dimostrare una delle leggi che coinvolgono l'intersezione, l'unione, il complementare di insiemi contenute nel Teorema 5.2 (la legge viene scelta dalla commissione).
2. Esporre l'enunciato del principio di induzione e del principio del minimo.
3. Fare una dimostrazione in cui si usa il principio di induzione.
4. Fare una dimostrazione in cui si usa il principio del minimo.
5. Definire la successione di Fibonacci e dare una formula esplicita per i numeri di Fibonacci. Spiegare.
6. Saper spiegare il metodo per (provare a) trovare una formula esplicita per una successione definita per ricorrenza lineare e a coefficienti costanti.
7. Dare le definizioni di funzione iniettiva, surgettiva, bigettiva, funzione composta, immagine di una funzione, controimmagine di un elemento, controimmagine di un sottoinsieme.
8. Date $f : X \to Y$ e $g : Y \to Z$, è vero o falso che $g \circ f$ iniettiva implica f iniettiva? È vero o falso che $g \circ f$ iniettiva implica g iniettiva? Spiegare.
9. Date $f : X \to Y$ e $g : Y \to Z$, è vero o falso che $g \circ f$ surgettiva implica f surgettiva? È vero o falso che $g \circ f$ surgettiva implica g surgettiva? Spiegare.
10. Teorema di divisione euclidea: enunciato e dimostrazione.
11. Dare la definizione di massimo comune divisore, descrivere l'algoritmo di Euclide e saperlo dimostrare. Saper applicare l'algoritmo a casi specifici.
12. Identità di Bezout: dire cosa è e saperla determinare in casi specifici.
13. Siano $a, b, c \in \mathbb{Z}$, con a, b non entrambi nulli. Esporre una condizione necessaria e sufficiente perché l'equazione diofantea $ax + by = c$ abbia soluzione e saperla dimostrare.
14. Definizione di congruenza modulo m. Dimostrazione delle principali proprietà delle congruenze. Condizione di invertibilità modulo m.
15. Enunciare i criteri di divisibilità per 3 e per 11 e saper spiegare perché funzionano.
16. Esporre una condizione necessaria e sufficiente perché l'equazione $ax \equiv b \mod m$ abbia soluzione e saperla dimostrare.
17. Definizione di numero primo e teorema di caratterizzazione dei primi.

18. Enunciato e dimostrazione del teorema di fattorizzazione unica degli interi. Saper dimostrare che $\sqrt{2}$ è irrazionale.

19. Dimostrare che i numeri primi sono infiniti.

20. Enunciare e dimostrare il teorema cinese del resto per due equazioni. Risoluzione di sistemi di congruenze. Discussione della risolubilità di sistemi di congruenze con parametri.

21. Dare la definizione di classe di congruenza. Definire $\mathbb{Z}_m$ e le oerazioni che lo rendono un anello. Dimostrare che $\mathbb{Z}_m$ è un campo se e solo se m è primo.

22. Enunciare e dimostrare il 'piccolo teorema di Fermat'.

23. Risolvere una congruenza esponenziale.

24. Saper spiegare il metodo RSA e saperlo applicare ad esempi concreti

25. Dato un insieme X di cardinalità n e un insieme Y di cardinalità m, quante sono le funzioni da X a Y? E quante sono le funzioni iniettive da X a Y? (Considerare i casi $n > m$ e $n \leq m$). Spiegare.

26. Dato un insieme finito X di cardinalità $n \geq 0$, qual è la cardinalità del suo insieme delle parti? Spiegare.

27. Sia $n \in \mathbb{N}$ e sia $0 \leq r \leq n$. Dare la definizione di $\binom{n}{r}$ e dimostrare la formula

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$

28. Sia $n \in \mathbb{N}$ e sia $0 \leq r \leq n$. Dare la definizione di $\binom{n}{r}$ e spiegare come mai $\binom{n}{n-r} = \binom{n}{r}$.

29. Sia $n \in \mathbb{N}$ e sia $1 \leq r \leq n-1$. Dimostrare la formula

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$$

con ragionamenti sugli insiemi

30. Considerato il poker a 52 carte, saper contare quante sono le mani che contengono: un calore oppure una scala oppure nessun punto, oppure un poker oppoure un full, oppure un tris, oppure una doppia coppia, oppure una coppia.

31. Sia $n \in \mathbb{N}$. Quanto vale $\sum_{i=0}^{n} \binom{n}{i}$? Spiegare.

32. Sia $n \in \mathbb{N}$. Quanto vale $\sum_{i=0}^{n} (-1)^i \binom{n}{i}$? Spiegare.

33. Enunciare e dimostrare il principio di inclusione-esclusione per 2,3 o 4 insieme.

34. Contare le funzioni surgettive da un insieme X di cardinalità n ad un insieme Y di cardinalità $n-1$ o $n-2$.

35. Spiegare come mai per ogni $a \in \mathbb{Z}$ vale $a^{561} \equiv a \mod 561$.

36. Anello dei polinomi con coefficienti in un campo: operazioni, proprietà' del grado.

37. Enunciato del teorema di divisione tra polinomi. Algoritmo di divisione tra polinomi. Algoritmo di Euclide per il calcolo del massimo comune divisore tra polinomi.

38. Teorema di Ruffini enunciato e dimostrazione.

39. Definizione di polinomio irriducibile, Teorema di fattorizzazione unica in $K[x]$ (enunciato) e sue conseguenze (dimostrazione che un polinomio di grado n ha al più' n radici in un campo).

40. Numeri complessi passaggio dalla forma algebrica alla forma trigonometrica. Calcolo di potenze e radici. Radici n-esime di 1.

41. Enunciato del teorema fondamentale dell'algebra e dimostrazione delle sue conseguenze per polinomi con coefficienti reali. Polinomi irriducibili in $R[x]$.

42. Fattorizzazione in $Q[x]$: ricerca delle radici, enunciato lemma di Gauss, criterio di Eisenstein.

43. Fattorizzazione in $\mathbb{Z}_p[x]$. Dimostrazione della proposizione: se f e' un polinomio di $\mathbb{Z}[x]$ che e' irriducibile in $\mathbb{Z}_p[x]$, allora f e' irriducibile anche in $\mathbb{Z}[x]$.

44. Fattorizzazione di polinomi del tipo $x^n - a$ in $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$.

Modulo di Algebra Lineare.

45. Mostrare l'algoritmo di eliminazione di Gauss per la soluzione di un sistema lineare e dimostrare che esso non cambia le soluzioni del sistema.

46. Enunciare il metodo per trovare una base di $\operatorname{im} A$ e mostrare perché funziona (cioè perché i vettori trovati sono una base).

47. Enunciare il metodo per trovare una base di $\ker A$ e mostrare perché funziona.

48. Enunciare e dimostrare i criteri basati sul numero dei pivot trovati facendo l'eliminazione di Gauss per dire quando una funzione del tipo $f(\vec{x}) = A\vec{x}$ è iniettiva o suriettiva.

49. Definizione di matrice invertibile/singolare e algoritmo per il calcolo dell'inversa di una matrice.

50. Mostrare che per ogni matrice $\dim \ker A + \dim \operatorname{im} A$ è uguale al numero di colonne.

51. Definire spazio e sottospazio vettoriale e saper dimostrare che un insieme (scelto dalla commissione; ad esempio un kernel o uno span) è un sottospazio vettoriale

52. Definire base (e quindi anche insieme di vettori generanti/indipendenti), coordinate, e dimostrare che le coordinate esistono e sono uniche.

53. Metodo per scrivere un sottospazio (dato tramite generatori) come ker di una matrice (e saper spiegare perché funziona).

54. Saper verificare se un'applicazione è lineare e costruire la matrice associata ad essa (anche su un esempio concreto).

55. Saper trovare nucleo/immagine di un'applicazione lineare (non solo da $\mathbb{R}^m$ a $\mathbb{R}^n$, ma anche tra spazi vettoriali diversi), anche su un esempio concreto.

56. Formula per trovare la matrice associata a un'applicazione lineare (da $\mathbb{R}^n$ a $\mathbb{R}^m$) secondo due basi date a partire da quella nelle basi canoniche.

57. Proprietà della matrice trasposta e dimostrazione che $\operatorname{rk} A^\top = \operatorname{rk} A$.

58. Determinante: definizione tramite la formula con $n!$ addendi (formula di Leibniz) e proprietà (linearità, comportamento rispetto a scambi di righe, comportamento rispetto a prodotto e trasposta...).

59. Metodi alternativi per calcolare il determinante: tramite eliminazione di Gauss e ricorsivamente (formula di Laplace).

60. Definizione di autovalori e autovettori di una matrice e loro metodo di calcolo (con giustificazione).

61. Relazione tra gli autovalori e autovettori di A e quelli di $V^{-1}AV$ (cambiamento di base).

62. Relazione tra autovalori, autovettori e fattorizzazione $A = VDV^{-1}$, e utilizzo di questa fattorizzazione per il calcolo delle potenze di una matrice.

63. Definizione di molteplicità algebrica e geometrica, e dimostrazione che $1 \leq m_g(\lambda_i) \leq m_a(\lambda_i)$ per ogni autovalore.

64. Relazione tra autovalori, traccia, determinante, e coefficienti del polinomio caratteristico (con giustificazione).

65. Definizione di ortogonalità, norma, e sue proprietà rispetto alle operazioni. Esempi di sottospazi definiti tramite ortogonalità.

66. Sistemi di vettori ortogonali e ortonormali; ortogonali implica linearmente indipendenti. Calcolo di coordinate rispetto a una base ortonormale.

67. Metodo di ortogonalizzazione di Gram-Schmidt: enunciare almeno l'idea e la versione per due vettori (e saperla applicare).