Algebra per l'informaticaGuida allo studio dell'esame

Ecco una breve guida, non esaustiva, al materiale che può comparire sugli esami.

- Lezione 1:
  (i) Il principio del buon ordinamento (enunciato formale).
  (ii) Il principio di induzione (enunciato formale).
  (iii) Dimostrazione per Induzione (Dimostrazione basata sul principio del buon ordinamento o sul principio di induzione).
  (iv) La dimostrazione di Euclide dell'esistenza di infiniti numeri primi.
  (v) Dimostrazione del teorema della divisione.
  (vi) Costruire dimostrazioni per induzione (Esempio: il teorema binomiale).
- Lezione 2:
  (i) Definizione di massimo comune divisore e minimo comune multiplo.
  (ii) Algoritmo di Euclide (enunciato formale)
  (iii) Dimostrazione che mcd$(a+b,b)=$ mcd(a,b)
  (iv) Identità di Bézout (enunciato formale).
  (v) Calcolo di $m=$ mcd(a,b) e determinazione degli interi u e v tali che $m=au+bv$.
- Lezione 3:
  (i) Lemma di Euclide (enunciato formale)
  (ii) Teorema fondamental dell'arithmetica (enunciato formale, dimostrazione della prima parte che tratta l'esistenza di una scomposizione in fattori primi.)
  (iii) Il piccolo teorema di Fermat (enunciato formale, dimostrazione – induzione o la teoria dei gruppi vanno entrambe bene).
  (iv) Calcolo mcm(a,b).
- Lezione 4:
  (i) Definizione di mcd e mcm per polinomi in $\mathbb{Q}[x]$.
  (ii) Teorema di divisione per polinomi in $\mathbb{Q}[x]$ (enunciato formale)
  (iii) Teorema di Fattorizzazione Unica per polinomi in $\mathbb{Q}[x]$ (enunciato formale).
  (iv) Teorema delle radici razionali.
  (v) Calcolo di $m=$ mcd(p,q) e determinazione di $u, v\in\mathbb{Q}[x]$ tale che $m=up+qv$.
  (vi) Determinazione delle radici razionali di $f\in\mathbb{Z}[x]$.
- Lezione 5:
  (i) Definizione di reticolo e matrici unimodulari.
  (ii) $L(B)=L(C)$ se e sole se esiste una matrice U unimodulare tale che $C=BU$.
  (iii) Volume del parallelepipedo fondamentale.
  (iv) Algoritmo di Gauss (enunciato formale).
  (v) Calcolo di vettori di lunghezza minima tramite l'algoritmo di Gauss.
  (vi) Dimostrazione che due reticoli non sono equivalenti.
- Lezione 6:
  (i) Definizione relazioni riflessive, simmetriche, antisimmetriche e transitive. Definizione di relazione di equivalenza e ordini parziali.
  (ii) Dimostrare che una relazione di equivalenza definisce una partizione.
  (iii) Dimostrare che una partizione definisce una relazione di equivalenza.
  (iv) Risolvi problemi della forma "Dimostra che R è una relazione di equivalenza".

(v) Risolvi problemi della forma “Costruisci una biiezione da X modulo R a Y”.

- Lezione 7:
  (i) Mostra che $\mathbb{Z}_n$ è un anello commutativo con identità.
  (ii) Mostra che $[a]$ ha un inverso in $\mathbb{Z}_n$ se e solo se mcd$(a, n) = 1$.
  (iii) Mostra che se m e n sono coprimi allora $\mathbb{Z}_{mn}$ è isomorfo a $\mathbb{Z}_n \times \mathbb{Z}_m$ (dimostrazione).
  (iv) Definizione e proprietà della funzione toziente di Eulero ϕ.
  (v) Formula del prodotto di Eulero per ϕ.
  (vi) Il teorema di Eulero mcd$(a, n) = 1$ implica che $a^{phi(n)} = 1 \mod n$.
  (vii) Trova l’inversa di una matrice modulo m. Risolvere sistemi lineari modulo m.
  (viii) Calcola $\phi(n)$, calcola le potenze usando $\phi(n)$.
  (ix) Mostra che un dominio d’integrità finito è un campo.
- Lezione 8 & 9:
  (i) Definizione di gruppo, sottogruppi, gruppi normali (enunciati, esempi).
  (ii) Teorema del fattore invariante (enunciato, applicazione).
  (iii) Numero di possibili gruppi abeliani (enunciato, applicazione).
  (iv) Il teorema di Lagrange (enunciato, dimostrazione).
  (v) Dimostrazione del teorema di Fermat e di Eulero usando il teorema di Lagrange.
  (vi) Formula delle Classi di Coniugio.
  (vii) Il kernel e le immagini di un omomorfismo di gruppo sono sottogruppi.
  (viii) Gruppi quoziente. Gruppi quoziente.
  (ix) Questa sezione contiene 28 esercizi per lo studente.
- Lezione 10:
  (i) Definizione di un campo.
  (ii) Dimostra che l’intersezione di due campi è un campo. Definizione del sottocampo primo.
  (iii) Un’estensione L di K è uno spazio K-vettoriale (dimostrazione).
  (iv) Se $[L : K]$ è finito allora ogni elemento di L è algebrico su K (dimostrazione).
  (v) La legge della torre per le estensioni del campo (enunciato formale, dimostrazione).
  (vi) Definizione del polinomio minimo.
  (vii) L’irriducibilità del polinomio minimo, e coverse.
  (viii) Teorema di Fattorizzazione Unica (enunciato formale).