



## Principali informazioni sull'insegnamento

Denominazione dell'insegnamento	<b>Matematica Discreta, Track A--L</b>	
Corso di studio	Informatica e Tecnologie per la Produzione del Software	
Anno Accademico	2023/24	
Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS)	9 CFU	
Settore Scientifico Disciplinare	Mat/03-Geometria	
Lingua di erogazione	Italiano	
Anno di corso	Primo	
Periodo di erogazione	1° semestre, le date esatte sono riportate nel manifesto/regolamento	
Obbligo di frequenza	La frequenza è fortemente raccomandata	
Sito web del corso di studio	<a href="https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/informatica-tps-270/laurea-triennale-in-informatica-e-tecnologie-per-la-produzione-del-software-d.m.-270">https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/informatica-tps-270/laurea-triennale-in-informatica-e-tecnologie-per-la-produzione-del-software-d.m.-270</a>	

## Docente/i

Nome e cognome	Vincenzo Carmine Nardoza
Indirizzo mail	Vincenzo.nardoza_AT_uniba.it
Telefono	+39 080 5442692
Sede	Dipartimento di Matematica, Via Orabona 4, 70125, Bari. Stanza n.16, 3° piano.
Sede virtuale	<a href="https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/informatica-tps-270/laurea-triennale-in-informatica-e-tecnologie-per-la-produzione-del-software-d.m.-270">https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/informatica-tps-270/laurea-triennale-in-informatica-e-tecnologie-per-la-produzione-del-software-d.m.-270</a>
Sito web del docente	<a href="https://www.dm.uniba.it/it/members/nardoza">https://www.dm.uniba.it/it/members/nardoza</a>
Ricevimento (giorni, orari e modalità, es. su appuntamento)	Venerdì, 10.00-12.00, su appuntamento. Per ricevimento in altri giorni/orari, consultare la pagina istituzionale: <a href="https://www.dm.uniba.it/it/members/nardoza/ricevimento">https://www.dm.uniba.it/it/members/nardoza/ricevimento</a>



Syllabus	
Obiettivi formativi	Il corso si propone di introdurre alcuni elementi base della matematica discreta. In particolare si propone di fornire gli strumenti matematici di base relativi alla logica, teoria degli insiemi, funzioni, combinatoria, numeri interi e aritmetica modulare, strutture algebriche.
Prerequisiti	Calcolo elementare, calcolo polinomiale, primi elementi di teoria degli insiemi e di logica formale. Tecniche di risoluzione di equazioni e disequazioni algebriche.



Contenuti di insegnamento  
(Programma)

### 1. Concetti di base.

- a) **Logica:** Proposizioni. Connettivi logici fondamentali e tavole di verità. Proposizioni equivalenti. Contraddizioni e tautologie. Implicazione logica e sue parafrasi. Formulazioni equivalenti della implicazione logica. Bicondizionale. Ordine di precedenza tra gli operatori logici. Regole di negazione (formule di De Morgan). Negazione dell'implicazione e della bicondizionale. Predicati e quantificatori. Regole per la negazione di una proposizione predicativa. Proposizioni dipendenti da più variabili logiche. Regole per la negazione di una proposizione predicativa. Terminologia: Definizione, Teorema, Proposizione, Lemma, Corollario, Osservazione, Esempi, Controesempi, Dimostrazioni.
- b) **Insiemistica:** Oggetti e insiemi. Appartenenza di un oggetto a un insieme. Insieme universo. Inclusione e uguaglianza insiemistica. Rappresentazioni di un insieme e costruttori logici e funzionali. Insieme vuoto; l'insieme vuoto è contenuto in ogni insieme; un insieme non cambia se si permutano i suoi elementi o se li si riportano più volte. Unione, intersezione e complementare. Proprietà elementari delle operazioni insiemistiche. Famiglia di insiemi. Leggi di De Morgan. Unione, intersezione e leggi di De Morgan per famiglie di insiemi. Insieme delle parti di un insieme.
- c) **Relazioni:** Prodotto cartesiano. Relazioni. **Funzioni:** Definizione di funzione; immagine e controimmagine di un elemento. Rappresentazione di una funzione con diagrammi di Venn, come array a due righe, come parola, tramite il modello d'occupazione. Uguaglianza tra funzioni. Composizione di funzioni. Funzione identità. Funzioni invertibili. Funzioni iniettive, suriettive e bigettive. Caratterizzazione delle funzioni invertibili. **Posets:** relazioni d'ordine parziale. Insiemi totalmente ordinati. Massimo e minimo di un sottinsieme di un poset. Insiemi ben ordinati. Ogni insieme ben ordinato è totalmente ordinato. Diagramma di Hasse di un poset. **Relazioni di equivalenza:** relazione di equivalenza su un insieme. Classi di equivalenza. Insieme quoziente. Partizione di un insieme. Equivalenza logica tra partizione di un insieme e relazione di equivalenza sullo stesso insieme.
- d) **Principio di induzione e ricorsività:** Successioni. Sommatorie. Principio di induzione matematica nelle sue formulazioni equivalenti: induzione semplice, induzione completa e principio del minimo. Procedimento di dimostrazione per induzione. **Ricorsività:** Algoritmi ricorsivi. Successioni ricorsive. Forma chiusa di una successione ricorsiva. Progressioni aritmetiche e geometriche. Numeri di Fibonacci.

### 2. Interi.

Divisibilità tra interi. Algoritmo di divisione euclidea. Rappresentazione degli interi in un sistema posizionale in base  $b > 1$ . Massimo comun divisore tra interi. Proprietà elementari del  $\text{MCD}(a, b)$ . Teorema di Bezout. Forma di Bezout per l'espressione del  $\text{MCD}(a, b)$ . Numeri coprimi. Lemma di Euclide. Algoritmo euclideo per il calcolo del MCD. Calcolo dei coefficienti di Bezout. Minimo comune multiplo tra interi. Espressione del mcm tramite il MCD. Generalità e richiami sulle equazioni. Equazioni diofantee lineari. Metodo di risoluzione delle equazioni diofantee lineari. Numeri interi primi e numeri interi irriducibili. Teorema fondamentale dell'Aritmetica. Esistenza di infiniti interi primi. Esistenza di numeri irrazionali. Crivello di Eratostene.

### 3. Combinatoria

Cardinalità e confronto di cardinalità. Insiemi finiti e infiniti. I naturali naturali costituiscono un insieme infinito. Confronto tra le cardinalità degli insiemi numerici. Cardinalità degli insiemi finiti e significato del termine "contare". Principio di addizione. Principio di moltiplicazione. Cardinalità dell'insieme delle parti di un



insieme finito. Numero di divisori di un intero. Disposizioni con ripetizione. Numero di disposizioni con ripetizione di classe  $k$  su  $n$  oggetti. Disposizioni semplici. Numero di disposizioni semplici di classe  $k$  su  $n$  oggetti. Permutazioni. Fattoriale. Combinazioni semplici. Coefficiente binomiale. Proprietà elementari del coefficiente binomiale. Triangolo di Tartaglia. Sviluppo delle potenze di un binomio. La somma dei numeri del triangolo di Tartaglia lungo una stessa riga è una potenza di 2. Formula chiusa del coefficiente binomiale. Combinazioni con ripetizioni di classe  $k$  su  $n$  oggetti. Numero di combinazioni con ripetizione di classe  $k$  su  $n$  oggetti. Multinsiemi. Principio di inclusione-esclusione. Principio dei cassetti.

#### **4. Aritmetica Modulare**

Congruenza modulo  $n$ . La congruenza modulo  $n$  è una relazione di equivalenza. Caratterizzazione alternativa della congruenza modulo  $n$ . Descrizione delle classi di congruenza. Cardinalità dell'insieme quoziente. Compatibilità della congruenza con le operazioni tra interi. Inversi aritmetici e loro determinazione. Congruenze lineari. Risolubilità di una congruenza lineare. Soluzioni di una congruenza lineare risolubile. Metodi di risoluzione di una congruenza lineare. Ripartizione in classi delle soluzioni di una congruenza lineare. Sistemi di congruenze lineari. Normalizzazione di un sistema di congruenze lineari. Prima formulazione del Teorema Cinese dei Resti. Funzione  $\varphi$  di Eulero e sue proprietà (moltiplicatività, formula per il calcolo di  $\varphi(n)$ , calcolo dell'inverso aritmetico di un intero tramite  $\varphi$ ). Teorema di Eulero-Fermat (enunciato). Se un intero  $a$  è coprimo con  $n$ , allora il minimo esponente  $k > 0$  tale che  $a^k \equiv 1 \pmod{n}$  è un divisore di  $\varphi(n)$ . Applicazioni: criteri di divisibilità per numeri  $< 17$ , sistema crittografico RSA.

#### **5. Gruppi**

Operazioni binarie su un insieme. Proprietà distintive di operazioni binarie: Associatività, commutatività, esistenza di un elemento neutro, esistenza del simmetrico di un elemento. Tavola moltiplicativa di un'operazione. Semigrupp e monoidi. Monoide libero generato da un insieme  $X$ . Definizione di gruppo. Esempi di gruppi. Notazioni additiva e moltiplicativa. Ordine di un gruppo. Addizione tra classi di congruenza modulo  $n$ . Il gruppo  $\mathbb{Z}_n$ . Lemma di cancellazione in un gruppo. Proprietà della tavola moltiplicativa di un gruppo. Proprietà elementari di un gruppo: unicità dell'elemento neutro e del simmetrico di un elemento. Potenze (o multipli) di un elemento di un gruppo e loro proprietà. Elementi periodici e aperiodici. Periodo di un elemento periodico. Tutti gli elementi di un gruppo finito sono periodici, e hanno come periodo un divisore dell'ordine del gruppo. Proprietà degli elementi aperiodici di un gruppo. Proprietà del periodo di un elemento periodico. Sottogruppo di un gruppo. In un sottogruppo elemento neutro e inversi si conservano. Lemma di caratterizzazione dei sottogruppi. Sottogruppo generato da un sottinsieme di un gruppo. Sottogruppi ciclici di un gruppo e gruppi ciclici. Relazione tra periodo di un elemento e ordine del sottogruppo ciclico da esso generato. Teorema di Lagrange per gruppi finiti. Numero di generatori di un gruppo ciclico finito. Classificazione dei gruppi ciclici. Proprietà dei gruppi ciclici. Teorema fondamentale sui gruppi abeliani finiti. Prodotto diretto di gruppi.

#### **6. Gruppi simmetrici**

Inversa della composizione di due bigezioni. Supporto di una permutazione. Permutazioni a supporto disgiunto commutano. Cicli. Orbita di un elemento sotto una permutazione. Relazione di equivalenza indotta da una permutazione. Cicli associati alle orbite di una permutazione. Decomposizione di una permutazione in un prodotto di cicli disgiunti. Struttura ciclica di una permutazione. Periodo di una permutazione. Ogni permutazione è un prodotto di trasposizioni. Parità di una permutazione e funzione segno. Gruppo alterno.



### **7. Anelli**

Definizione di anello. Anelli commutativi e anelli unitari. Proprietà di  $0$  in un anello. Divisori di zero. Elementi invertibili in un anello. Terminologia: anelli interi, domini di integrità, corpi, campi. Esempi di anelli:  $\mathbf{Z}$ ,  $\mathbf{Q}$  ed  $\mathbf{R}$ . L'anello  $\mathbf{Z}_n$ . Divisori dello zero e elementi invertibili formano sottinsiemi disgiunti. Somma diretta di anelli. Gruppo degli elementi invertibili di una somma diretta di anelli. Elementi invertibili e divisori di zero di  $\mathbf{Z}_n$ . L'anello  $\mathbf{Z}_n$  è un campo se e solo se  $n$  è primo. Omomorfismi tra anelli e loro proprietà. Nucleo di un omomorfismo e caratterizzazione dell'iniettività di un omomorfismo tramite il suo nucleo. Teorema di Eulero—Fermat e Piccolo Teorema di Fermat (dimostrazioni). Seconda formulazione del Teorema Cinese dei Resti. Moltiplicatività della funzione  $\varphi$  di Eulero e formula per il calcolo della  $\varphi$  (dimostrazioni).

### **8. Polinomi e campi finiti**

Anelli di polinomi univariati a coefficienti in un campo. Algoritmo di divisione euclidea. MCD tra polinomi e Teorema di Bezout. Polinomi primi, irriducibili ed equivalenza logica tra i due concetti. Funzioni polinomiali e radici (o zeri) di un polinomio. Teorema di Ruffini. Caratterizzazione dell'irriducibilità di polinomi di grado due e tre tramite le sue radici. Caratterizzazione dei polinomi irriducibili di  $\mathbf{C}[x]$  e di  $\mathbf{R}[x]$ . Congruenza modulo un polinomio e anelli polinomiali quoziente. Caratterizzazione degli elementi invertibili e dei divisori dello zero di un anello polinomiale quoziente tramite il MCD. Teorema:  $F[x]/(f)$  è un campo se e solo se  $f$  è un polinomio irriducibile di  $F[x]$ . Teorema: se  $f$  ha grado  $n$ , allora  $F[x]/(f)$  ha  $|F|^n$  elementi. Campi finiti. La cardinalità di un campo finito è una potenza di un primo. Costruzione del campo  $\mathbf{C}$  come quoziente di  $\mathbf{R}[x]$ . Teorema cinese dei resti per anelli quoziente.

### **9. Anelli di matrici**

Matrici a coefficienti in un campo. Addizione tra matrici quadrate e prodotto righe per colonne tra matrici. Anello delle matrici quadrate. Gruppo generale lineare  $GL_n(F)$ . Determinante di una matrice. Caratterizzazione delle matrici invertibili e delle matrici divisori di zero tramite il determinante. Formula di Binet. Calcolo esplicito del determinante per matrici di forma o taglia particolare. Inversa di una matrice  $2 \times 2$  invertibile tramite il determinante. Operazioni elementari  $R_{ij}(\alpha)$ ,  $\mu_i(\alpha)$  e  $T_{ij}$  sulle righe di una matrice. Invertibilità e calcolo dell'inversa di una matrice tramite le operazioni elementari sulle righe. Calcolo del determinante di una matrice tramite le operazioni elementari sulle righe.

### **10. Applicazione del calcolo matriciale: sistemi lineari**

Matrice completa, dei coefficienti e dei termini noti di un sistema. Matrici in forma normale e riduzione di una matrice alla sua forma normale. Rango di una matrice. Metodo di riduzione di Gauss-Jordan e riduzione di un sistema alla sua forma normale. Caratterizzazione della risolubilità di un sistema tramite la sua forma normale. Teorema di Rouché-Capelli. Numero di soluzioni di un sistema compatibile su un campo finito.



<b>Testi di riferimento</b>	<p><b>Testo adottato per il corso:</b></p> <p>G.M. Piacentini Cattaneo, "Matematica Discreta e applicazioni", Zanichelli Editore (2008)</p> <p><b>Altri testi, non obbligatori ma consigliati per consultazione o eventuali approfondimenti personali:</b></p> <ul style="list-style-type: none"><li>• C. Delizia, P. Longobardi, M. Maj, C. Nicotera, "Matematica Discreta", McGraw-Hill Editore, (2009).</li><li>• A. Facchini, "Algebra e Matematica Discreta", Decibel Zanichelli Editore (2000)</li><li>• K. H. Rosen, "Discrete Mathematics and Its Applications", McGraw-Hill, 7th Edition (2012) (in Inglese)</li><li>• R. Johnsonbaugh, "Discrete Mathematics", Pearson Education, 8th Edition (2018) (in Inglese)</li></ul> <p>Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo <a href="https://opac.uniba.it/easyweb/w8018/index.php?">https://opac.uniba.it/easyweb/w8018/index.php?</a> e contattare la biblioteca per concordare il prestito.</p>
<b>Note ai testi di riferimento</b>	<p>Gli argomenti del programma sono stati sviluppati secondo l'esposizione e la notazione presenti sul testo ufficiale adottato, <b>che pertanto è un riferimento essenziale</b> per la preparazione all'esame. Fanno eccezione i punti 7, 9 e 10 del programma, i cui contenuti sono stati presentati secondo gli appunti messi a disposizione dal docente, comprensivi di teoria ed esercizi (svolti e non).</p> <p>Inoltre, a integrazione dei contenuti di base (punto 1 del programma) è disponibile anche una raccolta di esercizi su logica, insiemistica e induzione.</p> <p>Tutto tale materiale didattico è disponibile all'indirizzo:</p> <p><a href="https://www.dm.uniba.it/it/members/nardoza/homepage/aa-2023-24/md-2023-24/md-2023-24-itps-track-a-l">https://www.dm.uniba.it/it/members/nardoza/homepage/aa-2023-24/md-2023-24/md-2023-24-itps-track-a-l</a></p> <p>Si consiglia vivamente di studiare attenendosi al materiale <b>ufficiale</b> di riferimento, diffidando da materiale di dubbia provenienza (appunti altrui, siti web, chat di studenti, etc), eventualmente verificando a ricevimento la correttezza dei propri appunti.</p>



## Organizzazione della didattica

### Ore

Totali	Didattica frontale	Pratica (esercitazione)	Studio individuale
225 ore	56 ore	30 ore	139 ore
<b>CFU/ETCS</b>			
9 CFU	7 CFU	2 CFU	

## Metodi didattici

Lezioni frontali ed esercitazioni in presenza in aula.

## Risultati di apprendimento previsti

### Conoscenza e capacità di comprensione

Acquisizione di capacità logiche formali e familiarità con concetti matematici astratti.  
Acquisizione delle tecniche dimostrative di base e di procedimenti formali, i principi dell'astrazione, le teorie formali del calcolo. Sviluppo della abilità di calcolo e di ragionamento astratto.

### Conoscenza e capacità di comprensione applicate

Le conoscenze acquisite trovano applicazione nello svolgimento di esercizi. Lo studente possiede le conoscenze per risolvere piccoli problemi, eseguire algoritmi e calcoli nelle varie strutture trattate. Acquisizione di capacità logiche e ragionamento astratto. Affinamento delle capacità di problem solving, tramite la riduzione di un problema ai suoi costituenti elementari.



<b>Competenze trasversali</b>	<p><b>Autonomia di giudizio</b> Capacità di individuare il metodo risolutivo opportuno per un particolare problema. Capacità di stabilire la coerenza e la correttezza di un ragionamento logico o di una dimostrazione. Tali abilità sono sviluppate tramite esercizi e quesiti proposti periodicamente durante il corso.</p> <p><b>Abilità comunicative</b> Acquisizione del linguaggio formale matematico, necessario per poter acquisire negli anni successivi delle competenze professionali d'avanguardia. Capacità di esporre le conoscenze acquisite in maniera chiara e rigorosa. Tali abilità sono sviluppate tramite esercizi e quesiti proposti periodicamente durante il corso.</p> <p><b>Capacità di apprendere in modo autonomo</b> Acquisizione di un metodo di studio adeguato, supportato dalla consultazione dei testi e dalla risoluzione di esercizi e quesiti proposti periodicamente durante il corso.</p>
-------------------------------	---

Valutazione	
<b>Modalità di verifica dell'apprendimento</b>	<p>Prova scritta della durata di circa 2 ore contenente esercizi a carattere algoritmico/computazionale e quesiti a carattere teorico.</p> <p>La votazione utilizzata è il voto in trentesimi.</p> <p>La prova scritta si ritiene superata se si raggiunge la valutazione di 18.</p> <p>Correzione da parte del docente e incontro per la visualizzazione dell'elaborato, prima della verbalizzazione.</p> <p>Prova orale facoltativa nello stesso appello, dopo il superamento della prova scritta. (Quindi almeno 18 alla prova scritta).</p> <p>Informazioni dettagliate, tracce passate, esercizi svolti e comunicazioni sono disponibili nella pagina ufficiale del docente:</p> <p><a href="https://www.dm.uniba.it/it/members/nardoza/homepage">https://www.dm.uniba.it/it/members/nardoza/homepage</a></p>





Criteri di valutazione	<ul style="list-style-type: none"><li>• <b>Conoscenza e capacità di comprensione:</b> Qualità e correttezza delle tecniche dimostrative, procedimenti formali e del ragionamento astratto.</li><li>• <b>Conoscenza e capacità di comprensione applicate:</b> Qualità e correttezza delle capacità logiche.</li><li>• <b>Autonomia di giudizio:</b> Correttezza delle tecniche dimostrative e del metodo risolutivo.</li><li>• <b>Abilità comunicative:</b> Qualità, chiarezza e correttezza dell'esposizione delle conoscenze acquisite.</li><li>• <b>Capacità di apprendere:</b> Correttezza degli svolgimenti e dei risultati elaborati.</li></ul>
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	<p>Il voto finale è attribuito in trentesimi. L'esame è superato quando il voto è superiore o uguale a 18.</p> <p>Il voto finale (18-30 e lode) dipende dalla conoscenza, dal rigore e dalla correttezza dello svolgimento degli esercizi nella prova scritta.</p>



## Altro

Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:

- <https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea>
- <https://www.uniba.it/it/ricerca/dipartimenti/informatica>
- <https://elearning.di.uniba.it/>

I programmi degli insegnamenti sono disponibili qui:

- <https://programmi.di.uniba.it/>

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito:

- <https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea>

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

---

### SI CONSIGLIA VIVAMENTE:

- la frequenza costante delle lezioni e delle esercitazioni;
- lo studio costante durante lo svolgimento dell'insegnamento;
- lo svolgimento costante degli esercizi proposti.
- **Materiale didattico integrativo e complementare, informazioni dettagliate, tracce passate e comunicazioni sono disponibili sul sito del docente:**  
<https://www.dm.uniba.it/it/members/nardozza>