Principali informazioni sull'insegnamento	**A.A. 2020-2021**
Titolo insegnamento	**Matematica Discreta**
Corso di studio	Informatica e Tecnologie per la Produzione del Software
Crediti formativi	9
Denominazione inglese	**Discrete Mathematics**
Obbligo di frequenza	No, ma la frequenza è fortemente consigliata
Lingua di erogazione	italiana

Docente responsabile	Nome Cognome	Indirizzo Mail e telefono
	Vincenzo Nardozza	Vincenzo.nardozza@uniba.it 080 5442692
Luogo ed orario ricevimento	**Stanza 16 3° Piano Dipartimento di Matematica**	Da concordare in base alla disponibilità dello studente e del docente tramite email. Il ricevimento avverrà in forma telematica sino al termine dell'emergenza Covid

Dettaglio credi formativi	Ambito disciplinare	SSD	Crediti
	Matematico	Mat 02/Algebra	9

Modalità di erogazione	
Periodo di erogazione	Primo semestre
Anno di corso	Primo anno
Modalità di erogazione	Lezioni frontali ed esercitazioni in aula.

Organizzazione della didattica	Lezioni frontali:	esercitazioni:
Ore totali	175	50
Ore di corso	56	30
Ore di studio individuale	119	20

Calendario	
Inizio attività didattiche	24 settembre 2019
Fine attività didattiche	10 gennaio 2020

Syllabus	
Prerequisiti	Calcolo polinomiale elementare. Rudimenti di teoria degli insiemi.
Propedeuticità obbligatorie	Nessuna
Risultati di apprendimento previsti (declinare rispetto ai Descrittori di Dublino) (si raccomanda che siano coerenti con i risultati di apprendimento del CdS, riportati nei quadri A4a, A4b e A4c della SUA, compreso i risultati di apprendimento trasversali)	• *Conoscenza e capacità di comprensione* Acquisizione di capacità logiche 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 abilita' di calcolo e di pensiero 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 sviluppare il calcolo matriciale.

	• *Autonomia di giudizio* 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. • *Abilità comunicative* Acquisizione del linguaggio formale matematico, necessario per poter acquisire negli anni successivi delle competenze professionali d'avanguardia. Capacità di esporre le conoscenze acquisite. • *Capacità di apprendere* Acquisizione di un metodo di studio adeguato, supportato della consultazione dei testi e dalla risoluzione di esercizi e quesiti proposti periodicamente durante il corso.
Contenuti di insegnamento	**(1) Concetti di base**. **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. **Insiemistica** Insieme universo, insieme, appartenenza. Inclusione e sua negazione. Uguaglianza insiemistica. Rappresentazioni di un insieme e costruttore logico. 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 complementari. Proprietà elementari delle operazioni insiemistiche. Leggi di De Morgan. Famiglia di insiemi. Unione, intersezione e leggi di De Morgan per famiglie di insiemi. Insieme delle parti di un insieme. **Relazioni** Prodotto cartesiano. Relazioni insiemistiche. ***a) Funzioni:*** Definizione di funzione; immagine e controimmagine di un elemento. Rappresentazione di una funzione con diagrammi di Venn, come array a due righe, come parole, tramite il modello d'occupazione. Uguaglianza tra funzioni. Composizione di funzioni. Funzione identità. Funzioni invertibili. Funzioni iniettive, suriettive e bigettive. Caratterizzazione delle funzioni invertibili. ***b) Posets:*** relazioni d'ordine parziale. Diagramma di Hasse di un poset. Insiemi totalmente ordinati. Poset duale e principio di dualità. Massimo e minimo di un sottinsieme di un poset. ***c) Relazioni di equivalenza:*** relazione di equivalenza su un insieme. Classi di equivalenza. Insieme quoziente. Partizione di un insieme. Relazione tra partizione di un insieme e relazione di equivalenza su un insieme. Trasversale di una relazione di equivalenza. Proiezione canonica. Relazione di equivalenza indotta da una funzione. **Principio di induzione e ricorsività** Successioni. Sommatorie. Formulazioni del principio di induzione. Procedimento di dimostrazione per induzione. Principio del minimo e

	insiemi ben ordinati. Ogni insieme ben ordinato è totalmente ordinato. Ricorsività e algoritmi ricorsivi. Successioni ricorsive. Ricorrenza lineare, ricorrenza omogenea. Forma chiusa di una successione ricorsiva. Progressioni aritmetiche e geometriche. Problema della Torre di Hanoi. Numeri di Fibonacci. Problema dei dimezzamenti. **(2) Interi** Gli interi come quoziente di **N**x**N**. Richiami sulle operazioni tra interi, loro ordinamento e valore assoluto. Divisibilità tra interi. Algoritmo di divisione euclidea. Massimo comun divisore tra interi. Proprietà elementari del MCD(*a,b*). Teorema di Bezout. Forma di Bezout per l'espressione del MCD(*a,b*). Numeri coprimi. Lemma di Euclide. Algoritmo euclideo per il calcolo del MCD. Minimo comune multiplo tra interi. Espressione del mcm tramite il MCD. Rappresentazione degli interi in un sistema posizionale in base $b>1$. Algoritmo di rappresentazione di un intero in base $b>1$. Numero delle cifre di un dato intero in una base b fissata. Soluzione completa del problema dei dimezzamenti. Equazioni diofantee. 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 di insiemi e confronto di cardinalità. Insiemi finiti e infiniti. I 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. 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 una stessa riga è una potenza di 2. Permutazioni. Fattoriale. 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, semplice e generalizzato. **(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. **(5) Gruppi** Operazioni binarie su un insieme. Definizione di gruppo. Esempi di gruppi. Proprietà elementari di un gruppo: unicità dell'elemento neutro e del simmetrico di un elemento. Multipli e potenze di un elemento di un gruppo e loro proprietà. Ordine di un gruppo. Sottogruppo di un gruppo. In un sottogruppo elemento neutro e inversi si conservano. Lemma di caratterizzazione dei sottogruppi. Sottogruppi di **Z**. Omomorfismi di gruppi. Prime proprietà degli

	omomorfismi. Nucleo e immagine di un omomorfismo. Caratterizzazione dell'iniettività tramite il nucleo. Prodotti diretti di gruppi. Gruppo degli automorfismi di un gruppo. Elementi periodici di un gruppo. Periodo di un elemento periodico. Proprietà del periodo di un elemento periodico. Proprietà di un elemento non periodico. Teorema di Lagrange per i gruppi abeliani finiti. Teorema di Lagrange per i gruppi finiti. Addizione tra classi di congruenza modulo n. Il gruppo $\mathbf{Z}_n$. Epimorfismo canonico. L'unione di sottogruppi non è un sottogruppo. Il prodotto di sottogruppi non è un sottogruppo. L'intersezione di sottogruppi è un sottogruppo. Sottogruppo generato da un sottinsieme di un gruppo. Proprietà rilevanti di <X>. Caratterizzazione di <X> per X finito con elementi che commutano a due a due. Sistema di generatori di un gruppo. Gruppi ciclici. $\|<g>\|=o(g)$. $\mathbf{Z}$ e $\mathbf{Z}_n$ sono ciclici. Caratterizzazione dei generatori ciclici di un gruppo ciclico. Teorema di classificazione dei gruppi ciclici. Sottogruppi di un gruppo ciclico. Reticolo dei sottogruppi di un gruppo ciclico. Numero di generatori di un gruppo ciclico. Funzione φ di Eulero. $n=\sum\varphi(d)$ al variare di d tra i divisori di n. Automorfismi di un gruppo ciclico. Automorfismo $g\rightarrow g^{(-1)}$ di un gruppo abeliano. Coniugio in un gruppo non abeliano. **(6) Gruppi simmetrici** Supporto di una permutazione. Permutazioni a supporto disgiunto commutano. Cicli. Orbita di un elemento sotto una permutazione. Relazione di equivalenza indotta dalle orbite di 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. Alcuni fatti di base sulle permutazioni. Permutazioni coniugate. Ogni permutazione è 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. Gruppo degli elementi invertibili di un anello. Sottoanelli e ideali di un anello. Tipologie di anelli: anelli integri, domini di integrità, corpi, campi. Studio dell'anello $\mathbf{Z}$ e dei suoi ideali.Omomorfismi tra anelli. Nucleo di un omomorfismo. Il nucleo di un omomorfismo è un ideale e ogni ideale è il nucleo di un omomorfismo. Somma diretta di anelli. Divisori di zero in una somma diretta di anelli. Elementi invertibili di una somma diretta di anelli. Anello degli interi $\mathbf{Z}_n$. Elementi invertibili e divisori di zero in $\mathbf{Z}_n$. Epimorfismo canonico da $\mathbf{Z}$ a $\mathbf{Z}_n$. Piccolo Teorema di Fermat. Teorema di Eulero-Fermat. Seconda formulazione del TCR. Moltiplicatività della funzione di Eulero e formula per il calcolo della φ. Criteri di divisibilità. Crittografia ed RSA. Anelli booleani. **(8) Polinomi, funzioni polinomiali e campi finiti** Polinomi a coefficienti in un anello commutativo con unità. Funzione grado e sue proprietà. Polinomi univariati a coefficienti in un campo F. Divisione euclidea in $F[x]$. MCD e mcm tra polinomi e Teorema di Bezout. Polinomi irriducibili e polinomi primi. Equivalenza tra primo e irriducibile in $F[X]$. Teorema di fattorizzazione unica in $F[X]$. Funzioni polinomiali e valutazioni. Radici di un polinomio. Teorema di Ruffini. Principio di identità dei polinomi a coefficienti in un campo infinito. Interpolazione di Lagrange. Ogni funzione da un campo finito in sè è polinomiale. Congruenza modulo un polinomio. Anelli polinomiali.

	Teorema Cinese del Resto per anelli polinomiali. Costruzione di campi finiti. Classificazione dei campi finiti. **(9) Algebre di Boole e reticoli** Circuiti logici e porte logiche. Sistemi funzionalmente completi. Porte logiche NAND e NOR. Assiomi di un'algebra di Boole. Identità principali delle algebre di Boole. Esempi notevoli di algebre di Boole. Algebra delle funzioni booleane di più variabili. Funzioni booleane e circuiti logici. Espressioni booleane. Letterali e congiunzioni fondamentali. Forma normale disgiuntiva. Forme normali minimali e mappe di Karnaugh. Relazione d'ordine indotta in un'algebra di Boole. Elementi minimali, minoranti, estremi inferiori di un sottinsieme di un poset e concetti duali. Reticoli. Reticoli limitati. Reticoli complementati. Reticoli distributivi. Trirettangolo e reticolo pentagonale. Caratterizzazione della distributività tramite le leggi di cancellazione. Reticoli di Boole. Equivalenza logica tra reticoli di Boole, anelli booleani e algebre booleane. Teorema di rappresentazione di Stone per algebre di Boole finite.

Programma	
Testi di riferimento	G.M. Piacentini Cattaneo, "*Matematica Discreta e applicazioni*", Zanichelli Editore (2008). K. H. Rosen, "*Discrete Mathematics and Its Applications*", McGraw–Hill Editore, Settima Edizione (2012) (in Inglese). M. Bianchi, A. Gillio, "*Introduzione alla Matematica Discreta*", McGraw–Hill Editore, Seconda Edizione (2005). C. Delizia, P. Longobardi, M. Maj, C. Nicotera, "*Matematica Discreta*", McGraw–Hill Editore, (2009).
Note ai testi di riferimento	I testi devono esser integrati con gli appunti di lezione e le note e dispense fornite dal docente.
Metodi didattici	Lezioni frontali, esercitazioni in aula. Supporto alla didattica disponibile alla pagina web del docente
Metodi di valutazione (indicare almeno la tipologia scritto, orale, altro)	Prova scritta, prova orale facoltativa (dopo il superamento della prova scritta)
Criteri di valutazione (per ogni risultato di apprendimento atteso su indicato, descrivere cosa ci si aspetta lo studente conosca o sia in grado di fare e a quale livello al fine di dimostrare che un risultato di apprendimento è stato raggiunto e a quale livello)	Lo studente deve risolvere gli esercizi in maniera corretta. I voti (18-30 e lode) dipendono dalla scelta del metodo di risoluzione, dal rigore e dalla chiarezza nell'esposizione.
Altro	