Principali informazioni sull'insegnamento	
Denominazione dell'insegnamento	**Matematica Discreta, Track A--L**
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	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

Docente/i	
Nome e cognome	Vincenzo Carmine Nardozza
Indirizzo mail	Vincenzo.nardozza_AT_uniba.it
Telefono	+39 080 5442692
Sede	Dipartimento di Matematica, Via Orabona 4, 70125, Bari. Stanza n.16, 3° piano.
Sede virtuale	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
Sito web del docente	https://www.dm.uniba.it/it/members/nardozza
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: https://www.dm.uniba.it/it/members/nardozza/ricevimento

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 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. 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 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 φ di Eulero e sue proprietà (moltiplicatività, formula per il calcolo di φ(n), calcolo dell'inverso aritmetico di un intero tramite φ). Teorema di Eulero-Fermat (enunciato). Se un intero a è coprimo con n, allora il minimo esponente k>0 tale che $a^k \equiv 1 \ (mod\ n)$ è un divisore di φ(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. Semigruppi 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 $\mathbf{Z}_n$. 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 integri, domini di integrità, corpi, campi. Esempi di anelli: **Z**, **Q** ed **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 φ di Eulero e formula per il calcolo della φ (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 **C**[x] e di **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 **C** come quoziente di **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 2x2 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.

Testi di riferimento	***Testo adottato per il corso**:* G.M. Piacentini Cattaneo,"*Matematica Discreta e applicazioni*", Zanichelli Editore (2008) ***Altri testi, non obbligatori ma consigliati per consultazione o eventuali approfondimenti personali:*** • C. Delizia, P. Longobardi, M. Maj, C. Nicotera, "*Matematica Discreta*", McGraw–Hill Editore,(2009). • A. Facchini, "*Algebra e Matematica Discreta*", Decibel Zanichelli Editore (2000) • K. H. Rosen, "*Discrete Mathematics and Its Applications*", McGraw--Hill, 7th Edition (2012) *(in Inglese)* • R. Johnsonbaugh, "*Discrete Mathematics*", Pearson Education, 8th Edition (2018) *(in Inglese)* Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php? e contattare la biblioteca per concordare il prestito.
Note ai testi di riferimento	Gli argomenti del programma sono stati sviluppati secondo l'esposizione e la notazione presenti sul testo ufficiale adottato, **che pertanto è un riferimento essenziale** 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). Inoltre, a integrazione dei contenuti di base (punto 1 del programma) è disponibile anche una raccolta di esercizi su logica, insiemistica e induzione. Tutto tale materiale didattico è disponibile all'indirizzo: https://www.dm.uniba.it/it/members/nardozza/homepage/aa-2023-24/md-2023-24/md-2023-24-itps-track-a-l Si consiglia vivamente di studiare attenendosi al materiale **ufficiale** 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.

Organizzazione della didattica

Ore

Totali	Didattica frontale	Pratica (esercitazione)	Studio individuale
225 ore	56 ore	30 ore	139 ore

CFU/ETCS

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.
Competenze trasversali	**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. Tali abilità sono sviluppate tramite esercizi e quesiti proposti periodicamente durante il corso. **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 in maniera chiara e rigorosa. Tali abilità sono sviluppate tramite esercizi e quesiti proposti periodicamente durante il corso. **Capacità di apprendere in modo autonomo** Acquisizione di un metodo di studio adeguato, supportato della consultazione dei testi e dalla risoluzione di esercizi e quesiti proposti periodicamente durante il corso.

Valutazione	
Modalità di verifica dell'apprendimento	Prova scritta della durata di circa 2 ore contente esercizi a carattere algoritmico/computazionale e quesiti a carattere teorico. La votazione utilizzata è il voto in trentesimi. La prova scritta si ritiene superata se si raggiunge la valutazione di 18. Correzione da parte del docente e incontro per la visualizzazione dell'elaborato, prima della verbalizzazione. Prova orale facoltativa nello stesso appello, dopo il superamento della prova scritta. (Quindi almeno 18 alla prova scritta). Informazioni dettagliate, tracce passate, esercizi svolti e comunicazioni sono disponibili nella pagina ufficiale del docente: https://www.dm.uniba.it/it/members/nardozza/homepage
Criteri di valutazione	● **Conoscenza e capacità di comprensione:** Qualità e correttezza delle tecniche dimostrative, procedimenti formali e del ragionamento astratto. ● **Conoscenza e capacità di comprensione applicate:** Qualità e correttezza delle capacità logiche. ● **Autonomia di giudizio:** Correttezza delle tecniche dimostrative e del metodo risolutivo. ● **Abilità comunicative:** Qualità, chiarezza e correttezza dell'esposizione delle conoscenze acquisite. ● **Capacità di apprendere:** Correttezza degli svolgimenti e dei risultati elaborati.
Criteri di misurazione dell'apprendimento e di attribuzione del voto finale	Il voto finale è a attribuito in trentesimi. L'esame è superato quando il voto è superiore o uguale a 18. Il voto finale (18-30 e lode) dipende dalla conoscenza, dal rigore e dalla correttezza dello svolgimento degli esercizi nella prova scritta.

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

Main information on the course		
Course name	**Discrete Mathematics, Track A--L**	
Degree	Computer Science and Software Production Technologies	
Academic Year	2023/24	
European Credit Transfer and Accumulation System (ECTS) / Italian Crediti formativi universitari (CFU)		9 CFU (each CFU corresponds to 25 hours (h) of student's time); CFU types: T1, T2 or T3 T1 = 8 h lecture + 17 h individual study T2 = 15 h practice + 10 h individual study T3 = 25 h individual study
Settore Scientifico Disciplinare	Mat/03-Geometria	
Course language	Italian	
Anno di corso	First year	
Periodo di erogazione	First semester	
Obbligo di frequenza	It is highly recommended to attend classes	
Course web site	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	

Docente/i	
Name and Surname	Vincenzo Carmine Nardozza
Mail address	Vincenzo.nardozza_AT_uniba.it
Phone (office)	+39 080 5442692
Office	Dipartimento di Matematica, Via Orabona 4, 70125, Bari. Room n.16, 3rd Floor.
E-learning platform	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
Teacher's institutional website	https://www.dm.uniba.it/it/members/nardozza
Office hours	Friday, 10.00-12.00, on appointment. To agree on a different date/time, please visit: https://www.dm.uniba.it/it/members/nardozza/ricevimento

Syllabus	
Course aims and goals	The course deals with several basic Discrete Mathematics topics. It aims to provide mathematical tools pertaining Logic, Set Theory, Functions, Combinatorics, Integer numbers and Modular Arithmetic, Abstract Algebraic Structures.
Previous knowledge	Elementary algebraic manipulations and computations; elementary techniques for solving simple algebraic equations and inequalities.

Course topics	***1. Basics***. a) **Logic:** Statements. Fundamental logic operators and truth tables. Equivalent statements. Contradictions and tautologies. Logical implication. Equivalent formulations of logical implication. Biconditional operator. Priority order among logical operators. Negation rules (De Morgan formulae). Negation of logical implication and of the biconditional operator. Predicates and quantifiers. Rules for negating a predicative statement. Statements depending on several logical variables. b) **Set Theory:** Sets and objects. Membership between an object and a set. Universe set. Inclusion and set equality. Representation of a set, logical and functional builders. Void set; the void set is a subset of any set; a set does not change when permuting its objects or when writing several times the same object. Union, intersection and complement of a set. Basic properties of set operations. Family of sets. De Morgan laws. Power set of a set. c) **Relations:** Cartesian product. Relations. **Functions:** Definition of a function; image and preimage of an elemento. Representation of a function by Venn diagrams, as a two-rows array, as a word, through occupation model. Functions equality. Function composition. Identity function. Invertible functions. Injective, surjective, bijective functions. Characterization of invertible functions. **Posets:** partial order relations. Totally ordered sets. Maximum and minimum of a subset in a poset. Well ordered sets. Any well ordered set is totally ordered. Hasse diagrams of a poset. **Equivalence relations:** equivalence relation on a set. Equivalence classes. Factor set. Set partition. Logical equivalence between set partitions and equivalence relations on a fixed set. d) **Induction and recursivity:** Sequences. Summations. Mathematical induction in its different forms: simple induction, complete induction, minimum principle. Proofs by induction. **Recursivity**: recursive algorithms. Recursive sequences. Closed form of a recursive sequence. Arithmetic and geometric sequences. Fibonacci numbers. ***2. Integers.*** Integer divisibility. Euclidean division algorithm. Integer representarions in positional systems in basis b>1. Greatest common divisor (gcd) between integers. Basic properties of gcd(a,b). Bezout's Theorems. Bezout's expression for gcd(a,b). Euclid's Lemma. Euclidean algorithm for computing gcd(a,b). Computing Bezout's coefficients. Least common multiple (lcm) between integers. Expressing lcm(a,b) through gcd(a,b). Linear Diophantine equations. Solving linear Diophantine equations. Prime and irreducible numbers. Fundamental Theorem of Arithmetic. There exist infinite prime numbers. Existence of irrational numbers. Eratosthenes sieve. **3.** ***Combinatorics*** Cardinalities and their comparison. Finite and infinite sets. The natural numbers form an infinite set. Comparing cardinalities of number sets. Cardinality of a finite set and the meaning of "*counting*". Addition principle. Multiplication principle. Cardinality of the power set of a finite set. Number of divisors of an integer number. Dispositions with repetitions. Number of dispositions with repetitions of class k on n objects. Simple dispositions. Number of simple dispositions of class k on n objects. Permutations. Factorial. Simple combinations. Binomial coefficients. Basic properties of coefficient binomials. Tartaglia (Pascal) triangle. Expansion of a binomial power (Newton or binomial expansion Theorem). The sum of the Tartaglia n-th row-coefficients is 2^n. Closed form of a binomial coefficient. Combinations with repetitions of class k on n objects. Number of combinations with repetitions of class k on n objects. Multisets. Inclusion-Exclusion principle. Pigeonhole principle.

4. *Modular Arithmetic*

Congruence modulo *n*. Congruence modulo *n* is an equivalence relations. Alternative definition of congruence modulo *n*. Description of congruence classes. Cardinality of the factor set. Integer operations compatibility. Arithmetic inverses modulo n and their computation. Linear congruences. Solvability of a lineare congruence. Solutions of a solvable linear congruence. Partitioning the solutions of a solvable linear congruence into congruence classes. Linear congruences systems. Normalization of a linear congruences system. Chinese Remainder Theorem (First formulation). Euler φ totient function and its properties (multiplicativity, semi-closed formula for φ(n), computing an arithmetic inverse of an integer through φ). Euler-Fermat Theorem (statement). If an integer a is relatively prime with n, then the minimal exponent $k > 0$ such that $a^k \equiv 1(mod n)$ divides $\varphi(n)$. Applications: divisibility by numbers <17, RSA.

5. *Groups*

Binary operations on a set. Distinctive features of binary operations: associativity, commutativity, neutral element existence, existence of the symmetric of a chosen element. Multiplication table of a binary operation. Semigroups and Monoids. Free monoid generated by a set X. Definition of a group. Examples of groups. Additive and multiplicative notation. Cancellation lemma in a group. Order of a group. Addition of congruence classes modulo n. The group $\mathbf{Z}_n$. Properties of a multiplicative table of a group. Basic properties of a group: the neutral elementi s unique, the any element admits a unique symmetric element. Powers (or multiples) of an element of a group and their properties. Periodic and aperiodic elements of a group. Period of a periodic element. All elements of a finite group are periodic, and any period divides the group order. Properties of aperiodic elements. Properties of the period of a periodic element. Subgroups. Neutral element and inverses are preserved in any subgroup. Subgroups characterization Lemma. Subgroup generated by a subset. Cyclic subgroups of a group and cyclic groups. Relation between the period of an element and the order of the generated cyclic group. Lagrange Theorem for finite groups. Number of (cyclic) generators of a cyclic group. Classification of cyclic groups. Distinguished properties of cyclic groups. Direct products of groups and the Fundamental Theorem on finite abelian groups.

6. *Symmetric groups*

Inverse of a composition between permutations. Support of a permutation. Disjoint permutations. Disjoint permutations commute. Cycles. Orbit of an element under a permutation. Equivalence relation induced by a fixed permutation. Associated cycle of an orbit. Disjoint cycle decomposition of a permutation. Cyclic structure of a permutation. Period of a permutation. Any permutation is a product of transpositions. Parity and sign of a permutation. Sign function. Alternating group.

7. *Rings*

Definition of a ring. Commutative and unital rings. Properties of the zero element of a ring. Zero divisors. Invertible elements in a ring. Zero divisors and invertible elements form disjoint subsets of a ring. The invertible elements in a ring form a group: the unit group of the ring. Terminology: integral rings, integral domains, skew fields, fields. Examples: **Z**, **Q** and **R**. The ring $\mathbf{Z}_n$. Zero divisors and invertible elements of $\mathbf{Z}_n$. The ring $\mathbf{Z}_n$ is a field if and only if n is a prime. Direct sums of rings. Unit group of a direct sum of rings. Ring homomorphisms and their properties. Kernel of a ring homomorphism and a characterization of injectivity of a homomorphism through its kernel. Eulero—Fermat Theorem and Fermat's (Little)

Theorem (proofs). Chinese Remainder Theorem (Second formulation and proof). Multiplicativity of Euler totient φ function and semi-closed formula of φ (proofs).

8. *Polynomials and finite fields*

Ring of univariate polynomials with coefficients in a field. Euclidedan division algorithm. Greatest common divisor (GDC) between polynomials and Bezout Theorem. Prime and irreducible polynomials, and the logic equivalence between these two notions. Polynomial functions and roots of a polynomial. Ruffini's Theorem. A characterization Lemma for irreducible polynomials of degree two or three through their roots. Characterization of irreducible polynomials in **C**[x] and **R**[x]. Congruence modulo a polynomial and factor polynomial rings. Zero divisors and invertible elements in a factor polynomial ring through the GCD. Theorem: F[x]/(f) is a field if and only if f is an irreducible polynomial. Theorem: if f has degree n then F[x]/(f) has $|F|^n$ elements. Finite fields. The cardinality of any finite field is a prime power. The complex field **C** is a factor ring of **R**[x], and precisely **C** is isomorphic to **R**[x]/(x^2+1). Chinese Remainder Theorem for polynomial factor rings.

9. *Matrix rings*

Matrices with entries in a field. Matrix sum and product. Ring of square matrices. General Linear Group $GL_n(F)$. Determinant of a matrix. Characterization of invertible matrices and zero divisors through the determinant. Binet's Theorem. Explicit computation of the determinant for matrices of special shapes. Inverse matrix of an invertible 2x2-matrix through the determinant. Elementary row transformations $R_{ij}(a)$, $\mu_i(\alpha)$ and T_{ij}. Invertibility and explicit computation of the inverse of an invertible matrix through elementary row tranformations. Computation of the determinant of a matrix through elementary row transformations.

10. *Applications of Matrix Calculus: Linear systems*

Coefficient and extended coefficient matrix of a linear system. Row-echelon form of a matrix and reduction process. Matrix rank. Gauss-Jordan algorithm for solving a linear system. Characterization of a solvable linear system through row-echelon form. Rouché-Capelli Theorem. Number of solutions of a solvable linear system over a finite field.

Textbooks	***Adopted textbook**:* G.M. Piacentini Cattaneo,"*Matematica Discreta e applicazioni*", Zanichelli Editore (2008) ***Other textbooks, not mandatory but useful for consulting or personal studies:*** • C. Delizia, P. Longobardi, M. Maj, C. Nicotera, "*Matematica Discreta*", McGraw–Hill Editore,(2009). • A. Facchini, "*Algebra e Matematica Discreta*", Decibel Zanichelli Editore (2000) • K. H. Rosen, "*Discrete Mathematics and Its Applications*", McGraw--Hill, 7th Edition (2012) *(in Inglese)* • R. Johnsonbaugh, "*Discrete Mathematics*", Pearson Education, 8th Edition (2018) *(in Inglese)*
Further remarks	The course followed the exposition and the notation of the adopted textbook, which is therefore an essential reference in exam preparation. Program points 7, 9 and 10 are an exception, having been dealt with according to the teacher's lecture notes available at: https://www.dm.uniba.it/it/members/nardozza/homepage/aa-2023-24/md-2023-24/md-2023-24-itps-track-a-l

Educational activities organization

Hours

Total amount	Lectures	Practice sessions	Personal study
225 hours	56 hours	30 hours	139 hours

CFU/ETCS

9 CFU	7 CFU	2 CFU	

Teaching methods

	Lectures and class exercises

Risultati di apprendimento previsti	
Knowledge and understanding	Acquisition of logical competence and knowledge of abstract mathematical notions. Acquisition of basic proof techniques and formal procedures, abstract principles and formal calculus.
Applied knowledge and understanding	The acquired knowledge find application in the resolution of the exercises. The students will be able to solve problems, algorithms and matrix computations.
Other skills	**Making informed judgments and choices** Ability to choose a resolution procedure. Ability to decide the correctness and precision of a resolution procedure and of a logical proof. **Communicating knowledge and understanding** Ability to use formal mathematical language, that is fundamental for future studies. Talent to disseminate the acquired knowledge. Ability to explain the learnt knowledge. **Self-study abilities** Acquisition of a a suitable learning method, based on texts consulting and exercises.

Assessment	

Assesment methods	Written exam, with exercises and questions about lectures. Oral exam available upon request, only after the fulfilment of the written exam. More details available at: https://www.dm.uniba.it/it/members/nardozza/homepage
Evaluation criteria	● **Knowledge and understanding:** Quality and accuracy of the techniques and proofs used and abstract reasoning. ● **Applying knowledge and understanding:** Accuracy and precision of reasoning ● **Autonomy of judgment:** Quality and precision of the proofs and techniques used ● **Communicating knowledge and understanding:** Quality and accuracy of the acquired knowledge ● **Communication skills:** Property and accuracy of the exposition
Measurements and final grade	The student has to be able to solve the exercises in a correct way. The marks (18-30 e lode) depends on how the described solutions are strict, logical and correct. The exam is passed if the assessments is greater or equal to 18.

Further information	More information are available at: https://www.dm.uniba.it/it/members/nardozza **It is strongly advised to partecipate at the lecture and exercise classes.** **It is strongly advised to study each day.** **It is strongly advised to try to solve the proposed exercises day by day.**