Cenni di calcolo proposizionale. Enunciati, predicati, quantificatori, connettivi, tavole della verità.

Teoria degli insiemi. Il concetto di verità in matematica. Teoria degli insiemi: il sistema assiomatico di Zermelo Fraenkel (ZF): Gli assiomi ZF1, ZF2, ZF3, ZF4, ZF5, ZF6, ZF7. Proprietà dell'unione e dell'intersezione. Famiglie di insiemi. Unione e intersezione di famiglie di insiemi. Differenza tra insiemi. Le leggi di de Morgan. Coppie ordinate. Prodotto cartesiano. ZF8, ZF9.

Funzioni tra insiemi. Relazioni binarie di X in Y. Definizione intuitiva di funzione tra insiemi. Grafico di una funzione. Definizione rigorosa di funzione come relazione binaria. Dominio e codominio di una funzione. Immagine di un elemento. Immagine di un insieme. Immagine inversa o controimmagine. Esempi notevoli di funzione: identità, immersione, restrizione. L'insieme delle funzioni tra due insiemi. Funzioni iniettive, suriettive e biettive. Criteri per determinare se una funzione è iniettiva e/o suriettiva: (i) $f : X \to Y$ è iniettiva se e solo se $\forall T \subseteq X$ si ha $F(X \setminus T) \subseteq Y \setminus f(T)$; (ii) $f : X \to Y$ è isuriettiva se e solo se $\forall T \subseteq X$ si ha $F(X \setminus T) \supseteq Y \setminus f(T)$. Il teorema di Cantor. Lo spazio 2^X delle funzioni da X in $\{0, 1\}$. Funzione caratteristica. Costruzione di una biettività tra $P(X)$ e 2^X. Composizioni di applicazioni: definizione e primi esempi. Legami tra l'iniettività e la suriettività della funzione composta e delle funzioni che la compongono: f, g iniettive (suriettive) $\Rightarrow f \circ g$ e $g \circ f$ iniettive (suriettive); $g \circ f$ iniettiva (suriettiva) $\Rightarrow f$ iniettiva (g suriettiva). Funzioni iniettive ed inverse a sinistra: data $f : X \to Y$ iniettiva $\exists\ g : Y \to X$ suriettiva con $g \circ f = Id_X$. L'assioma della scelta. Funzioni suriettive ed inverse a destra: data $f : X \to Y$ suriettiva $\exists\ g : Y \to X$ iniettiva con $f \circ g = Id_Y$. Funzioni cancellabili. Proprietà della legge di cancellazione: f è cancellabile a destra $\Leftrightarrow f$ è suriettiva; f è cancellabile a sinistra $\Leftrightarrow f$ è iniettiva. Funzioni invertibili. Caratterizzazione delle funzioni invertibili come quelle biettive. Determinazione della funzione inversa.

I numeri naturali. Sistemi di Peano. Esistenza di un sistema di Peano. Isomorfismi di sistemi di Peano. Equivalenza tra sistemi di Peano (senza dimostrazione). Il principio di induzione debole. Definizioni per induzione. Definizione di potenza di una funzione. Definizione di somma di numeri naturali. Proprietà della somma di numeri naturali: associativa, commutativa, legge di cancellazione. Definizione di sommatoria. Definizione di prodotto di numeri naturali. Proprietà del prodotto di numeri naturali: legge di annullamento del prodotto, distributiva, commutativa, associativa, legge di cancellazione. Definizione di $\leq$ tra numeri naturali. Proprietà del $\leq$ (riflessiva, antisimmetrica, transitiva, dicotomia). Comportamento del $\leq$ rispetto alle operazioni di somma e prodotto di numeri naturali. Definizione di potenza di un numero naturale. Proprietà della potenza: $k^n\, k^m = k^{m+n}$, $m^k\, n^k = (m\, n)^k$. Definizione di numero pari e di numero dispari.

Insiemi finiti. Il principio di Dirichlet. Definizione di insieme finito. Proprietà degli insiemi finiti: Se X è finito allora $Y \subseteq X$ è finito; X finito e $f : X \to Z$ suriettiva allora Z è finito. Calcolo della cardinalità dell'intersezione, dell'unione, del prodotto cartesiano e dell'insieme delle parti. Insiemi finiti e equivalenza tra iniettività e suriettività di $f : X \to X$.

Insiemi infiniti. Definizione di insieme infinito come non-finito. Dimostrazione che $\mathbb{N}$ è infinito. Insiemi infiniti nel senso di Dedekind. Insiemi infiniti nel senso di Cantor.

Equivalenza tra l'esistenza di un insieme infinito nel senso di Cantor e un sistema di Peano. Equivalenza tra le tre definizioni di insieme infinito.

Relazioni di equivalenza. Definizione relazione di equivalenza. Corrispondenza tra relazioni di equivalenza e partizioni di un insieme. Definizione di insieme quoziente. Proiezione canonica sull'insieme quoziente. Funzioni tra insiemi e relazioni di equivalenza. Teorema fondamentale del passaggio al quoziente per le funzioni. Funzioni definite su uno spazio quoziente.

I numeri interi. Definizione di numeri interi come spazio quoziente. Definizione di somma e prodotto dei numeri interi. Proprietà dei numeri interi. Definizione di gruppo e di anello. Dimostrazione che $\mathbb{Z}$ è un anello. Definizione di relazione d'ordine negli interi. Proprietà della relazione d'ordine. Proprietà archimedea.

I numeri razionali. Definizione dei numeri razionali. Definizione di somma e prodotto di numeri razionali. Proprietà della somma e del prodotto. Proprietà dei numeri razionali. Definizione di campo. Dimostrazione che $\mathbb{Q}$ è un campo. Relazione d'ordine sui razionali.

Calcolo combinatorio. Definizione del fattoriale di un numero naturale. Il coefficiente binomiale. Proprietà del coefficiente binomiale. Formula del coefficiente binomiale. La formula del Binomio di Newton. Il triangolo di Tartaglia-Pascal. Conseguenze della formula del Binomio di Newton. Cardinalità dell'insieme delle funzioni tra due insiemi finiti. Cardinalità dell'insieme delle funzioni iniettive tra due insiemi finiti. Numero delle funzioni biettive (permutazioni) da un insieme finito in se stesso. Legame tra il numero delle partizioni di un insieme X con n elementi in m parti e il numero di funzioni suriettive da X in un insieme Y con m elementi. Cardinalità dell'insieme delle funzioni suriettive tra due insiemi finiti. Cardinalità delle partizioni di un insieme finito in m parti (numero di Sterling). Numero di tutte le partizioni di un insieme finito (numero di Bell).

Relazioni d'ordine. Relazioni d'ordine e di preordine. Definizione di insieme parzialmente ordinato e totalmente ordinato. Definizione di minimo, massimo, minimale, massimale, minorante e maggiorante. Definizione di estremo superiore e estremo inferiore. Definizione di ordinamento completo e ordinamento denso. Catene. Reticoli. Definizione di buon ordinamento. Esempio di insieme parzialmente ordinato non completo. Dimostrazione del principio di buon ordinamento dei numeri naturali. Il principio di induzione forte. Equivalenza tra il principio di induzione, il principio del buon ordinamento e il principio di induzione forte. Il lemma di Zorn (senza dimostrazione).

Cardinalità di insiemi infiniti. Confronto della cardinalità tra insiemi. ll teorema di Cantor-Bernstein (solo la dimostrazione del caso generale dando per buona la dimostrazione del caso particolare). Il teorema di Hartogs. Relazione d'ordine tra le cardinalità di insiemi. Definizione di insieme numerabile. Numerabilità di alcuni insiemi: $\mathbb{N}\times\mathbb{N}$; unione numerabile di insiemi numerabili. Numerabilità degli interi. Numerabilità dei razionali. Non numerabilità di $P(\mathbb{N})$. Cardinalità dell'unione, del prodotto e della differenza (senza dimostrazione).

I numeri reali. Densità dei razionali e dimostrazione che i razionali non sono completi. Sezioni di Dedekind. Definizione dell'insieme dei numeri reali. Definizione di ordine sui reali. Dimostrazione che l'ordine è totale e completo. Definizione di somma, zero ed opposto. Proprietà della somma (senza dimostrazione). Valore assoluto di un numero reale. Prodotto di numeri reali. Proprietà del prodotto (senza dimostrazione). I reali come campo ordinato. Proprietà archimede dei numeri reali. Densità di $\mathbb{Q}$ in $\mathbb{R}$. Radice di due come numero reale. Densità degli irrazionali in $\mathbb{Q}$. Cardinalità di $\mathbb{R}$ (senza dimostrazione).

I numeri complessi. Definizione. Operazioni nei numeri complessi. Rappresentazione dei numeri complessi nel piano di Gauss. Forma esponenziale dei numeri complessi. La formula di Eulero e la formula di De Moivre. Radici n-esime di un numero complesso e loro rappresentazione geometrica. Trasformazioni geometriche e numeri complessi.

Aritmetica in $\mathbb{Z}$. Divisione in un anello e divisione in $\mathbb{Z}$. Numeri irriducibili. Il Massimo Comune Divisore. Il Teorema della Divisione Euclidea. Il teorema di Bezout. L'algoritmo euclideo per il calcolo del MCD. Numeri primi di un dominio di integrità. Legami tra numeri irriducibili e numeri primi. Il minimo comune multiplo e legame con il MCD. Il teorema fondamentale dell'aritmetica. Il teorema di Euclide sull'esistenza di infiniti numeri primi. Il setaccio di Eratostene. Congruenze. Classi di resto modulo m. Addizione e moltiplicazione di due classi di resto. L'anello Z_m. Il campo Z_p con p primo. Rappresentazione b-adica dei numeri. Alcuni criteri di divisibilità. Il piccolo teorema di Fermat. Equazioni congruenziali. Sistemi di congruenze. Il Teorema cinese del resto. Equazioni Diofantee di primo grado. La funzione di Eulero. Il Teorema di Eulero sulle congruenze.

Algebra dei polinomi. Fatorizzazione in un dominio. Polinomi in una variabile. Polinomi in una variabile in un campo. Polinomi in più variabili. Polinomi omogenei.