I Settimana (25-27 settembre 2012)

Introduzione al corso. Nozione intuitiva di insieme. Operazioni tra insiemi (unione, intersezione, differenza, complementare) e loro proprietà. Insieme delle parti di un insieme. Esempi. Coppie ordinate. Prodotto cartesiano di due insiemi.
Proposizioni. Principali simboli logici: $\wedge$, $\vee$, $\neg$, $\Rightarrow$, $\Leftrightarrow$, simbolo di Sheffer. Tabelle di verità. Equivalenze logiche. Tautologie. Negazione di proposizioni del tipo $P \wedge Q$ e $P \vee Q$; negazione di proposizioni contenenti i simboli quantificatore esistenziale $\exists$ e quantificatore universale $\forall$. Dimostrazione per assurdo.

II Settimana (2-4 ottobre 2012)

Corrispondenza tra un insieme X ed un insieme Y. Esempi. Corrispondenza composta. Esempi. Corrispondenza inversa. Applicazioni o funzioni. Esempi. Corrispondenza inversa di una applicazione. Applicazione identica ed applicazioni costanti. Esempi. Prodotto operatorio di applicazioni e sue prime proprietà. La composizione di applicazioni iniettive è un'applicazione iniettiva. Una applicazione è iniettiva se e solo se ha una inversa a sinistra. Una applicazione è iniettiva se e solo è cancellabile a sinistra. Famiglia di elementi di un insieme X; famiglia di sottoinsiemi di un insieme X.

III Settimana (9-11 ottobre 2012)

La composizione di applicazioni suriettive è un'applicazione suriettiva. Una applicazione è suriettiva se e solo se è cancellabile a destra. Assioma della scelta. Una applicazione è suriettiva se e solo se ha una inversa a destra. Applicazioni biiettive. Teorema di Cantor: non esiste alcuna applicazione suriettiva da un insieme non vuoto sull'insieme delle sue parti. $f^{-1}\big(f(A)\big)$ e $f\big(f^{-1}(B)\big)$.
Relazioni (binarie) in un insieme X. Esempi. Relazioni d'equivalenza. Classi d'equivalenza. Insieme quoziente. Esempi. Ricoprimenti e partizioni di un insieme X. Relazioni di equivalenza e partizioni.

IV Settimana (16-18 ottobre 2012)

Relazione d'equivalenza ("nucleo") associata ad una applicazione. Teorema fondamentale di decomposizione di una applicazione. Esempi.
Divisione con il resto. Definizione di MCD. Esistenza del MCD. Identità di Bézout. Algoritmo Euclideo delle divisioni successive per la determinazione del MCD.

V Settimana (23-25 ottobre 2012)

Lemma di Euclide. Definizione di mcm; relazione tra MCD e mcm. Equazioni diofantee del tipo $aX + bY = c$: criterio di risolubilità e descrizione delle sue radici. Numeri primi. Teorema fondamentale dell'aritmetica. Determinazione del MCD e del mcm attraverso la fattorizzazione. Teorema sulla infinità dei

numeri primi. Crivello di Eratostene. Congruenze mod n. Insieme quoziente $\mathbb{Z}/\equiv_m$

VI Settimana (6-8 novembre 2012)

Inverso aritmetico modulo n. Sistemi completi di residui modulo n. Sistemi ridotti di residui modulo n. Esempi. Indicatore di Eulero.
Addizione e moltiplicazione nell'insieme quoziente $\mathbb{Z}/\equiv_m$ delle classi resto modulo un intero $m > 1$. Principali proprietà algebriche di $(\mathbb{Z}/\equiv_m, +, \cdot)$. Elementi invertibili e "divisori dello zero" in $\mathbb{Z}/\equiv_m$.
Congruenze del tipo $aX \equiv b \pmod{m}$: criterio di risolubilità, numero di soluzioni e ricerca di soluzioni. Esempi.

VII Settimana (13 - 15 novembre 2012)

Il Teorema cinese dei resti. Esempi. Risoluzione di sistemi di congruenze lineari.
Il piccolo Teorema di Fermat.
Teorema di Wilson. Caratterizzazione dei numeri primi tramite il Teorema di Wilson.

VIII Settimana (20 - 22 novembre 2012)

Teorema di Eulero-Fermat. Moltiplicatività dell'indicatore di Eulero (due dimostrazioni).
Operazione binaria in un insieme. Semigruppi e monoidi. Esempi. Gruppi. Esempi. Notazione moltiplicativa e additiva. Gruppi abeliani. Esempi. Prime proprietà. Tabelle. Potenze e multipli. Esempi.

IX Settimana (27 - 29 novembre 2012)

Il gruppo delle permutazioni su un insieme X: definizione, prime proprieta' ed esempi. S_n. Scrittura matriciale di una permutazione $f \in S_n$. Permutazione ciclica o ciclo di lunghezza l in S_n. Supporto di una permutazione. Permutazioni disgiunte. Definizione di orbita di un elemento sotto l'azione di una permutazione $f \in S_n$. Partizione del supporto di f attraverso le orbite degli elementi di X. Ogni permutazione in S_n si scrive in modo unico (a meno dell'ordine) come composizione dei suoi cicli.
Scrittura di permutazioni come prodotto di trasposizioni. Parita' di una permutazione. L'ordine di un l-ciclo e' l. L'ordine di una permutazione in S_n e' il m.c.m. delle lunghezze dei suoi cicli. Omomorfismi tra gruppi. Il segno di una permutazione induce un omomorfismo da S_n nel gruppo $\{1, -1\}$. Definizione di A_n. Definizione di sottogruppo di un gruppo. A_n è un sottogruppo di S_n.

X Settimana (4 - 6 - 7 dicembre 2012)

Anelli. Esempi. Anelli di applicazioni. Anelli di endomorfismi di gruppi abeliani. Prime proprietà. Anelli commutativi ed unitari. Esempi. Elementi invertibili e zero-divisori. Domini d'integrità. Corpi. Campi. Esempi.

Caratteristica di un anello commutativo unitario. Esempi. Sottoanelli. Omomorfismi di anelli.
Polinomi in una indeterminata a coefficienti in un anello commutativo unitario: somma e prodotto (di convoluzione). Grado: prime proprieà.
Polinomi a coefficienti in un dominio d'integrità D: formula del grado e $U(D[X]) = U(D)$. Elementi associati in un dominio d'integrità. Algoritmo di divisione tra polinomi a coefficienti in un dominio d'integrità. Esempi.
Costruzione di $\mathbb{Q}$ a partire da $\mathbb{Z}$.

XI Settimana (11 - 13 dicembre 2012)

Il campo dei quozienti di un dominio d'integrità. Cenni sulla proprietà di universalità del campo dei quozienti. Campo dei quozienti di un anello di polinomi a coefficienti in un campo ed in un dominio d'integrità.
Elementi primi ed irriducibili in un dominio.
Polinomi irriducibili.
Radici di un polinomio. Teorema del resto. Esistenza di radici e riducibilità. Polinomio derivato. Radici multiple.

XII Settimana (18 dicembre 2012)

Teorema di fattorizzazione unica in $K[X]$ con K campo. Polinomi a coefficienti numerici. Teorema Fondamentale dell'Algebra (solo enunciato). Polinomi irriducibili di $\mathbb{C}[X]$. Radici reali e complesse di polinomi a coefficienti reali. Polinomi irriducibili di $\mathbb{R}[X]$.