I Settimana (21-22-24 settembre 2009)

Introduzione al corso. Nozione intuitiva di insieme. Operazioni tra insiemi (unione, intersezione, differenza, complementare) e loro proprietà. Insieme delle parti di un insieme. Esempi. Famiglie di insiemi: definizione, unione e intersezione.
Coppie ordinate. Prodotto cartesiano di due insiemi. Relazioni binarie. Applicazioni o funzioni. Esempi. Relazione inversa di una applicazione. Applicazione identica ed applicazioni costanti. Esempi. Prodotto operatorio di applicazioni e sue prime proprietà. Applicazioni suriettive, iniettive e biiettive: definizioni e proprietà. Applicazione inversa di una biiezione.

II Settimana (29 settembre - 1 ottobre 2009)

Non esiste alcuna applicazione suriettiva da un insieme X sull'insieme delle sue parti. Funzione caratteristica di un sottoinsieme. Esistenza di una biiezione da $\mathcal{P}(\mathcal{X})$ a $\{0,1\}^X$. Principio di Dirichlet. Insiemi finiti.
Ricoprimenti e partizioni di un insieme X. Esempi. Assioma della scelta. Una applicazione suriettiva ha una inversa destra. Un sottoinsieme di un insieme finito è finito. Intersezione e unione di un numero finito di insiemi finiti.

III Settimana (6 - 8 ottobre 2009)

Numero degli elementi del prodotto cartesiano di due insiemi finiti. Numero delle applicazioni da un insieme finito in un insieme finito. Numero delle applicazioni iniettive da un insieme finito in un insieme finito. Una applicazione da un insieme finito in se stesso è iniettiva se e solo se è suriettiva se e solo se è biiettiva.
Relazioni d'equivalenza. Classi d'equivalenza. Insieme quoziente. Esempi. Relazioni di equivalenza e partizioni. Insieme quoziente. Relazione d'equivalenza ("nucleo") associata ad una applicazione. Teorema fondamentale di decomposizione di una applicazione. Esempi.

IV Settimana (13 - 15 ottobre 2009)

Costruzione di $\mathbb{Z}$ (numeri interi relativi) a partire da $\mathbb{N}$. Introduzione delle operazioni di somma e prodotto e della relazione d'ordine in $\mathbb{Z}$. Prime Proprietà. Divisione con il resto. Definizione di MCD. Esistenza del MCD. Identità di Bézout. Lemma di Euclide. Algoritmo di Euclide per la determinazione del MCD.

V Settimana (20 - 24 ottobre 2009)

Determinazione di una identità di Bézout. Esempi. Definizione ed esistenza del mcm. Numeri primi. Teorema fondamentale dell'aritmetica. Teorema sulla infinità dei numeri primi. Crivello di Eratostene. Congruenze. Addizione e moltiplicazione nell'insieme quoziente $\mathbb{Z}/\equiv_m$ delle classi resto modulo un intero $m > 1$. Principali proprietà algebriche di $(\mathbb{Z}/\equiv_m, +, \cdot)$.

VI Settimana (27 ottobre 2009)

Elementi invertibili e "divisori dello zero" in $\mathbb{Z}/\equiv_m$. Calcolo di un inverso aritmetico modulo m. Indicatore di Eulero. Sistemi completi di residui modulo m. Sistemi ridotti di residui modulo m. Esempi.

VII Settimana (9 - 10 - 12 novembre 2009)

Equazioni diofantee lineari del tipo $aX + cY = b$: criterio di risolubilità e soluzioni. Congruenze del tipo $aX \equiv b \pmod{m}$: criterio di risolubilità, numero di soluzioni e ricerca di soluzioni. Esempi. Il Teorema cinese dei resti. Esempi. Risoluzione di sistemi di congruenze lineari. Il piccolo Teorema di Fermat. Teorema di Eulero-Fermat.

VIII Settimana (17 - 12 novembre 2009)

Teorema di Wilson. Caratterizzazione dei numeri primi tramite il Teorema di Wilson. Se p è un numero primo dispari, la congruenza $X^2 \equiv -1 \pmod{p}$ è risolubile se e solo se $p \equiv 1 \pmod{4}$. Esercizi.
Operazione binaria in un insieme. Semigruppi e monoidi. Gruppi. Notazione moltiplicativa e additiva. Gruppi abeliani. Esempi. Prime proprietà. Leggi di cancellazione. Tabelle. Potenze e multipli. Esempi. Ordine di un elemento di un gruppo. Esempi.

IX Settimana (24 - 26 novembre 2009)

Proprietà dell'ordine di un elemento di un gruppo. Sottogruppi. Esempi. Sottogruppo generato da un sottoinsieme di un gruppo. Sottogruppo generato da un elemento di un gruppo. Esempi. Sottogruppi di $\mathbb{Z}$. Definizione di gruppo ciclico. Esempi di gruppi ciclici. Definizione di omomorfismo di gruppi.
Anelli. Esempi. Prime proprietà. Anelli commutativi ed unitari. Esempi. Elementi invertibili e zero-divisori. Domini d'integrità. Corpi. Campi. Esempi.

X Settimana (1 - 3 dicembre 2009)

Caratteristica di un anello commutativo unitario. Caratteristica di un dominio d'integrità. 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. Elementi associati in un dominio d'integrità. Polinomi invertibili a coefficienti in un dominio d'integrità. Algoritmo di divisione tra polinomi.

XI Settimana (10 dicembre 2009)

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 (15 - 17 dicembre 2009)

Teorema di fattorizzazione unica in $K[X]$ con K campo.
Polinomi a coefficienti numerici. Teorema Fondamentale dell'Algebra (solo enunciato).
Polinomi irriducibili di $\mathbb{C}[X]$ e di $\mathbb{R}[X]$.
Polinomi a coefficienti interi: contenuto di un polinomio, polinomi primitivi. Lemma di Gauss. Teorema di fattorizzazione unica in $\mathbb{Z}[X]$. Polinomi irriducibili in $\mathbb{Z}[X]$ ed in $\mathbb{Q}[X]$.