**I Settimana (18-20 febbraio)**

Introduzione al corso. Richiami sulle proprietà dell'anello $\mathbb{Z}/n\mathbb{Z}$ e del gruppo moltiplicativo dei suoi elementi invertibili. Sistemi completi di residui (mod $n$). Inverso aritmetico (mod $n$). Sistemi ridotti di residui (mod $n$). Equazioni diofantee e congruenze polinomiali. Teorema fondamentale sulla risolubilità delle congruenze del tipo $aX \equiv b \pmod{n}$. Esempi. Congruenze lineari ed equazioni diofantee lineari del tipo $aX + bY = c$. Il "piccolo" Teorema di Fermat. Il teorema di Eulero-Fermat. Il teorema di Wilson.

**II Settimana (25-27 febbraio)**

Caratterizzazione dei numeri primi tramite il Teorema di Wilson. Il Teorema Cinese dei Resti. Esempi. Risoluzione di un sistema di congruenze lineari. Esempi ed esercizi. Esistenza di infiniti numeri primi del tipo $4k+3$. Esistenza di infiniti numeri primi del tipo $4k+1$. Risoluzione della congruenza $X^2 \equiv -1 \pmod{p}$. Esponenziazione modulare. Esempi. Numeri pseudoprimi e numeri di Carmichael. Criteri di divisibilità.

**III Settimana (3-5 marzo)**

Risoluzione di congruenze polinomiali $f(X) \equiv 0 \pmod{n}$. Riconduzione del problema generale al caso della risoluzione di congruenze polinomiali $f(X) \equiv 0 \pmod{p^e}$ con $p$ numero primo. Procedimento di determinazione delle soluzioni di $f(X) \equiv 0 \pmod{p^{n+1}}$ a partire dalle soluzioni di $f(X) \equiv 0 \pmod{p^n}$.
Congruenza del tipo $X^{p-1} \equiv 0 \pmod{p^n}$, con $p$ numero primo.
Congruenze del tipo $X^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ e $X^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$ con $p$ numero primo dispari.
Congruenza del tipo $X^{\frac{p(p-1)}{2}} - 1 \equiv 0 \pmod{p^n}$, con $p$ numero primo dispari.
Polinomi identicamente congrui (mod $n$) e congruenze polinomiali equivalenti.
Congruenze polinomiali (mod $p$): teorema di Lagrange.

**IV Settimana (10-12 marzo)**

Applicazioni del teorema di Lagrange. Il gruppo $U_n$. Ordine di un intero modulo $n$. Radici primitive modulo $n$. Un gruppo abeliano finito ha un elemento di ordine l'esponente del gruppo. Un sottogruppo finito del gruppo moltiplicativo di un campo è ciclico. $U_p$ con $p$ numero primo è ciclico. Algoritmo di Gauss per la determinazione delle radici primitive modulo un primo. Esempi ed esercizi. Enunciato del teorema di Gauss sull'esistenza di radici primitive.

**V Settimana (17-19 marzo)**

Radici primitive ed indici. Proprietà degli indici. Tabelle degli indici. Congruenze del tipo $X^m \equiv a \pmod{n}$ con $n$ che possiede una radice primitiva. Criterio di Gauss di risolubulità. Criterio di Eulero per i numeri primi. Risolubilità delle congruenze esponenziali del tipo $a^X \equiv b \pmod{p}$. Esempi ed esercizi.

Congruenze quadratiche e riduzione al caso $X^2 \equiv a \pmod{p}$. Residui quadratici. Il gruppo $Q_n$ dei residui quadratici di $n$. Simbolo di Legendre e sue proprietà. Lemma di Gauss per il calcolo del simbolo di Legendre.

**VI Settimana (26 marzo)**
Calcolo di $\left(\frac{2}{p}\right)$ con il lemma di Gauss. Enunciato della LRQ e suoi corollari; calcolo di $\left(\frac{3}{p}\right)$ con la LRQ. Esempi ed esercizi.

**VII Settimana (31 marzo - 2 aprile)**
Dimostrazione della LRQ. Congruenze quadratiche del tipo $X^2 \equiv a \pmod{p^e}$. Congruenze quadratiche del tipo $X^2 \equiv a \pmod{2^e}$. Numeri primi di Sophie Germain. Esempi. Esercizi.

**VIII Settimana (14-16 aprile)**
Simbolo di Jacobi ed estensione della LRQ. L'equazione diofantea quadratica $X^2 = a$. Terne pitagoriche. Esempi. Esercizi.

**IX Settimana (21-23 aprile)**
Le equazioni diofantee $X^4 + Y^4 = Z^2$ e $X^4 + Y^4 = Z^4$. L'area di un triangolo rettangolo a lati interi non può essere uguale all'area di un quadrato con lato intero, Esercizi, Cenni sull'Ultimo Teorema di Fermat. Numeri primi esprimibili come somma di due quadrati.

**X Settimana (28-30 aprile)**
Elementi irriducibili di $\mathbb{Z}[i]$. Numeri interi somma di due quadrati, Numeri interi differenza di due quadrati, Esempi ed esercizi. Numeri interi somma di tre quadrati, Per ogni primo dispari $p$ la congruenza $X^2 + Y^2 \equiv -1 \pmod{p}$ ha soluzioni.

**XI Settimana (5-7 maggio)**
Identità di Eulero e quaternioni di Hamilton. Ogni intero positivo si può scrivere come somma di quattro quadrati di interi. Problema di Waring. Soluzioni intere positive dell'equazione $X^2 + 2 = Y^3$ e il dominio euclideo $\mathbb{Z}[\sqrt{2}]$ . Equazione di Pell. Dimostrazione dell'esistenza di infinite soluzioni dell'equazione di Pell.

**XII Settimana (12 maggio)**
Frazioni continuate finite semplici e numeri razionali. Cenni sulle frazioni continuate semplici. Risolubilità dell'equazione diofantea $aX + bY = c$ tramite le funzioni continuate finite semplici.

**XIII Settimana (19-23 maggio)**
Esempi ed esercizi.