I Settimana (24-27 febbraio 2009)

Introduzione al corso. Richiami sulla divisibilità in $\mathbb{Z}$, $K[X]$, $\mathbb{Z}[i]$. Richiami sulle proprietà delle congruenze in $\mathbb{Z}$. 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. Congruenze lineari ed equazioni diofantee lineari del tipo $aX + cY = b$. Teorema fondamentale sulla risolubilità delle congruenze del tipo $aX \equiv b \pmod{n}$. Esempi.

II Settimana (3-6 marzo 2009)

Il Teorema cinese dei resti. Il piccolo Teorema di Fermat. Numeri pseudo-primi. Numeri di Carmichael. Teorema di Eulero-Fermat. Il Teorema di Wilson. Caratterizzazione dei numeri primi tramite il Teorema di Wilson. Esistenza di infiniti numeri primi del tipo $4k + 3$. Esistenza di infiniti numeri primi del tipo $4k + 1$. Studio della congruenza $X^2 \equiv -1 \pmod{p}$.

III Settimana (10 marzo 2009)

Criteri di divisibilità (2,3,5,9,11,1001). Esponenziazione modulare. Risoluzione di congruenze polinomiali $f(X) \equiv 0 \pmod{n}$. Esempi.

IV Settimana (17-19-20 marzo 2009)

Risoluzione di congruenze polinomiali $f(X) \equiv 0 \pmod{n}$. Riconduzione del problema generale al caso della risoluzione di congruenze polinomiali $f(X) \equiv 0 \pmod{p^n}$ 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 $X^{p-1} - 1 \equiv 0 \pmod{p^n}$, 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 $X^{\frac{p(p-1)}{2}} - 1 \equiv 0 \pmod{p^2}$, con p numero primo dispari.
Polinomi identicamente congrui (mod n) e congruenze polinomiali equivalenti.
Congruenze polinomiali (mod p): teorema di Lagrange.
Applicazioni del teorema di Lagrange.
Il gruppo U_n. Ordine di un intero modulo n.

V Settimana (24-26 marzo 2009)

Radici primitive modulo n. U_p con p numero primo è ciclico. U_{p^e} con p numero primo dispari ed $e \geqslant 1$ è ciclico. Dimostrazione del teorema di Gauss sull'esistenza di radici primitive. Esempi ed esercizi.

VI Settimana (31 marzo - 2 aprile 2009)

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.

VII Settimana (21-23 aprile 2009)

Congruenze quadratiche e riduzione al caso $X^2 \equiv a \pmod{n}$. Residui quadratici di n. Il gruppo Q_n dei residui quadratici di n. Se $n = 2,\ 4,\ p^h,\ 2p^h$ con p primo dispari, allora Q_n è un gruppo ciclico con $\varphi(n)/2$ elementi . Simbolo di Legendre e sue proprietà. Lemma di Gauss per il calcolo del simbolo di Legendre. Calcolo di $\left(\frac{2}{p}\right)$ con il lemma di Gauss. Esempi ed esercizi.

VIII Settimana (30 aprile)

Definizione di $\sigma_{a,p}$ e dimostrazione della sua relazione con il simbolo di Legendre. LRQ e suoi corollari. Algoritmo per il calcolo del simbolo di Legendre. Esempi. Calcolo di $\left(\frac{3}{p}\right)$ con la LRQ.

IX Settimana (5-7-8 maggio)

Congruenze quadratiche del tipo $X^2 \equiv a \pmod{p^e}$. Congruenze quadratiche del tipo $X^2 \equiv a \pmod{2^e}$. Numero delle soluzioni incongruenti di congruenze quadratiche del tipo $X^2 \equiv a \pmod{n}$. Simbolo di Jacobi ed estensione della LRQ. Cenni sull'equazione diofantea quadratica $X^2 = a$ e le congruenze$X^2 \equiv a \pmod{p}$. Numeri primi di Sophie Germain. Esistenza di infiniti numeri primi del tipo $8k - 1$. Terne pitagoriche. Esempi. Esercizi.

X Settimana (14-15 maggio)

Non esistono triangoli pitagorici isosceli. Cenni sull'Ultimo Teorema di Fermat e sull'anello di Kummer delle radici p-esime dell'unità. Le equazioni diofantee $X^4 + Y^4 = Z^2$ e $X^4 + Y^4 = Z^4$. L'equazione diofantea $X^4 - Y^4 = Z^2$. L'area di un triangolo pitagorico non può essere uguale all'area di un quadrato con lato intero. Numeri primi esprimibili come somma di due quadrati. Elementi irriducibili di $\mathbb{Z}[i]$. Numeri interi somma di due quadrati. Numeri interi differenza di due quadrati. Esempi ed esercizi.

XI Settimana (19-21 maggio)

Numeri interi somma di tre quadrati. Identità di Eulero. Per ogni primo dispari p la congruenza $X^2 + Y^2 \equiv -1 \pmod{p}$ ha soluzioni. Ogni intero positivo si può scrivere come somma di quattro quadrati di interi. Problema di Waring. Richiami sui quaternioni di Hamilton e sugli anelli $\mathbb{Z}[\sqrt{d}]$. Equazione di Pell.

Dimostrazione dell'esistenza di una soluzione (x, y) con $y > 0$ dell'equazione di Pell.