I Settimana (18 - 21 febbraio 2014)

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. Equazioni diofantee lineari del tipo $aX + cY = b$. Risolubilità delle congruenze del tipo $aX \equiv b \pmod{n}$. Esempi.

II Settimana (27 - 28 febbraio 2014)

Il Teorema cinese dei resti. Sistemi di congruenze lineari. Esempi. Il Teorema di Wilson. Caratterizzazione dei numeri primi tramite il Teorema di Wilson. ll piccolo Teorema di Fermat. Numeri pseudo-primi. Il teorema di Eulero-Fermat. Esercizi.

III Settimana (4 - 6 marzo 2014)

Criteri di divisibilità per 2, 3, 4, 5, 9, 11, 2^m, 5^m, 1001 e per un qualunque intero positivo d primo con 10.
Esistenza di infiniti numeri primi. Esistenza di infiniti numeri primi del tipo $4k + 3$.
Studio della congruenza $X^2 \equiv -1 \pmod{p}$.
Esistenza di infiniti numeri primi p per i quali la congruenza $f(X) \equiv 0 \pmod{p}$ è risolubile. Esistenza di infiniti numeri primi del tipo $4k + 1$.
Applicazioni del piccolo teorema di Eulero-Fermat e del teorema di Wilson. Esponenziazione modulare. Esempi ed esercizi.

IV Settimana (11 - 13 marzo 2014)

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. Esempi.
Procedimento di determinazione delle soluzioni di $f(X) \equiv 0 \pmod{p^{n+1}}$ a partire dalle soluzioni di $f(X) \equiv 0 \pmod{p^n}$. Esempi.
Polinomi di $\mathbb{Z}[X]$ identicamente congrui (mod n); polinomi di $\mathbb{Z}[X]$ equivalenti (mod n). Congruenze polinomiali (mod p), con p numero primo. Teorema di Lagrange.
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. Esempi.

V Settimana (18 - 20 marzo 2014)

Esempi di congruenze polinomiali $f(X) \equiv 0 \pmod{p^n}$ con p numero primo con soluzioni non singolari.
Il gruppo U_n. Ordine di un intero modulo n.

Radici primitive modulo n.
Esponente di un gruppo abeliano finito. Esempi. 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. U_{p^e} con p numero primo dispari ed $e \geqslant 1$ è ciclico.

VI Settimana (25 - 27 marzo 2014)

Enunciato del Teorema di Gauss.
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 e a e n coprimi. Criterio di risolubilità di Gauss . Esempi.
Congruenze del tipo $X^m \equiv a \pmod{p}$ con p primo e $p \not| a$. Criterio di risolubilità di Eulero. Esempi.
Dimostrazione del teorema di Gauss sull'esistenza di radici primitive.
Risolubilità delle congruenze esponenziali del tipo $a^X \equiv b \pmod{p}$. Esempi ed esercizi.

VII Settimana (8 - 10 - 11 aprile 2014)

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. Lemma di Gauss per il calcolo del simbolo di Legendre. Calcolo di $\left(\frac{2}{p}\right)$ con il lemma di Gauss. 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.

VIII Settimana (15 - 17 aprile)

Calcolo di $\left(\frac{3}{p}\right)$ con la LRQ. 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 $X^2 \equiv 1 \pmod{2^e}$. Numero delle soluzioni incongruenti di 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.

IX Settimana (29 aprile)

Terne pitagoriche. Esempi. Esercizi.

X Settimana (6 - 8 maggio)

Definizione ed esempi di funzioni aritmetiche. Funzioni aritmetiche moltiplicative e totalmente moltiplicative. Funzioni dei divisori: τ e σ. Moltiplicatività di τ. Definizione della funzione σ_f con f funzione aritmetica. $\tau = \sigma_{\mathbf{1}}$, con $\mathbf{1}$ funzione identicamente uguale ad 1 da N^+ in $\mathbb{C}$ e $\sigma = \sigma_{\mathbf{e}}$ con $\mathbf{e}$ immersione di N^+

in $\mathbb{C}$. Moltiplicatività della funzione σ_f con f funzione aritmetica moltiplicativa. Definizione della funzione di Möbius μ ; moltiplicatività di μ. $\sigma_\mu = \mathbf{u}$ con $\mathbf{u} : \mathbb{N}^+ \longrightarrow \mathbb{C}$ definita da $\mathbf{u}(1) = 1$ e $\mathbf{u}(n) = 0$ se $n \geqslant 2$. Formula di inversione di Möbius. Una funzione aritmetica f è moltiplicativa se e solo se σ_f è moltiplicativa.
$\sigma_\varphi = \mathbf{e}$ (due dimostrazioni).
Definizione e proprietà del prodotto di Dirichlet tra funzioni aritmetiche;
l'insieme delle funzioni aritmetiche f con $f(1) \neq 0$ è un gruppo abeliano rispetto al prodotto di Dirichlet . Esercizi.

XI Settimana (13 - 15 maggio)

$\mu(n)$ è la somma delle radici n-esime primitive dell'unità. Non esistono triangoli pitagorici isosceli. Cenni sull'Ultimo Teorema di Fermat. Le equazioni diofantee $X^4 + Y^4 = Z^2$ e $X^4 + Y^4 = Z^4$.
S_k. Numeri primi esprimibili come somma di due quadrati. S_2 è chiuso rispetto al prodotto. Richiami sull'anello degli interi di Gauaa. Numeri primi esprimibili come somma di due quadrati. Numeri interi somma di due quadrati. Esempi.

XII Settimana (20 - 22 maggio)

Per ogni primo dispari p la congruenza $X^2 + Y^2 \equiv -1 \pmod{p}$ ha soluzioni (due dimostrazioni). Ogni intero positivo si può scrivere come somma di quattro quadrati di interi. Frazioni continue finite semplici e numeri razionali. Cenni sulle frazioni continue semplici. Risolubilità dell'equazione diofantea $aX + bY = c$ tramite le funzioni continue finite semplici. Esercizi.