TN410 TN410: Introduzione alla Teoria dei Numeri

A.A. 2012/2013

Prof. Francesca Tartarone

1. Teoria delle congruenze

Congruenze e polinomi. Congruenze polinomiali: soluzioni, relazione con le soluzioni di equazioni diofantee. Congruenze lineari in una indeterminata. Risolubilità, numero di soluzioni e ricerca di soluzioni.

Equazioni diofantee lineari in due e tre indeterminate. Relazione con le congruenze lineari. Risolubilità e ricerca di soluzioni.

Sistema ridotto di residui. Numero di elementi in un sistema ridotto di residui. Il "piccolo" teorema di Fermat. Il teorema di Euler(–Fermat). Prime applicazioni: risolubilità di congruenze lineari. Teorema di Wilson e caratterizzazione dei numeri primi. Teorema cinese dei resti. Risoluzione di sistemi di congruenze lineari.

Generalità sulle congruenze polinomiali. Uso del teorema cinese dei resti per ricondurre il problema generale al caso di congruenze polinomiali modulo una potenza di un numero primo. Tecnica di risoluzione (mod p^{n+1}) conoscendo le soluzioni (mod p^n). Congruenze polinomiali (mod p): teorema di Lagrange, numero delle soluzioni distinte.

Radici primitive (mod n). Esistenza di radici primitive (mod p). Numero delle radici primitive distinte.

Generalità sulle congruenze monomiali del tipo $X^m \equiv a \pmod{p}$. Teorema di Gauss di caratterizzazione degli interi che possiedono radici primitive (cenni). Applicazioni alla risoluzione di congruenze del tipo $X^m \equiv a \pmod{n}$. Numero di soluzioni. Indice di un elemento relato ad una radice primitiva. Prime proprietà dell'indice. Metodi effettivi di risolubilità di congruenze del tipo $X^m \equiv a \pmod{p}$. Criterio di risolubilità di Euler e di Gauss.

Risoluzione di una congruenza polinomiale in r indeterminate (mod p). Teoremi di Lagrange e di Chavelley.

Congruenze quadratiche: generalità e riduzione al caso $X^2 \equiv a \pmod{n}$. Residui quadratici. Numero dei residui quadratici (mod p). Distribuzione dei residui e dei non–residui quadratici.

Simbolo di Legendre. Prime proprietà del simbolo di Legendre. Criterio di Euler. Lemma di Gauss e Legge di Reciprocità Quadratica. Prime applicazioni. Calcolo del simbolo di Legendre. Metodi di risoluzione di congruenze quadratiche modulo la potenza di un primo (caso dispari e pari). Numero delle soluzioni incongruenti. Simbolo di Jacobi. Risoluzione delle congruenze del tipo $X^2 \equiv a \pmod{n}$: criteri di risolubilit e numero delle soluzioni. Forma generalizzata della Legge di Reciprocità Quadratica.

2. Funzioni Moltiplicative

Funzioni aritmetiche, moltiplicative e totalmente moltiplicative. La funzione φ di Euler, le funzioni σ (somma di divisori) e τ (numero dei divisori) e la funzione σ^k.

Per ogni funzione aritmetica moltiplicativa f , studio della funzione aritmetica moltiplicativa associata σ_f.

La funzione μ di Möbius. La formula di inversione di Möbius.

Il gruppo delle funzioni aritmetiche moltiplicative rispetto al prodotto di Dirichlet.

3. Somme di quadrati

Interi somma di due quadrati. Lemma di A. Thue di approssimazione razionale. Teorema di Fermat sui primi esprimibili come somma di due quadrati. Caratterizzazione degli interi che possono essere rappresentati come somma di due quadrati.

Caratterizzazione degli interi che si possono scrivere come somma di tre quadrati.

Interi che si possono scrivere come somma di quattro quadrati (cenni). Lemma di Euler. Teorema risolutivo di Lagrange (cenni). Problema di Waring (cenni).

4. Studio di alcune equazioni diofantee

L'equazione diofantea $X^2+Y^2 = Z^2$: teorema fondamentale sulle terne pitagoriche. Triangoli pitagorici con la stessa area e stessa ipotenusa sono uguali. Alcune proprietà notevoli dei triangoli pitagorici.

Le equazioni diofantee $X^4+Y^4 = Z^2$ e $X^4+Y^4 = Z^4$. Metodo della discesa infinita di Fermat.

L'equazione diofantea di Mordell $Y^2 = X^3 + k$. Studio di alcuni casi per i quali tale equazione non è risolubile (cenni). Equazione di Pell: prime proprietà, Teorema di esistenza di infinite soluzioni distinte. Soluzione Fondamentale e rappresentazione di tutte le soluzioni tramite la soluzione fondamentale.

Testi consigliati

[1] M. Fontana, Appunti disponibili in rete. - http://tn410-2012-2013.blogspot.it/

[2] G.A. Jones e J.M. Jones, *Elementary Number theory*. Springer, (1998).

Bibliografia supplementare

[3] D. M. Burton, *Elementary number theory*. Allyn and Bacon, (1976).

[4] H. Davenport, *Aritmetica superiore. Un'introduzione alla teoria dei numeri*. Zanichelli, (1994).

[5] K.H. Rosen, *Elementary number theory and its applications*. Addison Wesley, (1985).

Modalità d'esame

- valutazione in itinere ("esoneri")		■ SI	□ NO
- esame finale	scritto	■ SI	□ NO
	orale	■ SI	□ NO
- altre prove di valutazione del profitto (meglio descritte sotto)		□ SI	■ NO