AL2 Algebra (2^0 Modulo)

A.A. 2000/2001

Prof. Marco Fontana

Teoria elementare dei numeri

1. Teoria delle congruenze

Congruenze e polinomi.

Sistema completo di residui mod n. Inverso aritmetico mod n: esistenza ed unicità. 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 (o più) 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.

Ordine di un elemento mod n. Prime proprietà dell'ordine. Radici primitive mod n. Esistenza di radici primitive mod p. Numero delle radici primitive distinte.

Generalità sulle congruenze monomiali del tipo $X^m \equiv a$ mod p. Teorema di Gauss di caratterizzazione degli interi che possiedono radici primitive (cenni). Applicazioni alla risoluzione di congruenze del tipo $X^m \equiv a$ mod n. Numero di soluzioni. Indice relativamente ad una radice primitiva. Prime

proprietà dell'indice. Metodi effettivi di risolubilità di congruenze del tipo $X^m \equiv a$ mod p. Criterio di risolubilità di Euler e di Gauss.

Congruenze quadratiche: generalità e riduzione al caso $X^2 \equiv a$ mod 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. Forma generalizzata della Legge di Reciprocità Quadratica.

2. 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.

Cenno al problema relativo alla caratterizzazione degli interi che si possono scrivere come somma di tre quadrati (Legendre, Gauss, Dirichlet).

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

3. 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'area di un triangolo pitagorico non può essere uguale all'area di un quadrato con lato intero.

L'equazione diofantea di Mordell $Y^2 = X^3 + k$. Studio di alcuni casi per i quali tale equazione non è risolubile. Cenni su problemi aperti.

Curve ellittiche (cenni).

L'equazione di Pell(–Fermat) $X^2 - dY^2 = 1$. Soluzione fondamentale e determinazione di tutte le infinite soluzioni di tale equazione (cenni).

Cenni sulle applicazioni dell'equazione di Pell. Equazioni diofantee del tipo $X^2 - dY^2 = n$ (cenni).

4. Funzioni aritmetiche

Funzioni moltiplicative. La funzione φ di Euler e le funzioni σ (somma di divisori) e τ (numero dei divisori).

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.

****

Il materiale didattico del corso (testi di esercizi di "esonero", di prove scritte a casa, di esercizi dell'attività di tutorato e gli appunti del corso) è *disponibile al sito:*

`http://www.mat.uniroma3.it`

Didattica CdS Matematica → CdL n.o. → Didattica Interattiva → AL2

TESTI CONSIGLIATI

[1] M. FONTANA, Appunti distribuiti durante il corso.
[2] W.W. ADAMS – L.J. GOLDSTEIN, *Introduction to number theory*. Prentice-Hall, (1976).
[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).

BIBLIOGRAFIA SUPPLEMENTARE

[6] Z.I. BOREVICH – I.R. SHAFAREVICH, *Number theory*. Academic Press, (1964).
[7] C.F. GAUSS, *Disquisitiones Arithmeticae (trad. Ingl.)*. Yale Univ. Press, (1966).
[8] G.H. HARDY – E.M. WRIGHT, *An introduction to the theory of numbers*. Oxford Univ. Press, (1960). (4a Ed.).
[9] W.J. LEVEQUE, *Fundamentals in number theory*. Addison Wesley, (1977).
[10] H. E. ROSE, *A course in number theory*. Oxford Science Publ., (1988).
[11] A. WEIL, *Number theory: an approach through history*. Birkhäuser, (1983).

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

Gli studenti che hanno sostenuto con esito positivo, nel corso del semestre, le prove di valutazione parziale ("esoneri") accedono direttamente al colloquio di verbalizzazione del voto proposto dal docente, da effettuarsi durante la I Sessione di esame (I^o o II^o Appello).

Per tutti gli studenti che non si avvalgono della possibilità della valutazione del profitto durante il corso, l'esame finale consiste in una prova scritta, comprendente anche domande di tipo teorico.

Si noti che, in presenza di una valutazione positiva delle prove parziali durante il corso, l'eventuale consegna da parte dello studente di una successiva prova scritta di esame comporta la rinuncia implicita al "voto di esonero". Pertanto, in tal caso, la valutazione del profitto del corso verrà effettuata in base alla prova d'esame.