TN1 Introduzione alla teoria dei numeri

A.A. 2007/2008

Prof. Florida Girolami

1. Teoria delle congruenze

Richiami sulle proprietà dell'anello Z/nZ 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 $aX \equiv b \pmod{n}$. 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. Caratterizzazione dei numeri primi tramite il Teorema di Wilson. Il Teorema Cinese dei Resti. Esempi. Equazioni diofantee lineari in tre indeterminate. Congruenze lineari in due indeterminate. Risoluzione di un sistema di congruenze lineari. Sistemi lineari di congruenze: metodo di Cramer. Matrice dei coefficienti e matrice completa. Esistenza ed unicita' della soluzione nel caso in cui il delta e' invertibile. Esistenza della soluzione nei casi in cui il rango della matrice completa coincide con il rango della matrice dei coefficienti. 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. Numeri pseudoprimi e numeri di Carmichael. Criteri di divisibilità. 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. 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. Enunciato del teorema di Gauss sull'esistenza di radici primitive. 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 $a^X \equiv b \pmod{p}$. 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. Calcolo di $\left(\frac{2}{p}\right)$ con il lemma di Gauss. LRQ e suoi corollari; 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 $X^2 \equiv a \pmod{2^e}$. Numeri primi di Sophie Germain. Simbolo di Jacobi ed estensione della LRQ. L'equazione diofantea quadratica $X^2 = a$.

2. Funzioni aritmetiche

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. Studio di alcune equazioni diofantee

L'equazione diofantea $X^2 + Y^2 = Z^2$: teorema fondamentale sulle terne pitagoriche.

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 è mai uguale all'area di un quadrato con lato intero. Cenni sull'Ultimo Teorema di Fermat.

4. Somme di quadrati

Numeri primi esprimibili come somma di due quadrati. Elementi irriducibili di $Z[i]$. Numeri interi somma di due quadrati, Numeri interi differenza di due quadrati. Numeri interi somma di tre quadrati. Per ogni primo dispari p la congruenza $X^2 + Y^2 \equiv -1 \pmod{p}$ ha soluzioni. 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 $Z[\sqrt{2}]$. Equazione di Pell. Dimostrazione dell'esistenza di infinite soluzioni dell'equazione di Pell. 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.

Testi consigliati

[1] M. Fontana, Appunti del corso disponibili in rete - http://www.mat.uniroma3.it → didattica interattiva → TN1.
[2] D. M. Burton, *Elementary Number Theory*. Allyn and Bacon, (1976). (4a Ed.).
[3] G.H. Hardy – E.M. Wright, *An introduction to the theory of numbers*. Oxford Univ. Press, (1960). (4a Ed.).

Bibliografia supplementare

[4] H. Davenport, *Aritmetica superiore. Un'introduzione alla teoria dei numeri*. Zanichelli, (1994).
[5] C.F. Gauss, *Disquisitiones Arithmeticae (trad. Ingl.)*. Yale Univ. Press, (1966).
[6] I. Niven – H. Zuckerman – H. Montgomery, *An introduction to the theory of numbers. Fifth edition*. John Wiley & Sons, (1991).
[7] 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