TN1 introduzione alla teoria dei numeri
A.A. 2003/2004

Prof. Francesco Pappalardi

http://www.mat.uniroma3.it/users/pappa/CORSI/TN1_03_04/TN1.htm

1. Teoria della congruenze

Proprietà elementari delle congruenze, criteri elementari di divisibilità, congruenze lineari ed equazioni diofantee lineari, il piccolo Teorema di Fermat ($a^p \equiv a \bmod p$) e il Teorema di Eulero ($a^{\varphi(m)} \equiv 1 \bmod m \Leftarrow (a, m) = 1$), Teorema di Wilson ($(p-1)! \equiv -1 \bmod p$), Teorema cinese dei resti, l'algoritmo dei quadrati successivi, generalità sulle congruenze polinomiali, derivate formali, Teorema del sollevamento, Teorema di Lagrange, radici primitive dell'unità, Teorema di Gauss sull esistenza di radici primitiva ($\exists g \in \mathbf{Z}$ t.c. $\langle g \bmod n\rangle = (\mathbf{Z}/n\mathbf{Z})^* \iff n = 2, 4, p^k, 2p^k (k \in \mathbf{N}, p \geq 3)$), algoritmo di Gauss per il calcolo di radici primitive, congruenze del tipo $X^m \equiv a(\bmod n)$, congruenze quadratiche, simboli di Legendre e proprietà, criterio di Eulero, Lemma di Gauss ($\left(\frac{2}{q}\right) = (-1)^{(p^2-1)/8}$), legge di reciprocità ($\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$), simboli di Jacobi e calcolo dei simboli di Legendre senza fattorizzare.

2. Funzioni aritmetiche

Generalità, funzioni aritmetiche moltiplicative e totalmente moltiplicative, esempi: $\varphi, \tau, \sigma, \sigma_k, \mathbb{1}, e, u$, prodotto di Dirichlet di funzioni aritmetiche, gruppo delle funzioni aritmetiche moltiplicative, formule di inversione di Möbius.

3. Terne pitagoriche

Generalità, terne pitagoriche primitive, terne pitagoriche positive, teorema di classificazione delle terne pitagoriche, discesa di Fermat e l'equazione diofantea $X^4+Y^4 = Z^2$.

4. Interi che sono somme di due quadrati

Generalità, Teorema di Fermat sui primi che possono essere scritti come somma di due quadrati ($p = \square + \square \Leftrightarrow p \not\equiv 3 \bmod 4$), Teorema di caratterizzazione sui numeri che possono essere scritti come somma di due quadrati ($n = \square + \square \iff \forall p|n, \big(p \equiv 3(\mathrm{mod} 4) \Rightarrow v_p(n) = 2\alpha\big)$), numero di espressioni.

5. Interi che sono somma di quattro quadrati

Generalità, enunciato del Teorema di Legendre Gauss sui numeri che si possono scrivere come somma di 3 quadrati ($n = \square + \square + \square \iff n \neq 4^e(8k + 7) \forall e, k \in \mathbf{N}$), Formula di Eulero ($(\square + \square + \square + \square) \cdot (\square + \square + \square + \square) = \square + \square + \square + \square$), Teorema di Lagrange ($n = \square + \square + \square + \square$), enunciato del problema di Waring.

Testi consigliati

[1] M. Fontana, Note - http://www.mat.uniroma3.it/users/fontana/.

[2] G.H. Hardy – E.M. Wright, *An introduction to the theory of numbers*. The Clarendon Press, Oxford University Press, New York, (1979). (5a Ed.).

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

Bibliografia supplementare

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

[5] Z.I. Borevich – I.R. Shafarevich, *Number theory*. Academic Press, (1964).

[6] Autori Vari, *Dispense Online*. http://www.mat.uniroma3.it/ntheory/lecture_notes.html.

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