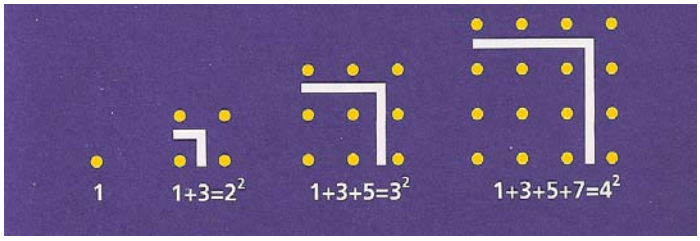
Innovazione e tradizione nella matematica e nel suo insegnamento

Ciclo di Conferenze



:: Lunedì 19 aprile 2010, ore 15:30

Aula Parco, Scienze della Formazione Primaria, Università di Roma Tre
via Ostiense 139, piano terra

Francesco Pappalardi
Università di Roma Tre

L'indagine sui numeri e la crittografia

"E ho capito perché la maestra ci ha dato questi numeri!
Perché ci ha fatto scoprire che non sempre puoi fare gli schieramenti.
Col 13 non c'è stato verso, i soldati li ho dovuto mettere per forza in fila indiana. Col 14 invece, visto che è uguale a 2 x 7, ho potuto schierarli in 2 file da 7 (ma potevo fare anche 7 file da 2) e col 15, che è 3 x 5, li ho sistemati in 3 file da 5 (Mattia, invece, ha disegnato 5 file da 3)"
Anna Cerasoli, *Sono il numero 1*

L'indagine matematica sui numeri primi è iniziata nel mondo greco e prosegue fino a oggi. Eppure, l'idea di divisore e quella di numero primo è fra quelle che possono capire e che posso interessare i i bambini più piccoli. La teoria dei numeri è stata sviluppata senza nessuna motivazione di indole pratica, come scrive Platone, "fino a tal punto che l'intelligenza possa contemplare la natura dei numeri, non già occupandosene a scopo di compra e vendita, come mercanti e rivenditori". Eppure, questa branca della matematica ha mostrato sorprendenti applicazioni dalla fine del Novecento, con ricadute nella sicurezza militare, delle comunicazioni e degli scambi commerciali. A partire dagli anni Ottanta del Novecento, dopo le scoperte di due studiosi statunitensi, il matematico Whitfield Diffie e l'ingegnere elettronico Martin Hellman, pubblicate in un fondamentale lavoro del 1976, i numeri primi hanno fatto il loro ingresso in crittografia. In questo seminario mostreremo alcune possibili applicazioni dei numeri primi in crittografia discutendo alcuni problemi aperti e aspetti storici collegati.

Francesco Pappalardi è professore presso il Dipartimento di Matematica di Roma Tre e si occupa di teoria dei numeri.