NUMERI PRIMI

Bologna 8/3/04

$n > 1$ e' **primo** se e' divisibile solo per 1 e per se stesso.

Gli antichi Greci si interessarono molto ai numeri primi; perche' i primi sono interessanti ? Sono i "*mattoni fondamentali*" con cui costruire i numeri interi:

Teorema Fondamentale dell'Aritmetica: ogni intero si fattorizza in modo unico come prodotto di primi.

Osservazione: dimostrazione semplice ma non banale; esempio di **Hilbert** di semplice "sistema numerico" in cui non vale la *fattorizzazione unica*: interi della forma $4k + 1$ con $k = 0, 1, ...$;

$$693 = 9 \cdot 77 = 21 \cdot 33$$

e 9, 77, 21, 33 sono "primi" in tale sistema.

"Quanti sono" i numeri primi ?

Teorema di Euclide: esistono infiniti numeri primi.

Come si "costruiscono" i numeri primi ?
Crivello di Eratostene:
- si scrivono tutti gli interi fino a N;
- si cancellano i multipli di 2, poi i multipli di 3 (il primo intero non cancellato), poi i multipli di 5 (il nuovo primo intero non cancellato), e cosi' via;
- arrivati a $\sqrt{N}$ ci si ferma: i numeri non cancellati sono tutti e soli i primi fino a N.

Osservazione: l'algoritmo di Eratostene e' semplice ma "*lento*", ovvero: **alta complessita' computazionale**; sono noti **algoritmi di primalita'** piu' *veloci* ma decisamente piu' *sofisticati*. Recentemente, per le esigenze della **crittografia a chiave pubblica** (metodo **RSA**, utilizzato su Internet), forte sviluppo: algoritmo di primalita' **polinomiale**; molto "*veloce*", con complessita' dell'ordine di

$$(\log n)^c.$$

Problemi classici sui numeri primi

1) *Distribuzione dei numeri primi*

Quanti sono i numeri primi fino a x ? (x "molto grande"). Ovvero: ordine di grandezza di

$$\pi(x) = \text{numero dei primi p} \leq \text{x.}$$

Congettura di **Gauss** (fine '700): $\pi(x) \sim \frac{x}{\log x}$

prima meta' '800: metodi elementari (**Chebyshev**)

1859: **Riemann** introduce la **funzione zeta**

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p (1 - \frac{1}{p^s})^{-1}$$

nello studio dei primi; le idee di Riemann portano nel 1896 alla dimostrazione della congettura di Gauss, il **Teorema dei Numeri Primi** (**Hadamard** e **de la Vallée Poussin**).

Problema aperto: **Ipotesi di Riemann** sugli zeri della funzione $\zeta(s)$; conseguenza: stima ottimale per la funzione $\pi(x)$.

2) *Distanza tra numeri primi consecutivi*

Successione dei primi: $p_1, p_2, ..., p_n, ...$; come si comportano le differenze

$$p_{n+1} - p_n$$

al variare di n ? Due famosi problemi aperti:

- tra due quadrati perfetti consecutivi c'e' sempre un numero primo (ovvero: $p_{n+1} - p_n < \sqrt{p_n}$)

- congettura dei **primi gemelli**: esistono infiniti primi p tali che che $p + 2$ e' ancora primo (3 e 5, 5 e 7, 11 e 13, 17 e 19, 29 e 31, ...), ovvero: $p_{n+1} - p_n = 2$ per infiniti n.

3) *Primi rappresentati dai polinomi*

Polinomio irriducibile: non e' prodotto di polinomi (a coeff. interi).

Congettura: se P e' un polinomio irriducibile allora $P(n)$ e' primo per infiniti n.

E' nota per i polinomi di grado 1 (progressioni aritmetiche, **Dirichlet** prima meta' '800); non e' nota per *alcun* polinomio di grado ≥ 2 e non si sa neppure dimostrare che *esiste* un tale polinomio!

4) *Congettura di Goldbach*

Congettura: ogni intero *pari* ≥ 4 e' somma di due numeri primi.

La congettura di Goldbach e' stata verificata al computer fino agli attuali limiti di computabilita'.

Sono note le seguenti "*approssimazioni*" alla congettura di Goldbach:

- ogni intero *dispari* e' somma di 3 primi (**Vinogradov**, 1936)

- "*quasi tutti*" gli interi *pari* sono somma di 2 primi (scuola di Vinogradov, anni '30; sostanziali miglioramenti di **Montgomery-Vaughan**, 1975)

- ogni intero *pari* e' somma di un primo e un "*quasi-primo*" P_2 (ovvero un numero con al piu' 2 fattori primi; **Chen**, 1966).