MATHESIS

Società Italiana di Scienze Matematiche e Fisiche - 1895
Sezione di Roma
21 gennaio 2007

Antonio Salmeri

"Capire la Matematica attraverso la Storia"

NELL'AFFASCINANTE MONDO DEI NUMERI PRIMI

Introduzione

Fra gli argomenti che potevo scegliere per quest'incontro, ho preferito questo per vari motivi:

- in primo luogo perchè l'interesse sui numeri primi ha radici antichissime; se ne occuparono gli antichi greci ed ancora oggi, a distanza di millenni l'argomento è uno dei più studiati.
- in secondo luogo perchè, pur essendo uno degli argomenti più complessi della matematica, basta pensare che la maggior parte delle congetture non sono ancora dimostrate nonostante l'impegno dei più famosi matematici, è oggetto di grande interesse anche da parte dei non addetti ai lavori e dei mezzi di comunicazione;
- infine perchè, nonostante la grande complessità della teoria, gli argomenti che tratterò sono interessanti e accessibili anche per i non addetti ai lavori;
- inoltre è uno dei pochi campi della scienza per i quali sono messi in palio ricchissimi premi per coloro che troveranno la dimostrazione di congetture che resistono da secoli agli attacchi dei maggiori esperti mondiali.

Definizione

Un numero positivo N si dice primo se N è diverso da 1 ed è divisibile esattamente solo per 1 e per se stesso.

Il numero 1 non è primo poiché ha un solo divisore; la scelta di non definire 1 come numero primo è dovuta a vari motivi: tra questi c'è il fatto che una tale definizione costringerebbe a riformulare in modo più complicato diversi teoremi di matematica, come ad esempio il teorema fondamentale del-l'aritmetica.

Ricerca dei numeri primi

Il metodo più veloce per trovare tutti i numeri primi inferiori ad un limite L prefissato è ancora oggi il "crivello di Eratostene".

Tutti i tentativi di trovare espressioni che forniscono soltanto numeri primi sono falliti, come la notissima relazione $n^2 - n + 41$ che fornisce numeri primi per n da 0 a 39, ma per $n = 40$ e ovviamente per $x = 41$, non dà un numero primo e la relazione $n^2 – 79n + 1601.$ che dà luogo a numeri primi per ogni n fino a 79, ma non per n = 80.

La ricerca di espressioni semplici che forniscono soltanto numeri primi è risultata vana.

Fu Euclide che dimostrò con molta eleganza che i numeri primi formano una successione infinita.

La distribuzione dei numeri primi non è però regolare e la differenza fra due numeri primi consecutivi non è prevedibile a priori.

Il passo decisivo nella ricerca di una legge da cui dipenda la distribuzione dei numeri primi fu fatto quando si cercò la legge della distribuzione media dei primi fra i numeri interi.

La distribuzione dei singoli primi tra gli interi è estrema-mente irregolare, ma questa irregolarità sparisce se si guarda la distribuzione media data dal rapporto $\pi(N) / N$.

Fu Gauss che tentò di capire se era possibile trovare una relazione fra N e $\pi(N)$, numeri primi minori di N.

Osservò che si profilava una stupefacente regolarità:

$$\pi(N) \sim N / \ln (N)$$

che vale senz'altro per N tendente all'infinito.
Legendre nel 1798 trovò, esaminando i numeri primi sino a 400 000 che con molta approssimazione si ha:

$$\pi(N) \sim N / [\ln (N) - 1{,}08366] .$$

Valori molto più approssimati si ottengono con la funzione Li (logaritmo integrale), sempre di Gauss, e soprattutto con la funzione R(N) che coinvolge esplicitamente la funzione zeta di Riemann.
Per cui si potette scrivere la seguente tabella, dove:
C = distanza media fra due numeri primi successivi

A = N	B = π (N)	C
10	4	2.5
100	25	4,0
1 000	168	6,0
10 000	1 229	8,1
100 000	9 592	10,4
1 000 000	78 498	12,7
10 000 000	664 579	15,0
100 000 000	5 761 455	17,4
1 000 000 000	50 847 534	19,7
10 000 000 000	455 052 511	22,0
…….	……	….
10^{100}	~ $4{,}34 \times 10^{97}$	230

Numeri primi particolari
Si trascrivono qui di seguito alcuni numeri primi singolari:

1) 1212121212121212……. 121212121 (7809 cifre)
2) 12345678 12345678 123 ….1234567 (1031 cifre)
3) 765432 765432 765432…… .765432 7 (1501 cifre)
4) 6789 6789 6789 6789 6789. ..6789 67 (818 cifre)

Questi numeri primi sono stati trovati da Giovanni Di Maria utilizzando i software *WinPFGM* e *Pari/GP*.
Osserviamo che un numero di 1000 cifre è lungo 3 metri (una cifra ogni 3 millimetri), pertanto il più grande numero primo conosciuto, che ha oltre 9 milioni e ottocentomila cifre, è lungo circa 30 chilometri! Un numero primo, unico ad avere questa proprietà, è:

$$5882353 = 588^3 + 2353^3$$

Numeri primi palindromi

Ricordiamo che un numero, ma anche una parola o una frase, si dice palindromo quando si può leggere indifferentemente sia sinistra verso destra che da destra verso sinistra.
Nella sequenza dei numeri primi si trovano nell'ordine:
11 – 101 – 131 – 151 – 181 – 313 – 353 – 373 ..
A titolo di curiosità elenchiamo alcune parole e frasi palindrome: nella lingua italiana si hanno le parole:

aerea - anilina - ingegni - ossesso - radar

ma anche frasi:

Anita lava la tina – arca sacra – Etna gigante -i topi non avevano nipoti - ai lati d'Italia

ed addirittura interi brani.
Fra le innumerevoli curiosità, per le quali si rimanda a siti specializzati, proponiamo i seguenti: Una lista di numeri primi palindromi che si accresce ogni volta a destra e a sinistra con coppie di numeri ovviamente simmetrici fra loro:

2
30203
133020331
1713302033171
12171330203317121
151217133020331712151
18151217133020331712151 81
…….ed altre quattro righe

Più interessante è la sequenza di 10 numeri primi palindromi di 27 cifre nei quali le cinque cifre centrali sono fra loro in progressione aritmetica di ragione 10101.

742950290870000078092059247
742950290871010178092059247
742950290872020278092059247
742950290873030378092059247
742950290874040478092059247
742950290875050578092059247
742950290876060678092059247
742950290877070778092059247
742950290878080878092059247
742950290879090978092059247

Ovviamente gli stessi numeri di 27 cifre sono in progressione aritmetica con ragione R =1010100000000000.

Numeri di Mersenne

Occupano un posto preminente nella storia dei numeri primi i *Numeri di Mersenne*, essi sono della forma

$$M_n = 2^n - 1.$$

Molti di essi sono primi e sono pertanto detti *Numeri primi di Mersenne*, tali sono quelli per n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127. Quest'ultimo di ben 39 cifre.

Se M_n è primo, allora n è primo, non vale il viceversa. I numeri primi di Mersenne sono collegati con i *numeri perfetti* di cui parleremo più avanti.

I numeri primi di Mersenne, alla data odierna, sono 44, l'ultimo è stato trovato nel settembre del 2006 ed è ad oggi il più grande primo conosciuto.

L'uso dei calcolatori ha accelerato la scoperta dei numeri primi di Mersenne, ma forse deve destare più ammirazione il numero di 39 cifre trovato nel 1876 che non i numeri di milioni di cifre trovati sfruttando le risorse di migliaia di computer collegati in rete. In ogni caso si tratta di diverso tipo di abilità.

Numeri perfetti e amicabili

Un numero intero si dice perfetto se è uguale alla somma dei suoi divisori incluso 1 ed escluso se stesso.

Il più piccolo numero perfetto è: 6 = 1 + 2 + 3.

I matematici greci da Pitagora ad Euclide erano affascinati dalla ricerca di questi rarissimi numeri, oltre al numero 6 trovarono 28, 496 e 8128.

Dovettero passare diciassette secoli per trovare il quinto numero perfetto, ed altri due secoli per trovare il sesto ed il settimo rispettivamente di 10 e 12 cifre.

Prima dell'avvento del computer ne furono scoperti dodici, il più grande, di 77 cifre, fu trovato da E. Lucas.

Il più grande numero perfetto ha più di 19 milioni!

Tutti i numeri perfetti sinora trovati sono pari, ma non si può escludere che se ne possa trovare uno dispari, ed ammesso che esista esso deve essere il prodotto di almeno 29 numeri primi. Non si sa se il loro numero sia finito o infinito.

Una notevole proprietà, ma ce ne sono moltissime altre, è quella che tutti i numeri perfetti, ad eccezione del 6, sono uguali alla somma della successione dei numeri dispari elevati al cubo:

$28 = 1^3 + 3^3$

$496 = 1^3 + 3^3 + 5^3 + 7^3$

$8128 = 1^3 + 3^3 + 5^3 + 7^3 + 9^3 + 11^3 + 13^3 + 15^3$

.....

I numeri perfetti (Np) sono intimamente legati ai numeri primi di Mersenne dalla seguente relazione:

$$NP_p = 2^{p-1} M_p$$

e questa relazione ha permesso di trovare numeri perfetti di milioni di cifre.

Numeri amicabili

Si chiamano *numeri amicabili* quelli per i quali la somma dei divisori del primo è uguale al secondo e viceversa la somma dei divisori del secondo è uguale al primo.
Si riporta per maggiore chiarezza l'esempio classico:

220 è divisibile per 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110
284 = 1+2+4+5+10+11+20+22+44+55+110
284 è divisibile per 1, 2, 4, 71, 142
220 = 1+2+4+71+142

Attualmente ne sono note oltre undici milioni di coppie.

Numeri primi gemelli

Si è notato che nella successione dei numeri primi si incontrano molto frequentemente coppie di numeri che differiscono di 2, ad esempio:

11 – 13, 17 – 19, 29 – 31, etc.

Queste coppie di numeri vengono chiamati *gemelli*.
Si ipotizza che i numeri gemelli siano infiniti, benché questa congettura non sia stata ancora dimostrata.
Sono state fatte ricerche in questa direzione per trovare numeri gemelli sempre più grandi e si è giunti a trovare numeri di molte migliaia di cifre. L'attuale record è dato dalla coppia:

$$2.003.663.613 \times 2^{195000} \pm 1$$

che sono numeri di 58.711 cifre ed è stato trovato nel gennaio 2007.

Numeri primi in progressione aritmetica

Ovviamente ci si domanda se esistono numeri trigemini, ovvero se esistono tre numeri primi consecutivi che differiscono di 2.
Si può affermare che l'unica terna di numeri è:

3 – 5 – 7.

Infatti qualunque terna di numeri dispari consecutivi, deve contenere al suo interno un numero divisibile per 3, e quindi non primo.
Se si consulta la sequenza di numeri primi si incontrano numeri primi consecutivi equidistanti, ovvero in progressione aritmetica.
Si incontrano le seguenti terzine:

47 – 53 – 59 con ragione R = 6,
151 – 157 – 163 con ragione R = 6,
199 – 211 – 223 con ragione R = 12,

e quindi una quartina

251 – 257 – 263 – 269 con ragione R = 6,

e poi ancora terzine e quartine con ragione uguale a 6, ed ancora una terzina:

16763 – 16787 – 16811 con ragione R = 24.

Nasce spontanea la domanda se esistono sequenze di nu-meri primi consecutivi di qualsivoglia lunghezza e con qualsivoglia ragione.
La ragione R della progressione aritmetica formata da numeri primi consecutivi non può assumere qualunque valore.
In primo luogo R non può essere un numero dispari in quanto ciò implicherebbe che tale progressione contenga un numero pari che essendo divisibile per 2 non è primo.
Analogamente si dimostra che R non può essere mai 4, in quanto in qualunque sequenza di tre numeri con R = 4, uno di essi è divisibile per 3 e quindi non è primo.
In definitiva si dimostra che la ragione *R* della progressione aritmetica formata da *m* numeri primi consecutivi può assumere soltanto questi valori:

$$R = k\ m\#\ \ (k = 1, 2, 3, ...),$$

dove il simbolo # che segue il numero *m* indica il prodotto dei numeri primi minori o uguali a *m*, chiamato *primoriale* di *m*, ovvero:

m# = *primorial* di m,

si ha pertanto:

2# = 2; 3# = 2 x 3 = 6; 4# = 2 x 3 = 6; 5# = 2 x 3 x 5 = 30; 6# = 2 x 3 x 5 = 30; 7# = 2 x 3 x 5 x 7 = 210; etc... .
Pertanto si possono avere terzine (m = 3) con ragione:

$$R = k \times 3\# = k \times 6,\ \text{con}\ k = 1, 2, 3, 4, ...$$

ovvero: $R_1 = 6$, $R_2 = 12$, $R_3 = 18$, $R_4 = 24$, ...
Analogamente si possono avere quartine (m = 4) con:

$$R_1 = 6,\ R_2 = 12,\ R_3 = 18, ...$$

Invece per le cinquine di primi consecutivi in progressio-ne aritmetica, la ragione può avere i seguenti valori:

$$R_1 = 30,\ R_2 = 60,\ R_3 = 90,\ R_4 = 120, ...$$

Analogamente si possono avere sei numeri primi consecutivi in progressione aritmetica, con ragione:

$$R_1 = 30,\ R_2 = 60,\ R_3 = 90,\ R_4 = 120, ...$$

Per le sequenze di 7, 8, 9 e 10 numeri, essendo:

$$7\# = 8\# = 9\# = 10\# = 2 \times 3 \times 5 \times 7 = 210,$$

la ragione può avere i valori:

$$R_1 = 210,\ R_2 = 420,\ R_3 = 630, ...$$

Per le sequenze di 11 e 12 numeri, essendo:

$$11\# = 12\# = 2 \times 3 \times 4 \times 5 \times 7 \times 11 = 2310,$$

la ragione può avere i valori:

$$R_1 = 2310,\ R_2 = 4620,\ R_3 = 6930, ...$$

Terzine - Sono stati esaminati i numeri primi sino a 10^9 e sono state contate circa un milione di terzine delle quali si trascrivono qui di seguito le prime per ciascuna ragione ed il loro numero:

47 –	53 –	59	(R = 6)	595 279
199 –	211 –	223	(R = 12)	330 221
21 893 –	21 911 –	21 929	(R = 18)	181 903
16 763 –	16 787 –	16 811	(R = 24)	90 678
69 593 –	69 623 –	69 653	(R = 30)	84 523
255 767 –	255 803 –	255 839	(R = 36)	9 444
247 099 –	247 141 –	247 183	(R = 42)	15 333
3 565 931 –	3 565 979 –	3 566 027	(R = 48)	899
6 314 393 –	6 314 447 –	6 314 501	(R = 54)	2 577
4 911 251 –	4 911 311 –	4 911 371	(R = 60)	2 329
12 012 677 –	12 012 743 –	12 012 809	(R = 66)	643
23 346 737 –	23 346 809 –	23 346 881	(R = 72)	233

È stata trovata da Fougeron nel 2002 una terzina di 2409 cifre con ragione R = 30 e nel 2000 da Rosenthal, Jobling e Forbes una terzina di 1545 cifre con R = 2682.

Quartine - Sino a 10^9 sono state trovate numerose quartine di cui si riportano le prime per ciascuna ragione:

251 –	257 –	263 –	269	(R = 6)
111 497 –	111 509 –	111 521 –	111 533	(R = 12)
74 453 –	74 471 –	74 489 –	74 507	(R = 18)
1 397 609 –	1 397 633 –	1 397 657 –	1 397 681	(R = 24)
642 427 –	642 457 –	642 487 –	642 517	(R = 30)
321 191 –	5 321 227 –	5 321 263 –	5 321 299	(R = 36)
23 921 257 –	23 921 299 –	23 921 341 –	23 921 383	(R = 42)
55 410 683 –	55 410 731 –	55 410 779 –	55 410 827	(R = 48)
400 948 369 –	400 948 423 –	400 948 477 –	400 948 531	(R = 54)
253 444 777 –	253 444 837 –	253 444 897 –	253 444 957	(R = 60)
491 525 857 –	491 525 929 –	491 526 001 –	491 526 073	(R = 72)

È stata trovata una quartina di 1004 cifre da Fougeron nel 2000, avente ragione R = 396 (= 66 x 6).

Cinquine - Sino a 10^9 sono state trovate otto cinquine, tutte con ragione R = 30:

9 843 019 + 30 k
37 772 429 + 30 k
53 868 649 + 30 k
71 427 757 + 30 k
78 364 549 + 30 k
79 080 577 + 30 k
98 150 021 + 30 k
99 591 433 + 30 k

per k = 0, 1, 2, 3, 4.

Sestine - Sino a 10^9 esiste una sola sestina con R = 30, trovata nel 1967 da Lander & Parkin:

121 174 811 + 30 k (k = 0, 1, 2, 3, 4, 5).

Si riportano qui di seguito le sestine trovate nell'intervallo da 10^9 a 4 x 10^9, tutte con ragione R = 30:

1 128 318 991 + 30 k
2 201 579 179 + 30 k
2 715 239 543 + 30 k
2 840 465 567 + 30 k
3 510 848 161 + 30 k
3 688 067 693 + 30 k
3 893 783 651 + 30 k

per k = 0, 1, 2, 3, 4, 5.

Sequenze di 7, 8, 9 e 10 numeri primi - Dal 1995 al 1998 sono stati trovati sette, otto, nove ed infine dieci numeri primi consecutivi in progressione aritmetica, tutti con R = 210, i numeri trovati sono i seguenti:

- Sequenza di 7 numeri primi di 97 cifre
  1 089 533 431 247 059 310 875 780 378 922 957 732\ 908 036 492 993 138 195 385 213 105 561 742 150 447 308 967 213 141 717 486 151 + 210 k,
  per k = 0, 1, 2, 3, 4, 5, 6
- Sequenza di 8 numeri primi di 92 cifre
  43 804 034 644 029 893 325 717 710 709 965 599 939\ 101 479 007 432 825 862 362 446 333 961 919 524 977 985 103 251 510+ 210 k,
  per k = 0, 1, 2, 3, 4, 5, 6, 7
- Sequenza di 9 numeri primi di 92 cifre
  99 679 432 066 701 086 484 490 653 695 853 561 638 982 364 080 991 618 395 774 048 585 529 071 475 461 114 799 677 694 651+ 210 k,
  per k = 0, 1, 2, 3, 4, 5, 6, 7, 8
- Sequenza di 10 numeri primi di 93 cifre
  100 996 972 469 714 247 637 786 655 587 969 840 329 509 324 689 190 041 803 603 417 758 904 341 703 348 882 159 067 229 719 + 210 k,
  per k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.

Non si pensa di poter trovare a breve tempo una sequenza di undici numeri primi consecutivi in quanto la ragione di tale successione ha un valore minimo di 2310.

Numeri *quasi-primi o semiprimi* - Si definiscono numeri *quasi-primi* i numeri prodotto di due primi > 2. Sono pertanto numeri quasi-primi:

9 - 15 - 21 - 25 - 33 - 35 - 39 - ...

rispettivamente uguali a:

3x3 - 3x5 - 3x7 - 5x5 - 3x11 - 5x7 - 3x13 - ...

I numeri quasi-primi si incontrano la prima volta nell'enunciato di una proposizione riguardante la congettura di Goldbach.

Alcuni Autori definiscono numeri quasi-primi o semiprimi il prodotto di due primi ≥ 2.
I numeri quasi-primi rivestono oggi una importanza strategica notevolissima per la scelta della chiave per l'algoritmo RSA di crittografia a chiave pubblica.
Vengono infatti offerti sostanziosi premi in denaro per chi riesce a fattorizzare i numeri conosciuti come **numeri RSA** che sono numeri quasi-primi sino a 617 cifre decimali.
Tale numero è chiamato RSA-617, oppure RSA-2048 (2048 cifre binarie secondo la più recente convenzione) ed è un numero quasi-primo; per la sua scomposizione in fattori viene offerta una cifra di 200.000 Dollari USA, modesta se posta in confronto a premi più grandi per la risoluzione di altri problemi.
Si riporta qui di seguito il più grande numero RSA sinora fattorizzato RSA 200 seguito dai due fattori nel quale è stato scomposto ed ancora il già citato numero RSA -617 ancora da fattorizzare.

RSA-200

RSA-617

Lo studio dei numeri quasi-primi può fornire la possibilità di estendere ad essi congetture paragonabili a quelle formulate per i numeri primi.
Si riportano nelle pagine seguenti l'elenco dei numeri quasi-primi sino a 10 000

Si sono qui esaminate proprietà dei numeri quasi-primi ipotizzate partendo da un campione molto modesto limitato ai numeri riportati nlle pagine precedenti..
Si osserva quanto segue:

- La frequenza sembra essere costante e oscillare intorno al valore 5.
- La ragione di numeri quasi-primi consecutivi sembra poter assumere indistintamente tutti i valori, ovviamente pari.
- Si incontrano, nella pur piccola sequenza presa in esame, sino a 8 numeri quasi-primi consecutivi in progressione aritmetica; nello stesso intervallo di primi consecutivi se ne incontrano soltanto 4.

Numeri *quasi-primi* in progressione aritmetica

Si riportano qui di seguito le sequenze di numeri quasi-primi, le prime per ciascuna ragione, e trascrivendo soltanto il primo numero di ciascuna sequenza.

-

Terzine: 91 - ... (R = 2)
11 - ... (R = 4)
9 - . (R = 6)
69 - ... (R = 8)
417 - ... (R = 10)
4915 - ... (R = 12)
1991 - ... (R = 14)
5855 - ... (R = 18)

- **Quartine:** 299 - ... (R = 2)
1191 - ... (R = 4)
1739 - ... (R = 6)
4955 - ... (R = 8)
7519 - ... (R = 12)

- **Cinquine:** 213 - ... (R = 2)
3031 - ... (R = 4)
5287 - ... (R = 6)

- **:Sestine:** 1383 - ... (R = 2)
1457 - ... (R = 4)

- **Settine:** 3091 - ... (R = 2)
481 - ... (R = 4)

- **Ottine:** 8129 - ... (R = 2)

BBLIOGRAFIA

1. H. DUBNER, T. FORBES, N. LYGEROS, M. MIZONY, H. NELSON, and P. ZIMMERMAN, *Ten consecutive primes in arithmetic progression*, Math. Comp., (1998).
2. H. DUBNER and H. NELSON, *Seven consecutive primes in arithmetic progression*, Math. Comp., 66 (1997) 1743-1749.
3. R. K. GUY, *Unsolved problems in number theory*, Springer-Verlag, New York, NY, 1994.
4. L. J. LANDER and T. R. PARKIN, *Consecutive primes in arithmetic progression*, Math. Comp., 21 (1967) 489.
5. E. GROSSWLD, *Arithmetic progressions that consist only of primes*, J. Number Theory, 14 (1982) 9-31.
6. H. E. ROSE, *A course in number theory*, second edition, Clarendon Press, Oxford, 1994.