9 Marzo 2011

Il mistero dei numeri primi

Andrea Loi

webpage: loi.sc.unica.it $\rightarrow$ didattica $\rightarrow$ seminari $\rightarrow$ il mistero dei numeri primi

Euclide ($\sim$ 367 a.C. - $\sim$ 283 a.C.)

Definizioni di numero primo 

Un numero composto è un intero positivo $n \geq 2$ che può essere fattorizzato come prodotto di due interi positivi

$$n = ab \quad \text{dove} \quad a < n \quad \text{e} \quad b < n$$

Un numero primo è un intero positivo $p \geq 2$ che non è composto ossia non può essere fattorizzato come prodotto di due interi positivi ognuno dei quali sia minore di p.

Equivalentemente un numero $p \geq 2$ è primo se può essere diviso **SOLO** per se stesso o per 1.

Qualche esempio

$$6 = 2 \times 3 \quad 17 = 1 \times 17 \quad 55 = 5 \times 11 \quad 101 = 1 \times 101$$

$$30 = 2 \times 3 \times 5 = 2 \times 15 = 5 \times 6 = 3 \times 10$$

Ogni intero è prodotto di primi

Proposizione. Ogni intero $n \geq 2$ o è primo o può essere scritto come prodotto di numeri primi.

dimostrazione. Sia $N \geq 2$ il più piccolo intero positivo che non è primo o non può essere scritto come prodotto di numeri primi $\Rightarrow N = ab,\ a < N,\ b < N \Rightarrow$

$$a = p_1 \dots p_L \qquad\qquad b = q_1 \dots q_M$$

$$\Downarrow \quad \Downarrow \quad \Downarrow$$

$$N = ab = p_1 \dots p_L\ q_1 \dots q_M$$

in contrasto col fatto che N non può essere scritto come prodotto di numeri primi. $\square$

Il Teorema fondamentale dell'aritmetica 

Teorema. (Elementi di Euclide, Libro IX) Ogni intero positivo $n \geq 2$ può essere scritto come prodotto di numeri primi elevati potenze positive:

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \dots p_M^{e_M}.$$

Se inoltre scegliamo $p_1 < p_2 < p_3 < \cdots < p_M$ allora la fattorizzazione è unica.

Esempio. $n = 12 = 2^2 \times 3$, $p_1 = 2$, $p_2 = 3$ $e_1 = 2$, $e_2 = 1$.

Infinità dei numeri primi 

Teorema.(Elementi di Euclide, Libro IX, Proposizione 20) I numeri primi sono infiniti.

dimostrazione. Supponiamo che $p_1, p_2, p_3, \ldots, p_N$ sia una lista completa di numeri primi. Consideriamo l'intero positivo

$$Q_N = p_1 p_2 p_3 \ldots p_N + 1$$ **COLPO DI GENIO!!**

Il numero Q_N non è divisibile per nessuno dei primi della lista $p_1, p_2, p_3, \ldots, p_N$. D'altra parte la proposizione precedente ci diceva che Q_N è divisibile da qualche numero primo. Quindi $p_1, p_2, p_3, \ldots, p_N$ non può essere una lista completa di numeri primi. $\square$

Considerazioni sul numero $Q_N = p_1 p_2 p_3 \dots p_N + 1$

$Q_1 = 2 + 1 = 3$ (primo)

$Q_2 = 2 \cdot 3 + 1 = 7$ (primo)

$Q_3 = 2 \cdot 3 \cdot 5 + 1 = 31$ (primo)

$Q_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$ (primo)

$Q_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$ (primo)

$Q_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$ (composto)

$Q_7 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510511 = 19 \cdot 97 \cdot 277$ (composto).

Problema aperto: Non si sa se i numeri primi della forma Q_N siano infiniti.

Eratostene (Cirene, 276 a.C.- Alessandria d'Egitto, 194 a.C.)

Crivello di Eratostene

Si eliminano tutti i multipli di 2 (tranne 2)

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ 9 ~~10~~ 11 ~~12~~ 13 ~~14~~ 15 ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23
~~24~~ 25 ~~26~~ 27 ~~28~~ 29 ~~30~~ 31 ~~32~~ 33 ~~34~~ 35 ~~36~~37 ~~38~~ 39 ~~40~~ 41 ~~42~~ 43
~~44~~ 45 ~~46~~ 47 ~~48~~ 49 ~~50~~ 51 ~~52~~ 53 ~~54~~ 55 ~~56~~ 57 ~~58~~ 59 ~~60~~ 61 ~~62~~ 63
~~64~~ 65 ~~66~~ 67 ~~68~~ 69 ~~70~~ 71 ~~72~~ 73 ~~74~~ 75 ~~76~~ 77 ~~78~~ 79 ~~80~~ 81 ~~82~~ 83
~~84~~ 85 ~~86~~ 87 ~~88~~ 89 ~~90~~ 91 ~~92~~ 93 ~~94~~ 95 ~~96~~ 97 ~~98~~ 99 ~~100~~

Crivello di Eratostene

Poi si eliminano tutti i multipli di 3 (tranne 3)

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23
~~24~~ 25 ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ 35 ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43
~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ 49 ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ 55 ~~56~~ ~~57~~~~58~~ 59 ~~60~~ 61 ~~62~~ ~~63~~
~~64~~ 65 ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ 77 ~~78~~ 79 ~~80~~ ~~81~~ ~~82~~ 83
~~84~~ 85 ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~ 91 ~~92~~ ~~93~~ ~~94~~ 95 ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

Crivello di Eratostene

Poi si eliminano tutti i multipli di 5 (tranne 5)

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23
~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43
~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ 49 ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~5758~~ 59 ~~60~~ 61 ~~62~~ ~~63~~
~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ 77 ~~78~~ 79 ~~80~~ ~~81~~ ~~82~~ 83
~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~ 91 ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

Crivello di Eratostene

Infine si eliminano tutti i multipli di 7 (tranne 7)

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23
~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43
~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~~~58~~ 59 ~~60~~ 61 ~~62~~ ~~63~~
~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ 79 ~~80~~ ~~81~~ ~~82~~ 83
~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~ ~~91~~ ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

Crivello di Eratostene

I numeri restanti sono i numeri primi da 1 a 100.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~
~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~
~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~ 47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~
~~57~~~~58~~ 59 ~~60~~ 61 ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73
~~74~~ ~~75~~ ~~76~~ ~~77~~ ~~78~~ 79 ~~80~~ ~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~ ~~91~~
~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

I numeri primi da 1 a 1000

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79
83 89 97 101 103 107 109 113 127 131 137 139 149 151 157
163 167 173 179 181 191 193 197 199 211 223 227 229 233
239 241 251 257 263 269 271 277 281 283 293 307 311 313
317 331 337 347 349 353 359 367 373 379 383 389 397 401
409 419 421 431 433 439 443 449 457 461 463 467 479 487
491 499 503 509 521 523 541 547 557 563 569 571 577 587
593 599 601 607 613 617 619 631 641 643 647 653 659 661
673 677 683 691 701 709 719 727 733 739 743 751 757 761
769 773 787 797 809 811 821 823 827 829 839 853 857 859
863 877 881 883 887 907 911 919 929 937 941 947 953 967
971 977 983 991 997

Un tentativo per capire come sono distribuiti i numeri primi

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38
39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56
5758 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73
74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91
92 93 94 95 96 97 98 99 100

Ci sono 5 numeri primi, 2, 3, 5, 7, 11, da 2 a 11, esattamente la metà; tra i successivi dieci da 12 a 21, ci sono 3 numeri primi, 13, 17, 19, cioè il 30% ; tra 22 e 31, ci sono ancora 3 numeri primi, 23, 29, 31, cioè ancora il 30% ; mentre tra 32 e 41, ci sono 2 numeri primi, 37, 41, cioè il 20%; e così tra 42 e 51. Sembra che il calcolo si stabilizzi a circa il 20% .....

....ma non è così

9.999.901 9.999.902 9.999.903 9.999.904 9.999.905 9.999.906 9.999.907
9.999.908 9.999.909 9.999.910 9.999.911 9.999.912 9.999.913 9.999.914
9.999.915 9.999.916 9.999.917 9.999.918 9.999.919 9.999.920 9.999.921
9.999.922 9.999.923 9.999.924 9.999.925 9.999.926 9.999.927 9.999.928
9.999.929 9.999.930 9.999.931 9.999.930 9.999.931 9.999.932 9.999.933
9.999.934 9.999.935 9.999.936 9.999.937 9.999.938 9.999.939 9.999.940
9.999.941 9.999.942 9.999.943 9.999.944 9.999.945 9.999.946 9.999.947
9.999.948 9.999.949 9.999.950 9.999.951 9.999.952 9.999.953 9.999.954
9.999.955 9.999.956 9.999.957 9.999.958 9.999.959 9.999.960 9.999.961
9.999.962 9.999.963 9.999.964 9.999.965 9.999.966 9.999.967 9.999.968
9.999.969 9.999.970 9.999.971 9.999.972 9.999.973 9.999.974 9.999.975
9.999.976 9.999.977 9.999.970 9.999.971 9.999.972 9.999.973 9.999.974
9.999.975 9.999.976 9.999.977 9.999.978 9.999.979 9.999.980 9.999.981
9.999.982 9.999.983 9.999.984 9.999.985 9.999.986 9.999.987 9.999.988
9.999.989 9.999.990 9.999.991 9.999.992 9.999.993 9.999.994 9.999.995
9.999.996 9.999.997 9.999.998 9.999.999 10.000.000

....ma non è così

10.000.000 10.000.001 10.000.002 10.000.003 10.000.004 10.000.005 10.000.006
10.000.007 10.000.008 10.000.009 10.000.010 10.000.011 10.000.012 10.000.013
10.000.014 10.000.015 10.000.016 10.000.017 10.000.018 10.000.019 10.000.020
10.000.021 10.000.022 10.000.023 10.000.024 10.000.025 10.000.026 10.000.027
10.000.028 10.000.029 10.000.030 10.000.031 10.000.032 10.000.033 10.000.034
10.000.035 10.000.036 10.000.037 10.000.038 10.000.039 10.000.040 10.000.041
10.000.042 10.000.043 10.000.044 10.000.045 10.000.046 10.000.047 10.000.048
10.000.049 10.000.050 10.000.051 10.000.052 10.000.053 10.000.054 10.000.055
10.000.056 10.000.057 10.000.058 10.000.059 10.000.060 10.000.061 10.000.062
10.000.063 10.000.064 10.000.065 10.000.066 10.000.067 10.000.068 10.000.069
10.000.070 10.000.071 10.000.072 10.000.073 10.000.074 10.000.075 10.000.076
10.000.077 10.000.078 10.000.079 10.000.080 10.000.081 10.000.082 10.000.083
10.000.084 10.000.085 10.000.086 10.000.087 10.000.088 10.000.089 10.000.090
10.000.091 10.000.092 10.000.093 10.000.094 10.000.095 10.000.096 10.000.097
10.000.098 10.000.099 10.000.100

Ancora peggio (o meglio?!)

Esistono intervalli di numeri naturali, di ampiezza arbitraria, all'interno dei quali non si incontra alcun numero primo!!!!

Il prodotto dei numeri naturali da 1 a n, si indica con il simbolo n! (da leggersi n fattoriale), cioè:

$n! = n \cdot (n–1) \cdot (n–2) \cdot (n–3) \cdot .... \cdot 3 \cdot 2 \cdot 1$

Esempi

$2! = 2 \cdot 1 = 2$

$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$

$10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

Il numero

$n! = n \cdot (n–1) \cdot (n–2) \cdot (n–3) \cdot .... \cdot 3 \cdot 2 \cdot 1$

è divisibile per ciascuno dei numeri tra 1 e n; n!+2 è divisibile per 2, ; n!+3 è divisibile per 3; ... n!+n è divisibile per n. Abbiamo così trovato un intervallo di numeri naturali consecutivi

$$n! + 2,\ n! + 3,\ \cdots,\ n! + n$$

e nessuno di essi primo.

Esercizio. **Costruire 1000 numeri consecutivi nessuno dei quali sia primo.**

Problema aperto. **Non si sa se esistono infiniti numeri primi della forma** $n! \pm 1$

Pierre de Fermat (1601-1665)

Numeri primi di Fermat

Fermat pensava di aver trovato una formula che producesse solo numeri primi:

$$\mathbf{F_n = 2^{2^n} + 1}$$

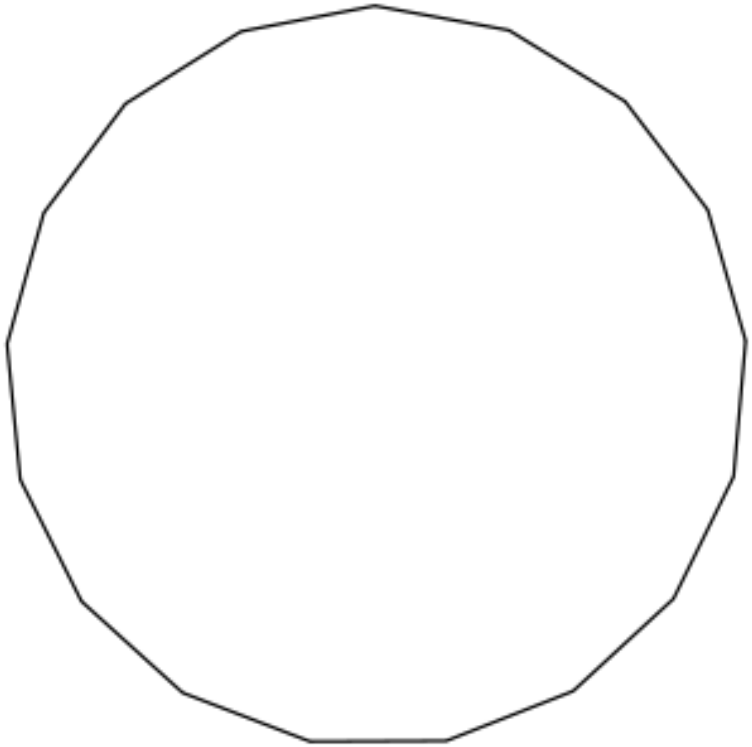
ennesimo numero di Fermat. Ma Fermat si sbagliava. Infatti $F_1 = 2^{2^1} + 1 = 5$, $F_2 = 2^{2^2} + 1 = 17$, $F_3 = 2^{2^3} + 1 = 257$, $F_4 = 2^{2^4} + 1 = 65537$ che sono primi.

Ma $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$ NON è primo (fattorizzazione dovuta a Eulero nel 1732).

Curiosità sui numeri primi di Fermat

1. Non sono stati trovati altri numeri primi della forma F_n per $n > 4$.

2. Carl Friedrich Gauss (1777-1855) riuscì a dimostrare che se F_n è primo, allora è possibile costruire geometricamente con riga e compasso, un poligono regolare di F_n lati. Fu così che all'età di 19 anni Gauss costruì un poligono regolare di 17 lati.



Un eptadecagono regolare

Marin Mersenne (Oizé, 8 settembre 1588 – Parigi, 1 settembre 1648)

Numeri di Mersenne 

Un numero di Mersenne è un numero della forma:

$$\mathbf{M_n = 2^n - 1}$$

con n intero positivo.

Numeri di Mersenne 

Ecco una lista dei numeri di Mersenne per alcuni numeri primi.

$M_2 = 2^2 - 1 = 3 \qquad M_3 = 2^3 - 1 = 7 \quad M_5 = 2^5 - 1 = 31$

$M_7 = 2^7 - 1 = 127 \quad M_{11} = 2^{11} - 1 = 2047 \quad M_{13} = 2^{13} - 1 = 8191$

$M_{17} = 131071 \quad M_{19} = 524287 \quad M_{31} = 2147483647$

$M_{61} = 2305843009213693951$

Numeri di Mersenne 

Fatto importante: Se M_n è primo allora anche n è primo, ma non è vero il viceversa (es. $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$)

Curiosità: Il più grande numero primo che si conosce (cioè che si riesce a scrivere) è un numero primo di Mersenne:

$$M_{43112609} = 2^{43112609} - 1$$

un numero di 1.209.780.189 cifre.

Leonhard Euler (Basilea, 15 aprile 1707 – San Pietroburgo, 18 settembre 1783)

Numeri di Eulero 

$\mathbf{E_n = n^2 + n + 41}$

produce solo numeri primi per n che varia da 0 e 39: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

Ma, per n=40, il numero che si ottiene non è primo, infatti:

$$40^2 + 40 + 41 = 40(40 + 1) + (40 + 1) = (40 + 1)(40 + 1)$$

Eulero scoprì che si poteva scegliere anche a=2, 3, 5, 11, 17 perché la formula $n^2 + n + a$ producesse numeri primi per ogni valore di n compreso fra 0 e a–2.

Somma di due quadrati e numeri primi

Per quali interi positivi N esistono interi positivi x e y tali che

$$x^2 + y^2 = N?$$

Esempio.

Il numero $N = 943451654345749038297 6$ può essere scritto come somma di due quadrati?

Si fattorizza N in prodotto di primi:

$$N = 943451654345749038297 6 = 2^7\ 3^4\ 13^3\ 23^2\ 61\ 97^2\ 1364161$$

Si considerano i primi nella fattorizzazione di N che hanno resto tre divisi per quattro. In questo caso 3 e 23 (mentre tutti gli altri primi danno resto uno divisi per quattro).

$$N = 943451654345749038297 6 = 2^7\ 3^4\ 13^3\ 23^2\ 61\ 97^2\ 1364161$$

Se l'esponente di questi primi è pari allora il numero si potrà scrivere come somma di due quadrati. In questo caso gli esponenti di 3 e 23 sono pari (4 e 2 rispettivamente) e quindi N è la somma di due quadrati:

$$N = 943451654345749038297 6 = 1117195560^2 + 97125014376^2$$

Esercizio. **Costruire un numero con più di un milione di cifre che non possa essere scritto come somma di due quadrati.**

La funzione ζ (zeta) di Eulero

Sia $1 < x$. Allora

$$\zeta(x) \stackrel{def}{=} 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \frac{1}{9^x} + \cdots =$$

$$= (1 + \frac{1}{2^x} + \frac{1}{2^{2x}} + \frac{1}{2^{3x}} + \frac{1}{2^{4x}} + \cdots)\ (1 + \frac{1}{3^x} + \frac{1}{3^{2x}} + \frac{1}{3^{3x}} + \frac{1}{3^{4x}} + \cdots)$$

$$(1 + \frac{1}{5^x} + \frac{1}{5^{2x}} + \frac{1}{5^{3x}} + \frac{1}{5^{4x}} + \cdots)\ (1 + \frac{1}{7^x} + \frac{1}{7^{2x}} + \frac{1}{7^{3x}} + \frac{1}{7^{4x}} + \cdots)$$

$$(1 + \frac{1}{11^x} + \frac{1}{11^{2x}} + \frac{1}{11^{3x}} + \frac{1}{11^{4x}} + \cdots)\ (1 + \frac{1}{13^x} + \frac{1}{13^{2x}} + \frac{1}{13^{3x}} + \frac{1}{13^{4x}} + \cdots) \cdots$$

Possiamo anche scrivere

$$\zeta(x) = \sum_{n=0}^{+\infty} \frac{1}{n^x} = \prod_{p \text{ primo}} (1 - p^{-x})^{-1}, \ 1 < x$$

Un'altra dimostrazione che i numeri primi sono infiniti

Eulero usò la sua formula per dimostrare che

$$\sum_{p \text{ primo}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} \cdots = +\infty$$

Osserviamo che

$$\sum_{n=1}^{+\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \cdots = +\infty$$

Mentre, per esempio,

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \frac{1}{25} + \cdots = \frac{\pi^2}{6}$$

Alcuni problemi aperti sui numeri primi

1. NON SI SA se un numero pari maggiore di 2 possa essere scritto come somma di due numeri primi (**congettura binaria di Goldbach (1690-1764)**).

2. NON SI SA se un numero dispari maggiore di 5 possa essere scritto come somma di tre numeri primi (**congettura ternaria di Goldbach**).

3. NON SI SA se esistono infiniti numeri primi della forma n^2+1.

4. NON SI SA se esiste sempre un numero primo tra n^2 e $(n+1)^2$ (il fatto che esista un numero primo tra n e $2n$ è stato dimostrato da Chebyshev (congettura di Bertrand).

5. NON SI SA se la successione di **Fibonacci**

$$F_0 = F_1 = 1, F_n = F_{n-1} + F_{n-2},\ n > 1$$

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55 \ldots$$

contrnga un numero infinito di numeri primi. Osserviamo che $F_{19} = 4.181 = 113 \times 37$ non è primo nonostante 19 lo sia.

6. NON SI SA se esistano infiniti numeri primi gemelli. Due numeri primi sono detti **gemelli** se la loro distanza è due (es. 17 e 19 sono primi gemelli).

Curiosità. I numeri primi gemelli più grandi che si conoscono sono:

$(2003663613)2^{2195000} - 1$ e $(2003663613)2^{2195000} + 1$

Carl Friedrich Gauss (Braunschweig, 30 aprile 1777 – Gottinga, 23 febbraio 1855)

La svolta di Gauss

Gauss definì la funzione che a $x \in \mathbb{R}$ associa

$$\pi(x) = \{\text{numero dei numeri primi minori} \quad \leq x\}.$$

Domande fondamentali: Quale è una buona approssimazione di $\pi(x)$?

$\pi(x) = \{\text{numero dei primi} \leq x\}$	$\frac{x}{\pi(x)}$
$\pi(10) = 4$	$\frac{10}{4} = 2,5$
$\pi(100) = 25$	$\frac{100}{25} = 4$
$\pi(1000) = 168$	$\frac{1000}{168} = 6$
$\pi(10.000) = 1229$	$\frac{10.000}{1229} = 8,1$
$\pi(100.000) = 9592$	$\frac{100.000}{9592} = 10,4$
$\pi(1.000.000) = 78498$	$\frac{1.000.000}{78498} = 12,7$

COLPO DI GENIO!! Gauss notò che ogni volta si moltiplica x per 10, si aggiunge 2,3 al rapporto $\frac{x}{\pi(x)}$, almeno per x abbastanza grande. Proprio questo legame tra moltiplicazione e addizione (che è la relazione racchiusa in un logaritmo), e il fatto che 2,3 è approssimativamente il valore rappresentato da $\ln 10$, portarono Gauss a ipotizzare che

$$\frac{x}{\pi(x)} \approx \ln x.$$

Da cui

$$\pi(x) \approx \frac{x}{\ln x} \quad \Longleftrightarrow \quad \lim_{x \to +\infty} \pi(x) \, \frac{\ln x}{x} = 1$$

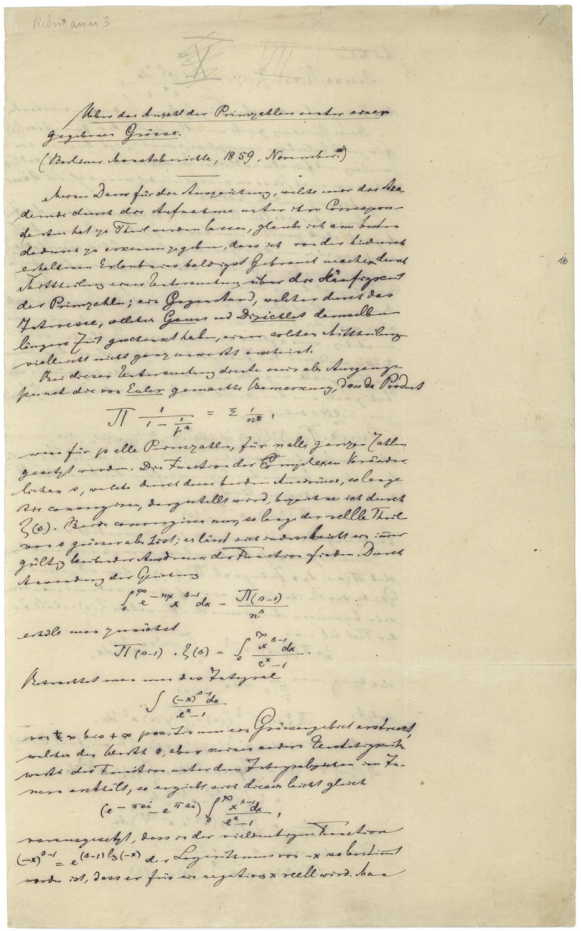
Questa congettura si rivelò poi vera, e oggi è nota come **Teorema dei numeri primi (Hadamard, de la Vallée Poussin, 1896)**.

Domanda: Si può stimare

$$|\pi(x) - \frac{x}{\ln x}|?$$

Risposta (vaga): La stima dipende dalla conoscenza degli zeri della funzione ζ (zeta) introdotta da Riemann nel 1859.

Georg Friedrich Bernhard Riemann (1826 -1866)



Il lavoro di Riemann (in soldoni)

Primo passo (numeri complessi) Quale è la radice quadrata di -1? In matematica si introduce un numero (chiamato unità immaginaria) tale che $i^2 = -1$. Un numero complesso è un numero della forma $a + ib$ con a e b numeri reali.

Il lavoro di Riemann (in soldoni)

Secondo passo (funzioni con i numeri complessi) La maggior parte di voi conosce le funzioni reali $y = f(x)$. Per ogni numero reale x si ottiene un numero reale $f(x)$

Esempio $f(x) = x^2$, $f(x) = \ln x$.

Non c'è niente che impedisca di considerare numeri complessi x.

Esempio $f(x) = x^2$ allora $f(i) = -1$.

Il lavoro di Riemann (in soldoni)

Terzo passo (la funzione ζ di Riemann) La funzione ζ di Riemann è una funzione che ad ogni numero complesso $a + ib$ associa il numero complesso $\zeta(a + ib)$ ed è costruita a partire dalla funzione $\zeta(x) = \sum_{n=0}^{+\infty} \frac{1}{n^x}$ di Eulero.

Il lavoro di Riemann (in soldoni)

Quarto passo (zeri della funzione ζ): uno zero di una funzione complessa è un punto $a+ib$ dove $f(a+ib)=0$.

Esempio. $f(x)=x^2+x$ gli zeri sono $x=0$ e $x=-1$. Infatti $f(0)=0$ e $f(-1)=0$.

Riemann dimostra che per la ζ ci sono due tipi di zeri: gli zeri banali $x=-2$, $x=-4$, $x=-6$,... e gli zeri non banali che sono tutti gli altri.

Il lavoro di Riemann (in soldoni)

Riemann riuscì a calcolare alcunii zeri non banali non banali della funzione ζ e verificò che erano della forma $\frac{1}{2} + ib$. Nel 1859 egli congetturò che questo fosse vero per tutti gli zeri non banali (questa congettura va sotto il nome di **Ipotesi di Riemann**.

Tutti i punti della forma $\frac{1}{2} + iy$ al variare di y costituiscono una retta nel piano complesso, la cosidetta retta critica.

Quindi l'ipotesi di Riemann si può anche formulare dicendo che **tutti gli zeri non banali della funzione ζ giaciono sulla retta critica.**

Perchè l'ipotesi di Riemann è importante? Più gli zeri della funzione ζ sono tutti sulla retta critica più i numeri primi sono regolari. Con un'analogia statistica: se il teorema dei numeri primi ci dice qualcosa sulla distribuzione media dei numeri primi l'ipotesi di Riemann ci dice qualcosa circa la deviazione dalla media.

Godfrey Harold Hardy (7 February 1877–1 December 1947)

Oggi

Al momento sono stati calcolati circa 1.5 billioni di zeri (un bilione $=10^{12}$) con i computers e stanno tutti sulla retta critica.

L'ipotesi di Riemann è stato uno dei 23 problemi proposti da Hilbert all'inizio del 1900 (l'ottavo). E' anche uno dei 7 Clay Millennium Prize Problems (2000).

Numeri primi e crittografia

Osservazione. Dato un numero intero positivo n molto grande è molto difficile trovare una sua fattorizzazione esplicita! Per esempio se n è il prodotto di due numeri primi con almeno cento cifre allora occorrerebbero secoli di calcoli su computer ultraveloci per fattorizzare n.

Quest'osservazione è alla base dell'algoritmo RSA (Rivest, Shamir, Adleman) di crittografia.

Bibliografia

1. Marcus du Sautoy, *The music of primes*, Fourth Estate 2003 (tradotto in italiano come *l'enigma dei numeri primi*).

2. Oliver Sacks, *L'uomo che scambiò sua moglie per un cappello*, Milano, Adelphi, 2008.

3. Paolo Giordano, *La solitudine dei numeri primi*, Mondadori, 2008.

Grazie per l'attenzione!!!

Buon proseguimento di 2011

$2011 = 157+163+167+173+179+181+191+193+197+199+211$