Formule per i numeri primi

A. Bernardi

13 aprile 2016

Il Teorema di Wilson permette di scrivere una "formula" per l'n-esimo numero primo, ed una formula esatta per $\pi(x)$. Purtroppo, però queste formule non sono utilizzabili nella pratica.

Osservazione. Se $k \geq 6$ non è primo allora $k \mid (k-2)!$, mentre per il Teorema di Wilson, se p è primo allora $(p-2)! \equiv 1 \pmod{p}$. Quindi, per $x \geq 3$, $\pi(x) = 2 + \sum_{5 \leq k \leq x} k \left\{ \frac{(k-2)!}{k} \right\}$, dove $\{x\}$ indica la parte frazionaria di x.

Definiamo:

$$f(x,y) := \begin{cases} 1 & \text{se } x > y, \\ 0 & \text{se } x \leq y \end{cases}$$

Lemma 0.1. *Sia p_n l'-ennesimo numero primo. Allora*

$$p_n = 1 + \sum_{d=1}^{2^{2^n}} f(n, \pi(d)).$$

Lemma 0.2. *Nessun polinomio in una variabile non costante può assumere solo valori primi, ma esistono polinomi in piú variabili che hanno questa proprietà.*

Dimostrazione. La prima parte in una sola variabile è facilmente reperibile in letteratura.

La seconda parte è più profonda e richiede un risultato di Y.V. Matiyasevich [2] (1970) (in russo) attualmente noto come il "Teorema di Matiyasevich–Robinson–Davis–Putnam" in quanto fortemente basato su dei risultati precedenti di questi ultimi che afferma che

> L'insieme dei numeri primi è diofanteo.

Un insieme S di interi positivi si dice diofanteo se e solo se esiste un polinomio $Q \in \mathbb{Z}[x_1, \ldots, x_m]$ tale che $S = \{Q(x_1, \ldots, x_m) \geq 1 \mid x_1 \geq 1, \ldots, x_m \geq 1\}$ (cfr. [3, §3.III]). □

Teorema 0.3. *Se $f \in Z[x]$ assume valore primo per ogni intero, allora f è costante.*

Esempio 0.4 (Eulero)**.** Il polinomio $f(n) = n^2 - n + 41$ è primo per $n = 0, 1, \ldots, 40$, ma non è primo per $n = 41$.

Teorema 0.5 (Schur)**.** *Sia $f \in Z[x]$ un polinomio non costante. L'insieme $P_f := \{p : \exists\, n \in \mathbb{N}\, t.c.\, f(n) \neq 0\, e\, p \mid f(n)\}$ è infinito.*

Siano $S(P_f) = \{n \in \mathbb{N}^* : p \mid n \Rightarrow p \in P_f\}$ e $V(x) = [1, x] \cap S(P_f)$.

La cardinalità di $V(x)$ è uguale al numero di punti a coordinate intere nel triangolo delimitato dagli assi cartesiani (x_1, x_2) e dalla retta di equazione $x_1 \log 2 + x_2 \log 3 = \log x$. Assegniamo ad ogni punto $(a_1, a_2) \in \mathbb{N}^2$ che soddisfa questa diseguaglianza il quadrato di vertici opposti (a_1, a_2), $(a_1 + 1, a_2 + 1)$. Il numero di questi punti è uguale all'area del triangolo con un errore dell'ordine del perimetro del triangolo stesso, e quindi l'area vale $(\log x)2/(2 \log 2 \log 3) + O(\log x)$. (Cfr. [1, Cap. 5]).

Non è necessario conoscere $|V(x)|$ con precisione: è sufficiente osservare che da $\log m = \alpha_1 \log p_1 + \cdots + \alpha_k \log pk \leq \log x$ segue che $0 \leq \alpha_i \leq (\log x)/\log p_i$ e quindi $|V(x)| \leq \prod_i (2 + (\log x)/\log p_i) = O_{p_1,\ldots,p_k}(\log x)^k$. In altre parole, si può dire che il semigruppo moltiplicativo S generato dall'insieme di numeri primi P_f è poco denso e non riesce a coprire tutti i valori assunti da un polinomio.

Esempio 0.6. Sia $f(x) = qx + a$ con $a, q \in \mathbb{Z}$, e $q \neq 0$. Se $(a, q) = 1$ allora $P_f = \{p : p \nmid q\}$. Se $(a, q) > 1$, allora $P_f = \{p : p \nmid q\} \cup \{p : p \mid (a, q)\}$.

Teorema 0.7. *Esistono infiniti numeri primi in ciascuna delle progressioni aritmetiche* $4n + 1$ *e* $4n - 1$.

Fermat e Mersenne proposero "formule" che generano primi: purtroppo le loro congetture si sono rivelate sbagliate.

Se il numero $2m + 1$ è primo, allora $m = 2^n$ per qualche intero n.

Definizione 0.8. Per $n \in \mathbb{N}$ si chiama n-esimo numero di Fermat il numero $F_n := 2^{2^n} + 1$. Per $n \in \mathbb{N}^*$ si chiama n-esimo numero di Mersenne il numero $M_n := 2^n - 1$.

Se il numero M_n è primo, allora n è primo.

Fermat congetturò che tutti i numeri F_n fossero primi, ma questo è vero solo per $n = 0, \ldots, 4$, e falso per $n = 5, \ldots, 32$. Esistono criteri di primalità ad hoc per i numeri di Fermat che hanno permesso di dimostrare che i numeri F_n con $n = 5, \ldots, 32$ sono composti, nella maggior parte dei casi senza poterne esibire esplicitamente un fattore primo. Mersenne dette una lista di numeri primi p per i quali M_p è primo, ma questa lista contiene vari errori ed omissioni. Anche nel caso dei numeri di Mersenne esistono criteri di primalità speciali.

Riferimenti bibliografici

[1] G.H. Hardy, Ramanujan. Twelve lectures on subjects suggested by his life and works, third ed., Chelsea, New York, 1999.

[2] Y.V. Matiyasevich, Yuri V. (1970). [Enumerable sets are Diophantine]. Doklady Akademii Nauk SSSR (in Russian) 191: 279?282. MR 0258744. English translation in Soviet Mathematics 11 (2), pp. 354?357.

[3] P. Ribenboim, The New Book of Prime Numbers Records, Springer, New York, 1996.