UNIVERSITÀ DEGLI STUDI DI TRENTO

Dipartimento di Matematica

Corso di Laurea in Matematica

Tesi di Laurea

Formule per i numeri primi

Supervisore:
Prof.ssa Alessandra Bernardi

Laureanda:
Gabriella Bettonte

Anno Accademico 2015 - 2016

Indice

Introduzione

La ricerca di numeri primi ha sempre affascinato i matematici di ogni epoca in quanto l'algebra era considerata la materia più elegante in cui impiegare il proprio intelletto, ma quest'ambito non è rimasto fine a se stesso e, come scrive Devin in [6] questa teoria matematica, apparentemente inutile ed esoterica, è divenuta la base di sistemi moderni di sicurezza. Ribenboim scrive in [2] che infatti nella crittografia a chiave pubblica è estremamente importante riconoscere la primalità di un numero o trovare i fattori di un numero molto grande, e questo rappresenta ai giorni nostri un'affascinante applicazione della teoria dei numeri alle comunicazioni.
In questa tesi, fornita prima una necessaria infarinatura sui test di primalità, ovvero degli algoritmi che permettono di sapere se un numero intero sia primo o composto, ci soffermeremo sul problema di trovare delle formule che siano in grado di generare numeri primi. Il continuo miglioramento della potenza di calcolo degli elaboratori richiede di trovare numeri primi sempre più grandi per riuscire a mantenere sicure le comunicazioni.
Una formula per i numeri primi è un'espressione che consenta di distinguere nell'ambito degli interi positivi tutti i numeri primi e solo essi. La ricerca di una tale formula impegna da secoli i matematici, ma finora non è stata data alcuna formula semplice di questo tipo. Il problema sta nel fatto che per quanto sia semplice trovare una funzione o una classe di funzioni che generi un'infinità di numeri primi a partire da una variabile che è un numero naturale o un numero primo, è tutt'altro che semplice trovare una funzione che generi esclusivamente numeri primi e, in secondo luogo, che li generi tutti.

Capitolo 1

Prerequisiti

Iniziamo fornendo i requisiti essenziali per poter inquadrare il problema che vogliamo trattare, dal punto di vista matematico.

Definizione. *Un numero p è primo se dato un prodotto di due numeri interi m e n tale che $p \mid mn$ allora $p \mid m$ o $p \mid n$. Un numero naturale che non è primo è detto composto.*

Una relazione molto importante per i numeri primi è il Piccolo Teorema di Fermat che utilizzeremo molto spesso nelle dimostrazioni seguenti, lo ricordiamo qui di seguito.

Piccolo Teorema di Fermat. *Sia p un numero primo. Se $a \in \mathbb{Z}$ è primo con p, allora: $a^{p-1} \equiv 1 \pmod{p}$. In particolare $x^p \equiv x \pmod{p}$ per ogni intero x.*

1.1 Test di primalità

Per scoprire se un numero intero sia primo si può effettuare un test di primalità che va distinto da un algoritmo di fattorizzazione, che ha lo scopo di determinare i fattori primi di un numero. Passiamo ora ad esaminarne alcuni.

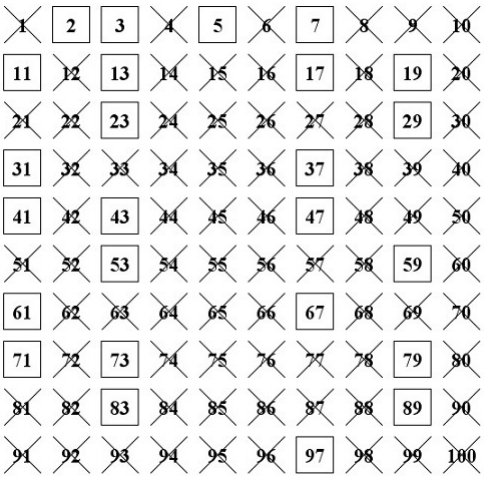

Figura 1.1: Il crivello di Eratostene (cf. [12])

Crivello di Eratostene.

Il crivello di Eratostene è un antico procedimento per il calcolo delle tabelle di numeri primi fino ad un certo numero n prefissato. Facendo riferimento alla Figura 1.1, il procedimento è il seguente: si scrivono tutti i numeri naturali a partire da 2 fino a n in un elenco detto setaccio. Poi si cancellano tutti i multipli del primo numero del setaccio (escluso lui stesso). Si prende poi il primo numero non cancellato maggiore di 2 e si ripete l'operazione con i numeri che seguono, proseguendo fino a che non si applica l'operazione all'ultimo numero in tabella non cancellato. I numeri che restano sono i numeri primi minori o uguali a n.

Teorema (Wilson). *Se $n > 1$ è un numero primo allora si ha*

$$(n-1)! \equiv -1 \ mod\ n. \tag{1.1}$$

Dimostrazione. Questa dimostrazione è tratta da [5]. Se n non è primo, allora $n = ab$, $1 < a \leq b < n$ e $(n-1)! = 1 \cdot 2 \cdots a \cdots b \cdots (n-1) \equiv 0 \bmod n$. Rimane da vedere che se $n = p$ è primo allora $1 \cdot 2 \cdots (p-a) \equiv$-1(mod p). Nel campo $\mathbb{Z}_p$, ogni elemento non nullo, x, ha un inverso: $xx^{-1} \equiv 1 \pmod p$. Abbiamo $x = x^{-1}$ se e solo se $x^2 - 1 = 0$. Il polinomio $x^2 - 1$ ha esattamente due radici nel campo $\mathbb{Z}_p$: ± 1. Siccome $p-1 \equiv -1 \pmod p$ allora $1 \cdot 2 \cdots (p-1) \equiv 2 \cdot 3 \ldots (p-2)(-1) \pmod p$. Gli elementi di $2, 3, \ldots, p-2$ vanno a coppia xx^{-1}, quindi $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod p$, pertanto vale la tesi. □

Il Teorema di Wilson è inutilizzabile come test di primalità, dal momento che il calcolo esplicito di $(n-1)!$ mod n, richiede n moltiplicazioni, è difficile per n grande.

Capitolo 2

Formule generatrici di primi

In questo capitolo dapprima affronteremo il problema di trovare una formula esatta per l' n-esimo numero primo e poi, vista l'impossibilità di trovare una formula efficiente, ci soffermeremo su alcune formule polinomiali che generano primi; in tutto questo percorso seguiremo l'impostazione data da Zaccagnini e Languasco in [4]. Successivamente esamineremo due classi di numeri "speciali", i numeri di Fermat e Mersenne, seguendo la presentazione di questi numeri proposta da Paulo Ribenboim in [2].

2.1 Formule esatte

Il Teorema di Wilson permette di scrivere una formula esatta per $\pi(x) = \#\{p \mid p \text{ primo}, p \leq x\}$ e così anche per p_n, n-esimo numero primo. Queste formule però non sono utilizzabili nella pratica perché richiedono troppi calcoli, più di quelli necessari a eseguire il crivello di Eratostene. Vediamo come ricavarle.

Osservazione 1. *Se $k \geq 6$ è un intero non primo allora $k \mid (k-2)!$.*

Dimostrazione. Se k non è primo possiamo trovare $a, b \in \mathbb{Z}$ tali che $k = ab$ con $1 < a \leq b < k$. Distinguiamo due casi:

- Se $k = p^2$ dove $p \geq 3$ è un numero primo allora $a = b$. Osserviamo che tra i fattori di $(k-2)!$ vi sono certamente p e $2p$, e quindi $p^2 \mid (k-2)!$.
- Se $k \neq p^2$ possiamo trovare a, b come sopra ma con $a < b$ dunque a e b sono fattori distinti di $(k-2)!$ e quindi $k \mid (k-2)!$.

□

Osservazione 2. *Se p è primo allora $(p-2)! \equiv 1$ (mod p).*

Dimostrazione. Per il Teorema di Wilson abbiamo che se p è primo allora $(p-1)! \equiv -1 (\text{mod } p)$. Poiché $(p-1) \equiv -1 (\text{mod } p)$ e $\gcd(p-1, p) = 1$ possiamo semplificare la congruenza (perché $p-1$ è invertibile modulo p) e ottenere $(p-2)! \equiv 1 (\text{mod } p)$. □

Usando queste due considerazioni possiamo scrivere una formula per $\pi(x)$.

$$\pi(x) = \#\Big\{ p \in \mathbb{Z} \ : \ p \,\text{primo}, p \ \leq x \Big\}. \tag{2.1}$$

Indichiamo con $\lfloor x \rfloor$ la parte intera di x, ossia $\lfloor x \rfloor = max\Big\{n \in \mathbb{Z} : n \leq x\Big\}$, e con $\{x\}$ la parte frazionaria di x, ossia $\{x\} = x - \lfloor x \rfloor$.
Con queste notazioni possiamo concludere che la quantità

$$k\left\{\frac{(k-2)!}{k}\right\} \tag{2.2}$$

vale 0 se $k \geq 6$ è un numero non primo e vale 1 se k è primo.
Dunque per $x \geq 3$ abbiamo: $\pi(x) = 2 + \sum_{5 \leq k \leq x} k\left\{\frac{(k-2)!}{k}\right\}$.

Ora ricaviamo la formula esatta per p_n indicata da Hardy e Wright in [1]. Per prima cosa ricordiamo il Postulato d Bertrand.

Postulato di Bertrand. *Per ogni $n \geq 1$, l'intervallo $[n, 2n]$ contiene un numero primo.*

Definiamo

$$f(x,y) = \begin{cases} 1 & x > y \\ 0 & x \leq y \end{cases}. \tag{2.3}$$

Dunque:

$$f(n, \pi(j)) = \begin{cases} 1 & n > \pi(j) \text{ i.e. } j < p_n \\ 0 & n \leq \pi(j) \text{ i.e. } j \geq p_n \end{cases}. \tag{2.4}$$

Dal postulato di Bertrand abbiamo $p < 2^n$, quindi abbiamo ottenuto il seguente lemma.

Lemma (Formula di Hardy e Wright). *Sia p_n l' n-esimo numero primo, allora:*

$$1 + \sum_{j=1}^{2^n} f(n, \pi(x)) = 1 + \sum_{j=1}^{p_n - 1} 1 = p_n. \tag{2.5}$$

2.2 Formule polinomiali

Continuando a parlare di formule che in qualche modo permettono di generare numeri primi ci soffermiamo ora sui polinomi.

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

Dimostrazione. Sia $f \in \mathbb{Z}[x]$ un polinomio che assume solo valori primi. Sia $p := f(1)$. Si ha che $f(1 + np) = f(1) = 0 \pmod p$ per ogni $n \in \mathbb{Z}$ e quindi $f(1 + np) = \pm p$ poiché deve essere un valore primo e i multipli di p non lo sono. Questo è assurdo se f non è costante perché l'equazione $f(x) = \pm p$ ha al massimo $2 \cdot \deg(f)$ soluzioni, infatti nessun polinomio non costante può assumere uno stesso valore un numero di volte maggiore al proprio grado. □

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

Dimostrazione. La prima parte è una conseguenza diretta del teorema precedente. La seconda parte richiede un risultato di Matiyasevich ([3]), enunciato qui di seguito. □

Definizione (Insieme diofanteo). *Un insieme S di interi positivi si dice diofanteo se e solo se esiste un polinomio $Q \in \mathbb{Z}[x_1, x_2, \ldots, x_m]$ tale che $S = \Big\{Q(x_1, \ldots, x_m) \geq 1 : x_1 \geq 1, \ldots, x_m \geq 1\Big\}$.*

Teorema di Matiyasevich-Robinson-Davis-Potnam, cf. [3]). *L'insieme dei numeri primi è diofanteo.*

D'altra parte, esistono polinomi, come l'esempio di Eulero, che mostriamo qui di seguito, che assumono moltissimi valori primi.

Esempio (Eulero, cf. [2]). La curva piana definita dall'equazione

$$f(x) = x^2 + x + 41 \tag{2.6}$$

è detta la "Parabola di Eulero". Per $0 \leq k < 40$, con $k \in \mathbb{Z}$, abbiamo che i valori di $f(k)$ sono tutti primi. Invece per $k = 40$ otteniamo $f(40) = 1681 = 41^2$ che non è primo. Lo stesso si può mostrare per $f(x) = x^2 - x + 1$, basta effettuare un cambio di variabili in (2.6); sostituiamo ad x il polinomio $x - 1$, con $x \in \mathbb{Z}$. Facendo i calcoli risulta:

$$(x-1)^2 + (x-1) + 41 = x^2 - 26 + x + 1 + x - 1 + 41 = x^2 - x + 41. \tag{2.7}$$

Altrimenti si può anche mostrare applicando la seguente simmetria rispetto all'asse y

$$\begin{cases} x = -x' \\ y = y' \end{cases} \tag{2.8}$$

alla parabola $y = x^2 + x + 41$ ottenendo $y' = x'^2 - x' + 41$. Questa seconda parabola presenta valori primi per $x' = 0, \ldots, 40$, invece valutata in $x' = 41$ restituisce un valore non primo.

Teorema (Schur). *Sia $f \in \mathbb{Z}[x]$ un polinomio non costante. L'insieme P_f, definito come segue, è infinito.*

$$P_f := \{p : \exists\, n \in \mathbb{N} \text{ tale che } f(n) \neq 0 \text{ e } p \mid f(n)\}. \tag{2.9}$$

Dimostrazione. Sia $f(x) = a_r x^r + \cdots + a_0$ con $a_r \neq 0$. Se $a_0 = 0$ allora $f(x) = x(a_r x^{r-1} + \cdots + a_1)$ e quindi il numero primo p divide $f(np)$, che non è nullo per $n \in \mathbb{N}$ sufficientemente grande, cioè $p \in P_f$. In questo caso dunque, P_f è l'insieme di tutti i primi. Possiamo ora supporre $a_0 \neq 0$. Per assurdo sia $P_f = \{p_1, ..., p_k\}$ finito e sia $c \in \mathbb{Z}$ tale che $|f(ca_0 p_1, ..., p_k)| > |a_0|$, dunque non nullo. Abbiamo anche che

$$\frac{1}{a_0} f(ca_0 p_1, ..., p_k) \equiv 1 \pmod{p_1, ..., p_k} \tag{2.10}$$

e quindi esiste un primo $p \notin P_f$ tale che $p \mid \frac{1}{a_0} f(ca_0 p_1, ..., p_k)$. Quindi abbiamo che P_f è infinito. □

Lemma. *Se p è un numero primo e $p \mid (n^2 + 1)$ per qualche $n \in \mathbb{N}$ allora $p = 2$ oppure $p \equiv 1$ (mod 4).*

Dimostrazione. Supponiamo, per assurdo, che $p \equiv -1 \pmod 4$. L'ipotesi equivale a $n^2 \equiv -1 \pmod p$ e per il Piccolo Teorema di Fermat abbiamo anche $n^{p-1} \equiv 1 \pmod p$. Poiché $p - 1 = 4m + 2$ per qualche $m \in \mathbb{N}$ si ha:

$$1 \equiv n^{p-1} = n^{4m+2} \equiv n^{2(2m+1)} \equiv -1 \pmod p \tag{2.11}$$

che è assurdo. □

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

Dimostrazione. Supponiamo che esistano solo un numero finito di primi $p_i \equiv 1 \pmod 4$. Poniamo $N := (2p_1, ..., p_k)^2 + 1$. Se q è un fattore primo di N per il lemma precedente abbiamo $q \equiv 1 \pmod 4$ ma q non è tra i p_i, dunque ogni insieme finito di primi della forma $4n + 1$ esclude i primi di quella forma. Se esistessero solo un numero finito di numeri primi $p_i \equiv -1 \pmod 4$, posto $N = 4p_1 \cdots p_k - 1$ si avrebbe $N \equiv -1 \pmod 4$ e non è possibile che tutti i fattori primi di N siano congrui a 1 (mod 4). □

2.3 Numeri di Fermat e Numeri di Mersenne

Fermat e Mersenne nel diciassettesimo secolo introdussero dei "numeri speciali" e affermarono che le loro formule producessero primi: purtroppo, come vedremo, le loro congetture si rivelarono sbagliate.

Definizione (Numeri di Fermat e Numeri di Mersenne). *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 $M_n = 2^n - 1$.*

Ora analizzeremo le relazioni note tra i numeri di Fermat e Mersenne e la primalità nei seguenti sottoparagrafi.

2.3.1 Numeri di Fermat

Teorema. *Se il numero $2^m + 1$ è primo, allora $m = 2^n$ per qualche intero n, dunque esso è un numero di Fermat $F_n = 2^{2^n} + 1$.*

Dimostrazione. Questa dimostrazione è tratta da [4]. Se m non fosse una potenza di 2, allora esisterebbero interi a e b tali che $m = ab$, con $b < 1$ dispari. Osservando che il polinomio $x^b + 1$ è divisibile per il polinomio $x + 1$ e applicando tale fatto al caso particolare $x = 2^a$ si ha che $2^a + 1 \mid 2^{ab} + 1$ e dunque quest'ultimo non può essere un numero primo, assurdo. □

Fermat congetturò che tutti i numeri F_n fossero primi ma questo è vero solo per $n = 0, 1, \ldots, 4$ 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 il fattore primo.
In particolare vediamo una dimostrazione di Eulero che mostra che F_5 non è

primo. Ricordiamo che $x+1$ divide x^4-1. Nel caso particolare che $x = 5 \cdot 2^7$ abbiamo che

$$641 = x + 1 \mid x^4 - 1 = 2^{28} \cdot 5^4 - 1 = A. \tag{2.12}$$

Inoltre

$$641 = 2^4 + 5^4 \mid 2^{28} \cdot (2^4 + 5^4) = 2^{32} + 2^{28} \cdot 5^4 = B. \tag{2.13}$$

Quindi

$$641 \mid B - A = 2^{32} + 1 = 2^{2^5} + 1 = F_5. \tag{2.14}$$

Dal momento che i numeri F_n crescono molto rapidamente con n, diventa molto laborioso controllare la loro primalità. Usando il piccolo Teorema di Fermat, Pepin ottenne nel 1877 un test di primalità per i numeri di Fermat. Prima di enunciare e dimostrare il teorema di Pepin premettiamo premettiamo una definizione fondamentale presa da [5].

Definizione. *Se p è un numero primo e a è un intero, allora il simbolo di Legendre $\left(\frac{a}{p}\right)$ è uguale a:*

- 0 *se p divide a;*
- 1 *se a è un quadrato modulo p;*
- -1 *se a non è un quadrato modulo p.*

Teorema (Pepin, cf. [2]). *Per $n > 1$ il numero $F_n = 2^{2^n} + 1$ è primo se e solo se $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$.*

Dimostrazione. Per ogni F_n si ha:

$$\begin{cases} F_n \equiv 1 (mod 4) \\ F_n \equiv 2 (mod 3) \end{cases} . \tag{2.15}$$

Per il Criterio di Eulero

$$3^{\frac{F_n-1}{2}} \equiv \left(\frac{3}{F_n}\right) \bmod F_n \tag{2.16}$$

dove si è usato il simbolo di Legendre; se F_n è primo si può applicare la legge di reciprocità quadratica, e quindi

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1. \tag{2.17}$$

Inversamente se $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$, la stessa congruenza deve valere per ogni fattore primo p di F_n; quindi si ha $3^{F_n-1} \equiv 1 \pmod{p}$ ovvero l'ordine di 3 modulo p divide $F_n - 1$ ed è quindi una potenza di 2. Ma tale ordine non divide $\frac{F_n-1}{2}$ (che è ancora una potenza di 2) e quindi deve essere precisamente $F_n - 1$. Quindi $p > F_n$ e p deve essere F_n, ovvero quest'ultimo deve essere primo. □

Il test di primalità di Pepin è molto utile nelle applicazioni ma, se F_n è composto, non indica alcun fattore di F_n. Ad esempio, usando il Test di primalità di Pepin, Selfrige e Hurwitz nel 1943 conclusero che F_{14} è composto, senza determinare nessuno dei suoi fattori.

Per fare alcuni esempi, citiamo alcuni "record".

- Il più grande numero primo di Fermat conosciuto è $F_4 = 65537$ (cf. [6]).
- Il più grande numero composto di Fermat è stato scoperto nel 2015, è $F_{2662088}$ e un suo fattore primo è $267 \cdot 2^{2662090} + 1$ (cf. [10])

Ci sono ancora molte questioni aperte riguardo ai numeri di Fermat, cioè se ci siano un numero infinito di numeri primi di Fermat e un numero infinito di numeri composti di Fermat.

2.3.2 Numeri di Mersenne

Teorema. *Se l'n-esimo numero di Mersenne M_n è primo, allora n è primo.*

Dimostrazione. Se n fosse composto allora esisterebbero $1 < a, b < n$ tali che $n = ab$. Di conseguenza $2^a - 1$ sarebbe un fattore di M_n perché $2^{ab} - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{a(b-1)}$, assurdo. □

Mersenne diede una lista di numeri primi p per i quali M_p è primo, ma questa lista contiene vari errori e omissioni. Infatti Mersenne nella sua lista valutò tutti i numeri di quel tipo considerando tutti i valori di n fino a $n = 257$ ma ha incluso erroneamente M_{67} e M_{257} (che non sono primi) e ha escluso M_{61}, M_{89} e M_{107} (che sono primi).
Lucas aveva già dimostrato nel 1886 che M_{67} è composto, ma trovarne i fattori era, all'epoca, un lavoro estenuante. Nell'ottobre del 1903 Frank N. Cole tenne a un incontro dell'American Mathematical Society la prima, e sinora unica, conferenza di matematica senza parole: quando arrivò il suo turno si alzò, andò alla lavagna e calcolò $2^{67} - 1$, poi calcolò $193707721 \cdot 761838257287$, ottenendo lo stesso numero (cf. [7]).
L'ultimo errore fu trovato da Kraitchik che, nel 1922, dimostrò che M_{257} è composto ma non è nota la fattorizzazione (cf. [8]).
Tuttavia i risultati di Mersenne sono comunque stupefacenti, considerata la grandezza dei numeri coinvolti.

Anche nel caso dei numeri di Mersenne esistono dei criteri di primalità speciali.

Teorema. *Se p e q sono numeri primi e $p \mid M_q$, allora $p \equiv 1$ mod q.*

Dimostrazione. Dimostrazione tratta da [4]. Essendo per definizione M_n dispari,abbiamo che sicuramente p è dispari. Sia r l'ordine di 2 in $\mathbb{Z}_p^*$,considerato come gruppo moltiplicativo cioè il minimo intero positivo per cui $2^r \equiv 1 \pmod{p}$. Evidentemente $r > 1$ poiché $2^1 = 2 \not\equiv 1 \pmod{p}$. Inoltre, per ipotesi, $2^q \equiv 1 \pmod{p}$ e quindi $r \mid q$. Dato che q è un numero primo abbiamo che $q = r$. Per il Teorema di Lagrange abbiamo che $r \mid p - 1$ e cioè $p \equiv 1 \pmod{q}$. □

Ci sono attualmente 44 numeri primi di Mersenne. I numeri di Mersenne con $p \leq 127$ sono stati scoperti prima dell'epoca dei computer. Turing provò, senza successo, nel 1951 a trovare un numero di Mersenne utilizzando un computer. Nel 1952, Robinson scoprì i numeri primi M_{521}, M_{607}, M_{1279}, M_{2203}, M_{2281} usando un computer SWAC, un computer digitale costruito nel 1950 dal National Bureau of Standards a Los Angeles.

Citiamo ora alcuni record:

- Il più grande numero primo conosciuto è stato scoperto nel 2016 (cf. [9]), è di Mersenne ed ha più di 22 milioni di cifre: $M_{74207281} = 2^{74207281} - 1$.
- Il massimo numero di Mersenne del quale siano noti i fattori primi è M_{63703}, un suo fattore primo è 42808417, (cf. [11]).

Ci sono questioni aperte sui numeri di Mersenne, non è ancora noto se i numeri di Mersenne composti e primi siano infiniti.

Bibliografia

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

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

[3] Y.V. Matiyasevich, Yuri V. (1970). *[Enumerable sets are Diophantine]. Doklady Akademii Nauk SSSR* (in Russian) 191: 27-282. . English translation in Soviet Mathematics 11 (2), pp. 354-357.

[4] A.Languasco, A.Zaccagnini. *Alcune proprietà dei numeri primi.* matematica-old.unibocconi.it/LangZac/LangZacc2.pdf

[5] P.Ellia. *Teoria dei numeri.* dm.unife.it/philippe.ellia/Docs/TeoriaNumeri2013-14-OnLine.pdf

[6] K.Devlin. *Dove va la matematica*, Bollati Boringhieri,1999.

[7] M. Du Sautoy. *L'enigma dei numeri primi*, Rizzoli, 2004.

[8] M.Kraitchink. *La mathématique des jeux*, Bruxelles : Editions techniques et scientifiques, 1953.

[9] American Mathematical society. *New Record for Largest Known Prime.* `ams.org/news?news_id=2939`

[10] PrimeGrid. *PrimeGrid's Proth Prime Search* `http://www.primegrid.com/download/PPS-F2662088.pdf`

[11] Mersenne.ca *Link al sito* `http://www.mersenne.ca/prp.php`

[12] Immagine Crivello di Eratostene *Link al sito* `http://www.cut-the-knot.org/Curriculum/Arithmetic/Eratosthenes.shtml`