Open Science Repository Mathematics

doi: 10.7392/openaccess.70081967

Mersenne Primes Cardinality

-.By Alberto Durán Meza.-

otreblam@gmail.com

University J.M.Vargas -Faculty Engineering/Education

Caracas/Venezuela

SMC: 2011. 11AXX

Abstract. This article is concerned with basic Number Theory.Our purpose is to show that, there are infinitely many Mersenne Prime Numbers, for this, we shall use, some known Theorems or results in Arithmetic and Cantorian set Theory.

Key Words. Prime, Mersenne's Primes, Eclid's Theorem, Cantor's Theorem, Schröder-Bernstein's Theorem, Pomerance'sTheorem.

1. **Notation and Preliminary Lemmas.**

1.1Starting with, we need to establish some basic notation.The symbol M_P, formally shall represent Mersenne's Primes numbers, that is $M_P = \{x \in \mathbb{N}, x = 2^p - 1\}$, where p and x **are both primes.** While the symbol P_r stands for the totality of prime numbers $[6][18]$.

Lemma 1. Euclid's Theorem. $Card.(P_r) = \aleph_0, [3]$.

Lemma 2. Schröder-Bernstein's Theorem.

If $f : S \to T$ and $g : T \to S$, are both injective functions, then there exists a Bijective function $h : S \to T. [16]$.

Lemma 3. **Cantor's Theorem.**

If $\psi : S \to T$, is an Bijective function, thus $Card.(S) = Card.(T), [2]$.

Lemma 4. **Pomerance´s Theorem.** Every prime number p has its proof of Primality. $[11]$.

2.1 For the sake of completeness, also we must define the following auxiliary set:

$D = \{p \in P_r : 3 \leq p \prec p+1\}$ Notice that, $p+1$ is even and this set **is finite** by construction, due to the fact that, for some prime p given, the number of Primes from three to $p+1$ **is finite** $[14]$. Furthermore, D can be represented by this equivalent form:

$D = \{p_1, p_2, ..., p_{\lambda-1}, p_\lambda\}$, consequently it contains λ primes and we can write the relation,

$$(1) \quad Card.(D) = \lambda \in \mathbb{N}.$$

It should be observer that, this set plays a very important role in our approach.

To solve our guess, also we need define a generating function $\phi : P_r \to \mathbb{N}$ as follows,

$$\phi(p) = \begin{cases} 2^p - 1, & \text{if and only if } 2^p - 1 \text{ is prime} \\ 2^p & \text{Otherwise} \end{cases}$$

As we shall see, Images of this function I_ϕ does contain (in particular) **two infinite subset**:

Mersenne Primes M_p and $H_0 = \{y \in \mathbb{N} : y = 2^n\}$, n belongs to $\mathbb{N}$, our aim in this article is to prove the following statement; which is immediate consequence of our preceding definitions.

Proposition 1.2.1 Sequence H_0 and M_p are both infinite sets.

Proof.

We first prove that H_0 is infinite. This arithmetical fact is immediate, because we have infinite possibilities for the choice of the quantity $n = p$, whenever $p \in P_r$, by applying Lemma 1 or Euclid's Theorem. It follows that, $Card.(H_0) = Card.(P_r) = \aleph_0$, next we must prove that,

$$(2) \quad Card.(M_p) = \aleph_0.$$

In order to show that important Cantorian relation, we need to construct another two "bizarre functions", by using our basic sets P_r, M_p and D in the following way: $\psi_1 : P_r \to M_p \cup D$

$$\psi_1(p) = \begin{cases} 2^p - 1, & \text{if and only if } 2^p - 1 \text{ is prime} \\ 2^p & \text{if } 2^P - 1 \text{ is not prime} \end{cases}$$

Remark 1. The quantity p is to be the **maximum prime** number inside D. But a sample it is needed to explain how $\psi_1(p)$ works: if $p=11$, thus $\psi_1(11)\notin M_p$. Since D belongs to the range of ψ_1, this means that, we must get the maximum prime of $D=\{3,5,7,11,12\}$, accordingly our definition at 2.1 above, obviously our **finite algorithm** provides the value,

$$(3)\quad \psi_1(11)=11$$

Under that **crucial restriction**, function $\psi_1:P_r\to M_p\cup D$ remains well defined (because $11\in P_r$, but it don´t generates none Mersenne´s prime). Likely, **existence** and **uniqueness** of a maximum prime p belonging to D, is based upon Lemma 4 or Pomerance's Theorem.

3.1 Continuing our task, also we define another generating function $\psi_2:M_p\cup D\to P_r$,

$$\psi_2(x)=\begin{cases} Log_2(x+1) & \text{If } x\in M_p \\ p & \text{If } x\notin M_p \end{cases}$$

Remark 2. By definition, only two cases can occur: either $x\in M_p$ or $x\notin M_p$ (similarly to preceding case) p is to be the **maximum prime** number inside D.With this caution, we are ready to prove a basic result, by employing functions ψ_1,ψ_2 previously constructed; in the next section we shall do it.

2. **Injectivity of** $\psi_1:P_r\to M_p\cup D$, $\psi_2:M_p\cup D\to P_r$.

Proposition 1.2.2 Functions ψ_1 and ψ_2 defined above, are both injective.

Proof. Formally, it is necessary to distinguish the following two cases:

Firstly, we study $\psi_1:P_r\to M_p\cup D$. Let us p_1,p_2 belonging to P_r. Whenever p_1 and p_2 satisfy these conditions, $\psi_1(p_1)\in M_p$ and $\psi_1(p_2)\in M_p$ as well.

We can assume by hypothesis that,

$$(5)\quad \psi_1(p_1)=\psi_2(p_2).$$

This means that there exist two primes p_1,p_2, contained in P_r satisfying the system:

(6) $$\begin{cases} \psi_1(p_1) = 2^{p_1} - 1 \\ \psi_1(p_2) = 2^{p_2} - 1 \end{cases}$$

But applying (5) we may write, $2^{p_1} - 1 = 2^{p_2} - 1 \Rightarrow 2^{p_1} = 2^{p_2}$ and so : $p_1 = p_2$.

We conclude that (in this case) $\psi_1 : P_r \rightarrow M_p \cup D$ **is injective.**

We have therefore left to examine, when $\psi_1(p_i) \in D_1$ and $\psi_1(p_j) \in D_2$; thence

there exists two primes p_i, p_j which satisfy the conditions: $p_i \prec p_j$ or $p_j \prec p_i$

now it is easily seen that, in either case we have,

(7) $p_i \neq p_j$. In accordance with definition of D, numbers p_i and p_j satisfy,

(8) $p_i =$ maximum prime of D_1 and simultaneously $p_j =$ maximum prime of D_2.

In turn from (7) we have immediately,

(9) $\psi_1(p_i) \neq \psi_1(p_j)$. And $\psi_1 : P_r \rightarrow M_p \cup D$ is injective. As was to be proved.

2.2 Well, at this point of the proof, we now analyze the function $\psi_2 : M_p \cup D \rightarrow P_r$.

Case 1. Let x_1, x_2 two arbitrary elements belonging to M_p, whence there exists two primes p_1, p_2 which by hypothesis satisfy the Diophantine equations:

(10) $x_1 = 2^{p_1} - 1$ and $x_2 = 2^{p_2} - 1$, we can suppose that: $p_1 \neq p_2$, hence one has,

(11) $2^{p_1} - 1 \neq 2^{p_2} - 1 \Rightarrow x_1 \neq x_2$, and from this, just we deduce the relation below:

(12) $Log_2(x_1 + 1) \neq Log_2(x_2 + 1) \Rightarrow \psi_2(p_1) \neq \psi_2(p_2)$.

We have showed (only in this case) the injectivity of the function $\psi_2 : M_p \cup D \rightarrow P_r$.

Case 2. If we get two prime numbers $p_i \in D_1$ and $p_j \in D_2$, for some i, j natural numbers. Being p_i and p_j the maximum primes contained in D_1 and D_2 respectively.

Next, by hypothesis we may assume that $p_i \neq p_j$, obtaining immediately,

(13) max. prime of $D_1 \neq$ max. prime of D_2.

It is quickly seen that, from (13) we may write,

(14) $\psi_2(p_i) \neq \psi_2(p_j)$. So, we have showed that $\psi_2 : M_p \cup D \to P_r$ **is injective**.

This completes the proof of the Proposition 1.2.2

3. **Applying Schröder--Bernstein's Theorem.**

In this section we shall show, our most important result of this brief research work. Before, We must point out the following.

3.1 By definition $3 \in M_p$ and $3 \in D$, which shows clearly that $M_p \cap D \neq \varnothing$, although being D finite; $Card.(M_p \cap D)$ is finite or not. Indeed, we can to show that, $Card.(M_p \cap D)$ **is finite**. Of course, if is not so; assume that $Card.(M_p \cap D)$ is infinite, whence both sets M_p and D should be infinite; eventually M_p would be infinite (we don't knows), [15]; but in particular D necessarily should be infinite, which contradicts Equation (1) at section 2.1 above. Taking in account all these arithmetical features, thus we may write:

(14) $Card.(M_p \cap D) = \alpha \in \mathbb{N}$.

Finally we can pay attention to the cardinality of Mersenne's prime numbers. As we saw already, functions $\psi_1 : P_r \to M_p \cup D$ and $\psi_2 : M_p \cup D \to P_r$ are both injective.

Lemma 1, or Schröder-Bernstein's Theorem guarantees that : there exists a Bijective Function $\Psi : M_p \cup D \to P_r$, additionally Lemma3 or Cantor's Theorem implies $M_p \cup D$ and P_r are certainly, **Equipollent sets**. In other words, they have **the same cardinality.** This is another way of saying that, the relation below,

(15) $Card.(M_p \cup D) = Card.(P_r)$ Holds.

Consequently, from (15), by applying Cantorian set Theory; we may write at once:

$(16) \quad Card.(M_p)+Card.(D)-Card.(M_p \cap D)=Card.(P_r)$.

Hence, substituting every known result in (16), we have obtained the equation:

$(17) \quad Card.(M_p)+\lambda-\alpha=\aleph_0 \Rightarrow Card.(M_p)=\aleph_0+(\alpha-\lambda)$.

Let $\alpha-\lambda=\beta$, it is clear that, in any case $\beta\in\mathbb{Z}$, ending this section we have that, (17) becomes, $Card.(M_p)=\aleph_0+\beta=\aleph_0$. Summarizing, equation (2) is true.

3.2 In the current literature, it is well known that: there exists a relationship (so important like interesting)between Even Perfect Numbers and Mersenne's prime. The classic result so-called **Euclid-Euler's Theorem** characterize Mersenne primes and Perfect Numbers $[8]$, which assert that: θ is an **Even Perfect Number**, if and only if ,It can be written in the form, $\theta=2^{p-1}.(2^p-1)$, where p and 2^p-1 are both Primes. It was not still **eighteenth century**, that Mathematicians become aware of such a Characterization $[4][9]$, due to the works of famous and prolific Swiss Mathematician, **Leonhard Euler (1707-1783),** $[1]$. He studied in every branch of Mathematics then known $[22]$, and his extensive writings are more numerous than those of any other Mathematician $[10]$.

3.3 As a result of Proposition 1.2.1; we have obtained the following statement,

Corollary 3.3.1 There exist infinitely many **Even Perfect Numbers.**

We must point out a historical fact: Mathematician **Nicomachus of Gerasa (60-120 AC**), conjectured this result $[7]$ He claimed : " **Perfect Numbers are infinite ".** However, accordingly actual references, **He does not prove** that important assertion $[19]$.

4. Concluding Comments.

From several references $[5]$, French monk: **Jean Baptist Marin Mersenne (1588-1648),** failed taking like primes the cases corresponding to $p = 11$, 23, 83, 131, 179, 191, 239, and 251. However, the posterity acknowledge his heroic contribution, by constructing its formula $2^p - 1$**,** to generate the first known Messene's prime $[12]$, much earlier of computation age $[21]$.

5. References

1. Andrews, G. Number Theory. Dover Publications INC., New York, 1994, pp.111-112.
2. Birkoff, G., Mac Lane, S. A Survey of Modern Algebra. New York, 1973. pp. 8-1.
3. Carmichael,D. The Theory of Numbers and Diophantine Analysis. Dover Publications INC. (1959), pp. 12-13.
4. Desnath L. Some recent results of Number Theory, discovered with electronic Computers. ijmest. 36:603-617, 1982. Ed. by Taylor and Francis. United Kingdom.
5. Dolan Daniel T, Mathematician on Stamps-NCTM, 1986- PP. 1-3, printed in USA.
6. Hardy, G., Wright, A. An Introduction to the Theory of Numbers, 5e Oxford University Press,U.K,1979, pp. 7-8.
7. Karpinsky L, Charles " Nicomachus of Gerasa ***Introduction to arithmetic*"**, translated into English by, Martin Luther D'Ooge; with studies in Greek arithmetic by Frank E, Robbins University of Michigan studies ,London:Macmillan(1926).
8. McDaniel, W. L. "On the Proof That All Even Perfect Numbers Are of Euclid's Type."Math. *Mag.* **48**, 107-108, 1975
9. Itard, J. Arimétique et Théorie des Numbres. Deuxieme edition mise a jour,Presses Universitaires, Boulevard des San Germain,Paris/France. 1967, pp. 39-45.10
10. Ogilvy, E., Anderson J. Excurxions in Number Theory.Oxford.,New York University Press., 1999, pp 21-24.
11. Pomerance, C. Every prime p has a proof of its primality.Math.of Comp. AMS, 48:315-322, 1987.
12. Ribenboim, P. The New Book of Prime Numbers Records,Springer Verlag,New York . 1995, QA246.R472.
13. Stanley, J., Margaret, J. Even Perfect Numbers, The Mathematics Teacher Boston College, Chesnut Hill, MA. 90: #8, 1997.

14. Shans, D. Solved and Unsolved Problems in Number Theory, 4ed. Chelsea New York, 1993, pp- 14-30.
15. Slowinski, D. Searching for the 27th Mersenne´s Prime,Journal of The Recreational Mathematics. pp. 258-261, 1979.
16. Sampson, J., Mostow, G., Mayer, J. Fundamental Structures of Algebra , MacGraw Hill, New York, USA.1963, pp.34-35.
17. Upenskiy James V, and Maxwell A. Heaslet, " Elementary Number Theory ", ch.9, (1939).Printed in USA.
18. Vinogradov, I., Number Theory, Printed in Moscow, edited by Group MIR. URSS. 1997, pp. 34-45.
19. Waterfiel Robert, the Theology of Arithmetic (English translation of the Greek), with a foreword by Keith Critchlow; 1988, p. 113.Retrived from Internet 2012-11-11.
20. Weil, André (1967), Basic number theory. Die Grundlehren der mathematischen Wissenschaften 144, Springer-Verlag New York, Inc., New York, USA.
21. Wells, David. The Penguin Dictionary of Curious and Interesting Numbers. New York-Viking Penguin. 1987, pp. 88-90.
22. Williams, Rob. "Google Doodle celebrates Leonhard Euler – Swiss mathematician considered one of the greatest of all time.
23. Youschkevich, A., Winter, E. Leonhard Euler and Christian Goldbach, Briefwechel, an more recent Edition, Berlin-Germain. 1965.
24. Zachariou, A. and Zachariou, E. "Perfect, Semi-Perfect and Ore Numbers." Bull. Soc. Math. Grèce (New Ser.) 13, 12-22, 1972.

Citation: Meza, A. D. (2013). Mersenne Primes Cardinality. Open Science Repository Mathematics, Online(open-access), e70081967. doi:10.7392/openaccess.70081967

Received: May 21, 2013

Published: May 29, 2013