PRIME NUMBERS THAT AVOID THE MERSENNE PROPERTY WITH RESPECT TO ALL OTHER PRIMES

DAVID EASDOWN

Abstract. An integer $m \geq 3$ is said to be *Mersenne with respect to* n, where $n \geq 2$, if $m = 1 + n + \ldots + n^k$ for some $k \geq 1$. This generalises the notion of a Mersenne prime number, since if m is a prime number Mersenne with respect to 2, then m is a usual Mersenne prime. For example, 31 is a usual Mersenne prime, but also Mersenne with respect to 5. By contrast, 13 is Mersenne with respect to 3 but not 2, and 5 and 11 are not Mersenne with respect to any prime. In this short note, we prove that there are infinitely many prime numbers that are not Mersenne with respect to any prime number. The first, more elementary, proof relies on a lower bound for $\pi(x) - \pi(x/2)$, established by Ramanujan (1919), where $\pi(x)$ is the number of primes not exceeding a given integer x. The second proof uses the full force of the Prime Number Theorem to deduce that $\mu(x) = O(\sqrt{x})$ and $\pi(x) - \mu(x)$ is asympotically equivalent to $x/\log x$, where $\mu(x)$ denotes the number of primes not exceeding x that are Mersenne with respect to some prime.

1. Introduction

Recall that a Mersenne prime has the form $2^k - 1$ for some integer $k \geq 2$. It is apparently an open problem whether infinitely many Mersenne primes exist. At the time of writing the largest known prime number is Mersenne. An integer $m \geq 3$ is said to be *Mersenne with respect to* n if $n \geq 2$ is an integer and $m = 1 + n + \ldots + n^k$ for some $k \geq 1$. Thus usual Mersenne primes are Mersenne with respect to 2. However a prime number may be Mersenne with respect to different primes. For example, 31 is Mersenne with respect to both 2 and 5. By contrast, 13 is Mersenne with respect to 3 but not 2, and 5 and 11 are not Mersenne with respect to any prime.

The motivation for this work comes from an example in a paper by Easdown and Hendriksen [1, Example 5.9], where they are given a list of primes $p_1, \ldots, p_k$ and, for the purpose of a particular group-theoretic construction, need the existence of a prime q such that $q < p_i^{s_i - 1}$ where s_i is the multiplicative order of p_i modulo q for each i. If $q > p^{s_i - 1}$ for some i then q is Mersenne with respect to p_i [1, Lemma 4.3]. Their task then is to locate a prime q that is not Mersenne with respect to each of $p_1, \ldots, p_k$. The existence of such q is guaranteed by [1, Theorem 5.8]. Their argument however does not guarantee that q is not Mersenne with respect to some other prime not on the original list.

The purpose of this note is to prove that there are infinitely many primes that are not Mersenne with respect to any prime, and moreover to show that such primes are asymptotically as plentiful as all primes. Ramanujan [2] established the following lower bound,

AMS subject classification (2010): 11A41.

Keywords: Mersenne numbers.

where $\pi(x)$ denotes the number of prime numbers not exceeding an integer x:

$$\pi(x) - \pi(x/2) \quad > \quad \frac{1}{\log x}\left(\frac{x}{6} - 3\sqrt{x}\right) \quad \text{for} \quad x > 300\ . \tag{1}$$

Certainly then

$$\lim_{x\to\infty} \frac{\pi(x) - \pi(x/2)}{\sqrt{x}} \;=\; \infty\ . \tag{2}$$

Note that (2) follows also from the Prime Number Theorem, but we retain the dependency on (1) to keep the proof of Theorem 2.3 below as elementary as possible.

2. Main result

Lemma 2.1. *If $m \neq 3$ is a prime number such that m is Mersenne with respect to a prime number n then $n < \sqrt{m}$.*

Proof. Suppose that m is prime, $m \neq 3$ and $m = 1 + n + \ldots + n^k$ for some prime n and integer k. Certainly, $m \geq 7$. If $n = 2$ then $n < \sqrt{7} \leq \sqrt{m}$, and we are done. Otherwise, m and n are both odd, so $k \geq 2$ and $n^2 < m$, and again we are done. $\square$

The following lemma is a sharpening of Lemma 5.5 of [1]:

Lemma 2.2. *If m is Mersenne with respect to n then k is not Mersenne with respect to n for $m < k \leq mn$.*

Proof. If m and k are Mersenne with respect to n and $m < k \leq mn$ then there exist positive integers α and β such that $m = 1 + n + \ldots + n^\alpha$ and $k = 1 + n + \ldots + n^{\alpha+\beta} = m + n^{\alpha+1} + \ldots + n^{\alpha+\beta}$, whence

$$n^{\alpha+1} \;\leq\; n^{\alpha+1} + \ldots + n^{\alpha+\beta} \;=\; k - m \;\leq\; (n-1)m \;\leq\; n^{\alpha+1} - 1\ ,$$

which is impossible. $\square$

Theorem 2.3. *There exist infinitely many primes that are not Mersenne with respect to any prime.*

Proof. Suppose to the contrary that there are only finitely many prime numbers that are not Mersenne with respect to any prime. Hence there is an integer N_0 such that whenever $p \geq N_0$ is a prime then there exists a prime $M(p)$ such that p is Mersenne with respect to $M(p)$. Clearly $N_0 > 3$ and so, by Lemma 2.1, $M(p) < \sqrt{p}$. By (2), there exists an integer $N \geq N_0$ such that $\pi(2N) - \pi(N) > \sqrt{2N}$. Put

$$P \;=\; \{p \mid p \text{ is prime and } N < p \leq 2N\} \quad \text{and} \quad Q \;=\; \{q \mid q \text{ is prime and } q \leq \sqrt{2N}\}\ .$$

From the above, M yields a mapping from P to Q, and, by Lemma 2.2, M is injective. This gives a contradiction, since the size of P exceeds that of Q, and the theorem is proved. $\square$

We can extract the main idea of the previous proof and combine it with the Prime Number Theorem to give the following result:

Theorem 2.4. *Let $\mu(x)$ denote the number of primes not exceeding x that are not Mersenne with respect to any prime. Then $\mu(x) = O(\sqrt{x})$.*

Proof. By (2) there exists N_1 such that for all integers $N \geq N_1$, $\pi(2N) - \pi(N) > \sqrt{2N}$. For each such N, put

$$P(N) = \{p \mid p \text{ is prime, } N < p \leq 2N, \text{ and } p \text{ is Mersenne with respect to some prime}\}$$

and $Q(N) = \{q \mid q \text{ is prime and } q \leq \sqrt{2N}\}$. As in the proof of Theorem 2.3, there exists an injective mapping from $P(N)$ to $Q(N)$. By the Prime Number Theorem,

$$|P(N)| \leq |Q(N)| \sim \sqrt{2N}/\log(\sqrt{2N}) = O(\sqrt{N}/\log N) .$$

Thus $\mu(2x) - \mu(x) = O(\sqrt{x}/\log x)$. It follows that $\mu(x) = O(\sqrt{x})$. □

There is no suggestion that the big-oh upper bound in the previous theorem is close to being sharp. It is not even known if there are infinitely many primes that are Mersenne with respect to some prime. By the Prime Number Theorem, we immediately have the following:

Corollary 2.5. *Primes that are not Mersenne with respect to any prime are as plentiful as arbitrary primes in the sense that* $\pi(x) - \mu(x) \sim x/\log x$*.*

Of course, Theorem 2.3 is a corollary of Corollary 2.5.

References

[1] D. Easdown and M. Hendriksen. Minimal faithful permutation representations of semidirect products of groups. Preprint.

[2] S. Ramanujan. A proof of Bertrand's postulate. *J. Indian Math. Soc*, 11:181–182, 1919.

School of Mathematics and Statistics, University of Sydney, NSW 2006, Australia

E-mail address: `david.easdown@sydney.edu.au`