ROCKY MOUNTAIN JOURNAL
OF MATHEMATICS
Volume 53 (2023), No. 3, 679–683

ON A QUESTION OF WITNO CONCERNING HYPOTHETICAL ELITE PRIMES FOR MERSENNE NUMBERS AND REPUNITS

ADEL ALAHMADI AND FLORIAN LUCA

We answer in the affirmative a question of Witno (2021) concerning elite primes for Mersenne numbers and repunits.

1. Introduction

Let $b \geq 2$ be a positive integer. For a positive integer m, we write

$$M_{b,m} = \frac{b^m - 1}{b-1}.$$

This is also called a repunit in base b. When $b = 2$, $M_{2,m}$ is the Mersenne number. Motivated by a question on primality testing for Fermat numbers, Witno [7] introduced the set of primes

$$\mathscr{P}_b = \left\{ 3 \leq p \text{ prime} : \left(\frac{M_{b,q}}{p}\right) = 1 \text{ for all primes } q \text{ sufficiently large} \right\}. \tag{1}$$

In the above, for an odd prime p the symbol $\left(\frac{a}{p}\right)$ stands for the Legendre symbol. Numerical calculations revealed some elements in $\mathscr{P}_b$ for some values of b, yet they appear to be very sparse. So, in [7, Section 4], it was asked whether it holds that

$$\sum_{p \in \mathscr{P}_b} \frac{1}{p} = O(1). \tag{2}$$

The main result of our article is that (2) holds.

Theorem 1. *Estimate* (2) *holds.*

Proof. For a set $\mathscr{A}$ of positive integers and a real number x, we write

$$\mathscr{A}(x) = \mathscr{A} \cap [1, x].$$

It suffices to show that

$$\#\mathscr{P}_b(x) = O\left(\frac{x}{(\log x)(\log\log x)^2}\right),$$

This project was funded by the Deanship of Scientific Research (DSR) at King Abdulaziz University in Jeddah under the grant DF-595-130-1441. The authors, therefore, gratefully acknowledge the DSR's technical and financial support.
2020 AMS *Mathematics subject classification:* 11A15, 11A41.
Keywords and phrases: elite primes, sieve methods.
Received by the editors on February 12, 2022, and in revised form on August 10, 2022.

DOI: 10.1216/rmj.2023.53.679

since afterwards the fact that the sum appearing in (2) is finite is a consequence of the Abel summation formula and the fact that the integral

$$\int_3^\infty \frac{dt}{t\log t(\log\log t)^2}$$

is convergent. We let $x > x_0$ be large and put $y := \sqrt{\log\log x}$. Consider primes $q \in (y, 2y)$. The number of them is

$$\pi := \pi(2y) - \pi(y) = \big(1+o(1)\big)\frac{y}{\log y} = \big(1+o(1)\big)\frac{2\sqrt{\log\log x}}{\log\log\log x} \quad \text{as } x \to \infty,$$

so $\pi < 3\sqrt{\log\log x}/\log\log\log x$ for $x > x_0$. Assume that $q \nmid p-1$. By Dirichlet's theorem on primes in progressions, there are infinitely many primes r such that $r \equiv q \pmod{p-1}$. Assuming $p > b$, we have that $b^r \equiv b^q \pmod p$, so $M_{b,r} \equiv M_{b,q} \pmod p$. In particular, $M_{b,q}$ is a quadratic residue modulo p. For y large, we have $q > 5$, so $M_{b,q}$ is not a square by work started by Nagell [6; 5] and completed by Ljunggren [3] to the effect that the only solutions of the Diophantine equation

$$\frac{u^m-1}{u-1} = v^2$$

in integers $u > 1$, $m \ge 3$, and $v \ge 1$ are

$$\frac{7^4-1}{7-1} = 20^2 \quad \text{and} \quad \frac{3^5-1}{3-1} = 11^2.$$

Write $M_{b,q} = D_{b,q}V_{b,q}^2$, with a squarefree number $D_{b,q} > 1$. We distinguish two cases for $p \in \mathscr{P}_b(x)$.

Case 1. Assume $p-1$ is divisible by at least $\pi/5$ primes q in $(y, 2y)$.

Let us denote by $\mathscr{P}_{b,1}(x)$ the set of such primes p. Putting $k := \lfloor \pi/5 \rfloor$, there are $q_1 < q_2 < \cdots < q_k$ primes q in $(y, 2y)$ such that $d = q_1\cdots q_k$ divides $p-1$. Note that

$$d = q_1\cdots q_k < (2y)^k < (2y)^\pi < \exp\left(\frac{3\sqrt{\log\log x}}{\log\log\log x}\log\big(2\sqrt{\log\log x}\big)\right) < \log x$$

for $x > x_0$. By the Montgomery–Vaughan sieve estimates [4], the number of primes $p \le x$ such that $p \equiv 1 \pmod d$ is

$$\le \frac{2x}{\phi(d)\log(x/d)} < \frac{3x}{\phi(d)\log x} \ll \frac{x\log\log d}{d\log x} \ll \frac{x\log\log\log x}{d\log x},$$

where we used the minimal order $\phi(d) \gg d/\log\log d$ of the Euler function and the fact that $d < \log x$. Note that $d > y^k \ge y^{(\pi-4)/5}$ and there are

$$\binom{\pi}{k} < 2^\pi$$

ways to choose the primes $q_1, \ldots, q_k$; hence, d. Thus, the number of such primes $p \le x$ is

$$\le \binom{\pi}{k}\frac{1}{y^{(\pi-4)/5}}\left(\frac{x\log\log\log x}{\log x}\right) \ll \frac{x}{\log x}\left(\left(\frac{32}{y}\right)^{\pi/5} y^{4/5}\log\log\log x\right).$$

Since $y^{4/5}\log\log\log x < y$, $\pi > 25$, and $y > 32$ for $x > x_0$, the factor in parenthesis is

$$\leq \left(\frac{32}{y}\right)^{25/5} y = \frac{2^{25}}{y^4} = \frac{2^{25}}{(\log\log x)^2}.$$

Hence, we get that

$$\#\mathscr{P}_{b,1}(x) \ll \frac{x}{(\log x)(\log\log x)^2}.$$

Case 2. Assume $p-1$ is divisible by less than $\pi/5$ primes in $(y, 2y)$.

Let $\ell := \lfloor 4\pi/5 \rfloor$. Then there exist $q_1 < \cdots < q_\ell$ in $(y, 2y)$ such that q_i is coprime to $p-1$ for $i = 1, \ldots, \ell$. Let $\mathscr{P}_{b,2}(x)$ be the set of such primes p. By the argument preceding Case 1, each one of the numbers $D_{b,q_i} > 1$ is a quadratic residue modulo p. Consider the field extension

$$\mathbb{K} = \mathbb{Q}\big[\sqrt{D_{b,q_i}} : 1 \leq i \leq \ell\big].$$

Since $\gcd(M_{b,m_1}, M_{b,m_2}) = M_{b,\gcd(m_1,m_2)}$, it follows that D_{b,q_i} and D_{b,q_j} are coprime for all $i \neq j$. In particular, the elements of $\{D_{b,q_i} : 1 \leq i \leq \ell\}$ are multiplicatively independent so the Galois group of $\mathbb{K}$ over $\mathbb{Q}$ is 2-elementary of cardinality 2^ℓ. The prime p has the property that each D_{b,q_i} is a quadratic residue, so its Frobenius is the identity element. Thus, by the Chebotarev density theorem, the density of such primes is $\mathrm{li}(x)/2^\ell$, except that there is some error term which we need to control. This we can do with the Lagarias–Odlyzko theorem [2]. We mention that there are many recent improvements of this theorem, but they are not needed for our purpose. Indeed, the Lagarias–Odlyzko theorem says that if $d_{\mathbb{K}}$ and $\Delta_{\mathbb{K}}$ denote the degree and discriminant of $\mathbb{K}$, then provided $x \geq \exp(10 d_{\mathbb{K}}(\log \Delta_{\mathbb{K}})^2)$, we have

$$\left|\pi_1(x) - \frac{\mathrm{li}(x)}{2^\ell}\right| < \frac{\mathrm{li}(x^{\beta_0})}{2^\ell} + c_2 x \exp\left(-c_3\sqrt{\frac{\log x}{d_{\mathbb{K}}}}\right), \tag{3}$$

where c_2, c_3 are absolute constants and $\pi_1(x)$ is the number of primes $p \leq x$ which split completely in $\mathbb{K}$ (so for which the Frobenius is the identity). Here, one can take $\beta_0 = 1$. For us, $d_{\mathbb{K}} = 2^\ell < \exp(\sqrt{\log\log x})$ for large x. Note that

$$D_{b,q_i} < b^{q_i} < b^{2y} = \exp\big(c_4\sqrt{\log\log x}\big) \quad \text{for } x > x_0,$$

with $c_4 = 2\log b$, and that $\mathbb{K}$ is the splitting field of the polynomial

$$f_{q_1,\ldots,q_\ell}(X) = \prod_{i=1}^{\ell}(X^2 - D_{b,q_i})$$

of degree $d = 2\ell$. Lemma 1 in [1] shows that

$$\Delta_{\mathbb{K}} \leq M^{d(d-1)d!/2},$$

where

$$M = \max\big\{\big|\sqrt{D_{b,q_i}} - \sqrt{D_{b,q_j}}\,\big| : 1 \leq i \leq j \leq \ell\big\} \leq 2b^y$$

is the maximum of the absolute value of the distance between any two roots of $f_{q_1,\ldots,q_\ell}(X)$. It follows that

$$\Delta_{\mathbb{K}} < (2b^y)^{d!d(d-1)/2} \leq \exp(c_4\sqrt{\log\log x})^{(d/e)^d d^3} < \exp\big(c_4\sqrt{\log\log x}\big)^{d^d} \quad \text{for } x > x_0.$$

Thus,

$$(\log \Delta_{\mathbb{K}})^2 < d^{2d} c_4^2 \log\log x = (2\ell)^{4\ell} c_4^2 \log\log x < 2^{8\pi \log \pi} c_4^2 \log\log x < \sqrt{\log x} \quad \text{for } x > x_0.$$

Since $d_{\mathbb{K}} < \exp(\sqrt{\log\log x}) < 0.1\sqrt{\log x}$ also holds for $x > x_0$, it follows that $x > \exp(10 d_{\mathbb{K}} (\log \Delta_{\mathbb{K}})^2)$ holds for $x > x_0$. It remains to show that the right–hand side of (3) is $O(\mathrm{li}(x)/2^\ell)$. Well, this is clear for the first term. As for the second term, we have

$$\sqrt{\frac{\log x}{d_{\mathbb{K}}}} = \sqrt{\frac{\log x}{2^\ell}} > (\log x)^{1/4} \quad \text{for } x > x_0,$$

and certainly $2^\ell \log x < \exp\bigl(\sqrt{\log\log x}\,\bigr) \log x = o\bigl(\exp((\log x)^{1/4})\bigr)$ holds as $x \to \infty$. So, the second term in the right–hand side of (3) is

$$\ll x \exp\bigl(-c_3 (\log x)^{1/4}\bigr) = o\left(\frac{x}{2^\ell \log x}\right) \quad \text{as } x \to \infty.$$

Hence, for $x > x_0$, we get

$$\pi_1(x) \le \frac{3\,\mathrm{li}(x)}{2^\ell} \ll \frac{x}{(\log x) 2^\ell}.$$

We now sum up over all the possibilities for $q_1, \ldots, q_\ell$, getting that

$$\#\mathscr{P}_{b,2}(x) \ll \binom{\pi}{\ell} \frac{x}{(\log x) 2^\ell}.$$

Note that $\ell = \lfloor \pi - \pi/5 \rfloor \ge \pi - k - 1$. Since we have the estimates

$$k = \frac{\pi}{5} + O(1) \quad \text{and} \quad \ell = \frac{4\pi}{5} + O(1),$$

we get using $(k+1)! \ge ((k+1)/e)^{k+1}$ that

$$\begin{aligned}
\binom{\pi}{\ell} \le \binom{\pi}{k+1} &\le \frac{\pi^{k+1}}{(k+1)!} \\
&\le \exp\left((k+1)\log\pi - (k+1)\log\left(\frac{k+1}{e}\right)\right) \\
&= \exp\left((k+1)\log\left(\frac{e\pi}{k+1}\right)\right) = \exp\bigl((c_5 + o(1))\pi\bigr),
\end{aligned}$$

where $c_5 := 0.2 \log(5e) = 0.52188\ldots$. Thus, we get that the above binomial coefficient is at most $\exp(0.53\pi)$ for $x > x_0$. Since also

$$2^\ell = \exp(\ell \log 2) = \exp\bigl(\bigl(\tfrac{4}{5}\pi + O(1)\bigr)\log 2\bigr) \gg \exp(c_6 \pi),$$

where $c_6 := 0.8 \log 2 = 0.554518\ldots$, we get that $2^\ell \ge \exp(0.55\pi)$ for $x > x_0$. Putting these together, we get that

$$\#\mathscr{P}_{b,2}(x) \ll \frac{x}{\log x} \exp\bigl((0.53 - 0.55)\pi\bigr) = \frac{x}{(\log x)\exp(0.02\pi)} \ll \frac{x}{(\log x)(\log\log x)^2} \quad \text{for } x > x_0. \quad \square$$

Acknowledgement

We thank the referee for suggestions which improved the quality of our paper.

References

[1] W. D. Banks, F. Luca, I. E. Shparlinski, and H. Stichtenoth, "On the value set of $n!$ modulo a prime", *Turkish J. Math.* **29**:2 (2005), 169–174.

[2] J. C. Lagarias and A. M. Odlyzko, "Effective versions of the Chebotarev density theorem", pp. 409–464 in *Algebraic number fields*: *L-functions and Galois properties* (Durham,1975), edited by A. Fröhlich, Academic, London, 1977.

[3] W. Ljunggren, "Einige Sätze über unbestimmte Gleichungen von der Form $(x^n-1)/(x-1)=y^q$", *Norsk Mat. Tidsskr.* **25** (1943), 17–20.

[4] H. L. Montgomery and R. C. Vaughan, "The large sieve", *Mathematika* **20** (1973), 119–134.

[5] T. Nagel, "Note sur l'équation indéterminée $(x^n-1)/(x-1)=y^q$", *Norsk Mat. Tidsskr.* **2** (1920), 75–78.

[6] T. Nagel, "Des équations indeterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$", *Norsk Mat. Forenings Skr.* (1) **2** (1921), 1–14.

[7] A. Witno, "Hypothetical elite primes for Mersenne numbers and repunits", *J. Integer Seq.* **24**:1 (2021), art. id 21.1.7.

ADEL ALAHMADI: analahmadi@kau.edu.sa
Research Group in Algebraic Structures and Applications, King Abdulaziz University, Jeddah, Saudi Arabia

FLORIAN LUCA: florian.luca@wits.ac.za
School of Mathematics, University of the Witwatersrand, Johannesburg, South Africa

and

Max Planck Institute for Software Systems, Saarbücken, Germany

and

Centro de Ciencias, Matemáticas UNAM, Morelia, Mexico