Journal of Integer Sequences, Vol. 13 (2010),
Article 10.1.7

On a Compositeness Test for $(2^p + 1)/3$

Pedro Berrizbeitia
Departmento de Matemáticas Pura y Aplicada
Universidad Simón Bolívar
Caracas, Venezuela
pedrob@usb.ve

Florian Luca
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán
México
fluca@matmor.unam.mx

Ray Melham
Department of Mathematical Sciences
University of Technology, Sydney
PO Box 123
Broadway, NSW 2007
Australia
ray.melham@uts.edu.au

Abstract

In this note, we give a necessary condition for the primality of $(2^p + 1)/3$.

1 Introduction

Let p be an odd prime and $M_p := 2^p - 1$. For $n \geq 0$ define the sequence $\{S_n\}_{n\geq 0}$ by

$$\begin{aligned} S_0 &= 4, \\ S_{k+1} &= S_k^2 - 2, \qquad k \geq 0. \end{aligned}$$

The celebrated Lucas-Lehmer test states:

Theorem 1. *M_p is prime if and only if $S_{p-2} \equiv 0 \pmod{M_p}$.*

The numbers M_p have interested experts and non-experts throughout history. See [7] for an interesting mathematical and historical account. These numbers have been a popular focus among those searching for large primes because of their unique set of convenient properties for primality testing, the most important of these being the Lucas-Lehmer test, given in Theorem 1. Indeed, via Lucas-Lehmer test, the determination of the primality of M_p is achieved through the calculation of $p-2$ ($< \log M_p$) squares modulo M_p. Furthermore, the reduction of a $2p$-bit integer modulo M_p is very fast compared to the reduction modulo any other number of a similar size.

Observe that $M_p = \phi_p(2)$, where $\phi_p(X)$ is the p-th cyclotomic polynomial. In this paper, we look at primes of the form

$$N_p := \phi_p(-2) = \frac{2^p+1}{3}.$$

For p a prime, the family of numbers $\{N_p\}_{p\geq 3}$ shares some of the properties that make the numbers $\{M_p\}_{p\geq 3}$ interesting to searchers of large primes. For instance, if N_p is prime, then p must be a prime. Additionaly, divisors of N_p are congruent to 1 modulo $2p$, an observation that helps in the search for small prime divisors of N_p. Furthermore, Melham proved the following theorem (see Theorem 7 in [5]), to which we will refer as Melham's probable prime test for N_p.

Theorem 2. *Let p be an odd prime. Define the sequence $\{S_n\}_{n\geq 0}$ by*

$$\begin{aligned} S_0 &= 6, \\ S_{k+1} &= S_k^2 - 2, \qquad k \geq 0. \end{aligned}$$

If N_p is prime then $S_{p-1} \equiv -34 \pmod{N_p}$.

Similar congruences involving Fibonacci numbers and more general Lucas sequences instead of only Mersenne numbers appear in [1] and [3].

It is easy to see that the reduction of a $2p$-bit number modulo N_p is also very fast. However, it is not known whether the numbers $\{N_p\}_{p\geq 3}$ have a very important property enjoyed by the numbers $\{M_p\}_{p\geq 3}$. Specifically, it is not known if $S_{p-1} \equiv -34 \pmod{N_p}$ implies that N_p is prime.

The numbers $\{N_p\}_{p\geq 3}$ were studied by Bateman, Selfridge, and Wagstaff, Jr. [2] who proposed the following conjecture.

Conjecture 3. *If two of the following statements about an odd positive integer p are true, then the third one is also true.*

- *$p = 2^k \pm 1$ or $p = 4^k \pm 3$;*
- *M_p is prime;*
- *N_p is prime.*

Currently, there are forty known primes/probable primes N_p, sometimes called Wagstaff primes/PRP. See, for example, [8]. Probable primes N_p can be discovered via any of the known pseudoprime tests. Examples of such tests are the strong pseudoprime test (or the Miller-Rabin test [6]), and the Grantham test [4]. They can also be discovered with the use of Melham's probable prime test, given in Theorem 2 above. This test has the computational advantadge of involving the computation of only $p-1$ modular squares, the subtraction of 2 in each step being neglected.

Melham's probable prime test for N_p can be derived by the application of a Frobenius test to $1+\sqrt{2}$ in the finite field $\mathbb{K} := \mathbb{Z}[\sqrt{2}]/N_p$. The application of the Frobenius test is equivalent to the determination of the quadratic character of $1+\sqrt{2}$ in $\mathbb{K}$.

Similarly, we will see that, by the application of a Frobenius test to $2+\sqrt{2}$, one can obtain the following weaker variant of Melham's test: If N_p is prime, then the sequence given by

$$\begin{aligned} R_0 &= 4, \\ R_{k+1} &= R_k^2 - 2^{2^k+1}, \qquad k \geq 0, \end{aligned}$$

satisfies $R_{p-1}^2 \equiv 64 \pmod{N_p}$ (see Lemma 5 below).

Curiously, we noticed experimentally that whenever N_p is prime, then $R_{p-1} \equiv 8 \pmod{N_p}$ holds. The object of this paper is to show that this is indeed the case. Our proof hinges on the determination of the biquadratic character of $2+\sqrt{2}$ in $\mathbb{K}$, a problem that we consider to be interesting in its own right.

2 The Main Result

Theorem 4. *If $p > 3$ is prime, and N_p is prime, then $R_{p-1} \equiv 8 \pmod{N_p}$.*

Let $\alpha := 2+\sqrt{2}$ and $\beta := 2-\sqrt{2}$. It is easy to see, by induction on n, that the formula

$$R_n = \alpha^{2^n} + \beta^{2^n} \qquad \text{holds for all } n \geq 0. \tag{1}$$

Since $p > 3$, it follows easily that $N_p \equiv 3 \pmod{8}$. In particular,

$$\left(\frac{-1}{N_p}\right) = \left(\frac{2}{N_p}\right) = -1, \tag{2}$$

where, as usual, for integers a, and $q \geq 3$ odd, we write $\left(\frac{a}{q}\right)$ for the Jacobi symbol of a with respect to q.

We start by giving a short proof of a somewhat weaker congruence using nothing else but the properties of the Frobenius automorphism.

Lemma 5. *Let $p > 3$ be prime. If N_p is prime, then $R_{p-1}^2 \equiv 64 \pmod{N_p}$.*

Proof. Assume that $q := N_p$ is prime. Again let $\mathbb{K} := \mathbb{F}_q[\sqrt{2}]$. By equation (2), it follows that $\mathbb{K}$ is a finite field with q^2 elements. Since $\alpha \notin \mathbb{F}_q$, we have that $\alpha^q = \beta$ in $\mathbb{K}$. Then $\alpha^{3q} = \beta^3$. Since $3q = 2^p + 1$, it follows that

$$\alpha^{2^p} = \beta^3 \alpha^{-1}.$$

Conjugating the above relation, we get

$$R_p = \alpha^{2^p} + \beta^{2^p} = \beta^3\alpha^{-1} + \alpha^3\beta^{-1} = \frac{\alpha^4+\beta^4}{\alpha\beta} = 68,$$

where we have used the relations

$$\alpha^4 = 68 + 48\sqrt{2}, \qquad \beta^4 = 68 - 48\sqrt{2}, \qquad \alpha\beta = 2.$$

However, again by formula (2), we have

$$2^{(q-1)/2} = -1 \ \text{ in } \ \mathbb{F}_q.$$

Since $(q-1)/2 = (2^{p-1}-1)/3$, we conclude that

$$2^{2^{p-1}-1} = -1. \tag{3}$$

Thus, $2^{2^{p-1}+1} = -4$. The desired relation now follows because

$$R_{p-1}^2 = R_p + 2^{2^p+1} = 68 - 4 = 64,$$

which is what we wanted. □

Let us now go to the proof of Theorem 4. We shall assume that $p > 3$, since for $p = 3$ the congruence can be verified directly. We keep the previous notations. Let i be a fixed square-root of -1 in $\mathbb{K}$. Put

$$\gamma := 1 + i + \sqrt{2}.$$

Let

$$\sigma := 1 + i - \sqrt{2} \qquad \text{and} \qquad \tau := 1 - i + \sqrt{2}.$$

Note that none of the elements $\gamma,\ \sigma,\ \tau$ is in $\mathbb{F}_q$. Indeed, assume say, that $\tau \in \mathbb{F}_q$. Then by writing $-i + \sqrt{2} = a$ with some $a \in \mathbb{F}_q$, rearranging the above relation and squaring it, we get

$$-1 = (-i)^2 = (a - \sqrt{2})^2 = a^2 - 2a\sqrt{2} + 2,$$

so that $a\sqrt{2} \in \mathbb{F}_q$, which is possible only if $a = 0$. However, with $a = 0$ the above relation becomes $-1 = 2$, which is false because $q = N_p > 3$.

Observe now that

$$\sigma\tau = 1 - (i - \sqrt{2})^2 = 2i\sqrt{2} = 2\sqrt{-2} \in \mathbb{F}_q,$$

where the last relation follows from the fact that -2 is a quadratic residue modulo q. Thus, $(\sigma\tau)^{q-1} = 1$. Since $(q^2-1)/4 = (q-1)((q+1)/4)$ is a multiple of $q-1$, we see that $(\sigma\tau)^{(q^2-1)/4} = 1$, which can be rewritten as

$$(\gamma\tau)^{(q^2-1)/4} = (\gamma\sigma)^{(q^2-1)/4} \left(\tau^2\right)^{(q^2-1)/4}. \tag{4}$$

Now,

$$\gamma\sigma = (1+i)^2 - 2 = 2(i-1), \qquad \text{and} \qquad \gamma\tau = (1+\sqrt{2})^2 - i^2 = 2\alpha. \tag{5}$$

Observe that $2(i-1) = -2\sqrt{2}\omega$, where $\omega = (1-i)/\sqrt{2}$ is a root of unity of order 8. Since $p \geq 5$, it follows that $q \equiv 3^{-1} \equiv 11 \pmod{32}$, which implies easily that $(q^2-1)/4 \equiv -2 \pmod 8$. Thus, the left side of formula (4) is

$$(\gamma\sigma)^{(q^2-1)/4} = (-2\sqrt{2})^{(q^2-1)/4}\omega^{(q^2-1)/4} = (-1)^{(q^2-1)/4}2^{3(q^2-1)/8}\omega^{-2} = -i. \tag{6}$$

Next, observe that

$$(\tau^2)^{(q^2-1)/4} = \left(\tau^{q+1}\right)^{(q-1)/2}.$$

By Frobenius, we have that $\tau^{q+1} = \tau^q\tau = \sigma\tau = 2i\sqrt{2}$. Thus,

$$(\tau^2)^{(q^2-1)/4} = (2i\sqrt{2})^{(q-1)/2} = i^{(q-1)/2}2^{(q-1)/2}(\sqrt{2})^{(q-1)/2} = -i(\sqrt{2})^{(q-1)/2}, \tag{7}$$

where we have used the fact that $(q-1)/2 \equiv 1 \pmod 4$, which follows easily from the fact that $q \equiv 11 \pmod{32}$. Inserting (6) and (7) into (4), and using also (5), we obtain

$$(2\alpha)^{(q^2-1)/4} = (-i)(-i)(\sqrt{2})^{(q-1)/2} = -(\sqrt{2})^{(q-1)/2}.$$

Using now $2^{(q^2-1)/4} = (2^{q-1})^{(q+1)/4} = 1$, and $\alpha^{q-1} = \alpha^q\alpha^{-1} = \beta/\alpha$, we deduce that

$$\left(\frac{\beta}{\alpha}\right)^{(q+1)/4} = \alpha^{(q^2-1)/4} = (2\alpha)^{(q^2-1)/4} = -(\sqrt{2})^{(q-1)/2}.$$

Now, $(q+1)/4 = (2^p+4)/12 = (2^{p-2}+1)/3$. Thus,

$$\left(\frac{\beta}{\alpha}\right)^{2^{p-2}} = -(\sqrt{2})^{3(q-1)/2}\left(\frac{\alpha}{\beta}\right).$$

Applying the Frobenius automorphism, and summing the resulting relations, we arrive at

$$\left(\frac{\beta}{\alpha}\right)^{2^{p-2}} + \left(\frac{\alpha}{\beta}\right)^{2^{p-2}} = -(\sqrt{2})^{3(q-1)/2}\left(\frac{\alpha}{\beta} - \frac{\beta}{\alpha}\right).$$

In the line immediately above, the left side is $R_{p-1}/(\alpha\beta)^{2^{p-2}} = R_{p-1}/2^{2^{p-2}}$. The right side is

$$-(\sqrt{2})^{3(q-1)/2}\left(\frac{\alpha^2-\beta^2}{\alpha\beta}\right) = -(\sqrt{2})^{3(q-1)/2}4\sqrt{2} = -2^{(3q+7)/4}.$$

Since $(3q+7)/4 = 2^{p-2}+2$, we obtain

$$\frac{R_{p-1}}{2^{2^{p-2}}} = -2^{2^{p-2}+2},$$

which finally leads to $R_{p-1} = -2^{2^{p-1}+2}$. Using (3), we obtain the desired result.

3 Acknowledgements

We thank the anonymous referees and Professor Jeffrey Shallit for useful remarks and for suggesting some references. This work was done while the first two authors attended the *Terceras Jornadas de Teoria de Números* in Salamanca, Spain in July of 2009. They thank the organizers of this event for the opportunity to attend this meeting and for financial support and to Javier Cilleruelo for enlightening conversations. We also thank the Astronaut who inspired the current approach to the problem. P. B. was also supported in part by the Decanato de Investigaciones from the Universidad Simón Bolívar, and F. L. was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508.

References

[1] G. Andrews, Some formulae for the Fibonacci sequence with generalizations, *Fibonacci Quart.* **7** (1969), 113–130.

[2] P. T. Bateman, J. L. Selfridge, and S. S. Wagstaff, The new Mersenne conjecture, *Amer. Math. Monthly*, **96** (1989), 125–128.

[3] C. N. Beli, Two conjectures by Zhi-Hong Sun, *Acta Arith.* **137** (2009), 99–131.

[4] J. Grantham, A probable prime test with high confidence *J. Number Theory* **72** (1998), 32–47.

[5] R. S. Melham, Probable prime tests for generalized Mersenne numbers, *Bol. Soc. Mat. Mexicana* **14** (2008), 7–14.

[6] M. O. Rabin, Probabilistic algorithm for testing primality, *J. Number Theory* **12** (1980), 128–138.

[7] H. Williams, *Edouard Lucas and Primality Testing*, Canadian Math. Soc. Monographs **22**, Wiley, New York, 1998.

[8] Wagstaff prime, Wikipedia entry, http://en.wikipedia.org/wiki/Wagstaff_prime .

2000 *Mathematics Subject Classification*: Primary 11Y11; Secondary 11A41, 11A51.
Keywords: primality, Wagstaff primes.

(Concerned with sequence A000979.)

Received November 16 2009; revised version received January 14 2010. Published in *Journal of Integer Sequences*, January 18 2010.

Return to Journal of Integer Sequences home page.