ON SIERPIŃSKI NUMBERS OF THE FORM $\varphi(N)/2^n$

Marcos J. González
Departamento de Matemáticas Puras y Aplicadas, Universidad Simón Bolívar, Sartenejas, Caracas, Venezuela
mago@usb.ve

Florian Luca
School of Mathematics, University of the Witwatersrand, Wits, South Africa
florian.luca@wits.ac.za

V. Janitzio Mejía Huguet
Departamento de Ciencias Básicas, Universidad Autónoma Metropolitana-Azcapotzalco, Azcapotzalco DF, México
vjanitzio@gmail.com

Received: 9/8/14, Revised: 8/16/16, Accepted: 12/11/16, Published: 12/29/16

Abstract

Let φ denote the Euler φ function. We prove that for all $n \geq s \geq 2$ there exist infinitely many Sierpiński numbers k such that $2^n k = \varphi(N)$ holds with some positive integer N that has exactly s distinct prime factors. This extends previous work of the last two authors.

1. Introduction

An odd positive integer k is called a Sierpiński number if $k2^n + 1$ is composite for every positive integer n. These numbers are named after Wacław Sierpiński who discovered their existence in 1960 (see [10]). In 1962, John Selfridge found the Sierpiński number $k = 78557$, which is conjectured to be the smallest Sierpiński number (see [9]). This number was found by using the method of covering systems of congruences used earlier by Paul Erdős in order to prove that there are infinitely many odd integers not of the form $2^k + p$ with p prime (see [3]). We review this method in Section 2.

If k is a Sierpiński number, then $2^n k \neq q - 1 = \phi(q)$ for any prime q, where φ is the Euler function. In [7, Theorem 1], it is shown that if k is a Sierpiński prime and $2^n k = \varphi(N)$ holds for some positive integers n and N, then k is a Fermat number. It is natural to ask whether or not we can fix both $n \geq 1$ and the number of distinct prime factors s (≥ 2) of N and still obtain infinitely many examples of such Sierpiński numbers k. We shall be interested only in the case when N is odd, because if N is even, then writing $N = 2^a N_1$ with N_1 odd, the equation

$$2^n k = \varphi(N) = \varphi(2^a N_1) = 2^{a-1}\varphi(N_1),$$

yields

$$2^{n-a+1}k = \varphi(N_1),$$

which is a similar problem with a smaller exponent of 2 in the left–hand side. So, we assume that N is odd. Clearly, if N has s distinct prime factors, then $2^s \mid \varphi(N)$, showing that, in order for the equation $2^n k = \varphi(N)$ to hold, it is necessary that $n \geq s$. The following result shows that the answer to the above question is in the affirmative.

Theorem 1. *For all integers $n \geq s \geq 2$ there exist infinitely many Sierpiński numbers such that*

$$2^n k = \varphi(N)$$

holds with some positive integer N having exactly s distinct prime factors.

The case $n = s = 2$ was proved in [7, Theorem 1, (i)]. For more results on Sierpiński numbers, see [2, 5, 8]. We hope our work will inspire further work on Riesel numbers with a fixed number of prime factors, or numbers which are simultaneously Riesel and Sierpińsky with a fixed number of prime factors, etc.

2. Covering Systems

Typically, the way to find Sierpiński numbers is the following. Assume that $\{(a_j, b_j, p_j)\}_{j=1}^{t}$ are triples of positive integers with the following properties:

cov for each integer n there exists $j \in \{1, 2, \ldots, t\}$ such that $n \equiv a_j \mod b_j$;

ord $p_1, \ldots, p_t$ are distinct prime numbers such that $p_j | 2^{b_j} - 1$ for all $j = 1, 2, \ldots, t$.

Next, one creates Sierpiński numbers k by imposing that

$$2^{a_j} k \equiv -1 \mod p_j \qquad \text{for} \qquad j = 1, 2, \ldots, t. \tag{1}$$

Since the primes p_j are all odd for $j = 1, 2, \ldots, t$, it follows that for each j, the above congruence (1) is solvable and puts k into a certain arithmetic progression modulo p_j. The fact that the congruences (1) are simultaneously solvable for all $j = 1, 2, \ldots, t$ follows from the fact that the primes $p_1, p_2, \ldots, p_t$ are distinct via the Chinese Remainder Theorem. Every odd positive integer k in the resulting arithmetic progression has the property that $k2^n+1$ is always a multiple of one of the numbers p_j for $j=1,2,\ldots,t$, and if

$$k>\max\{p_j\colon j=1,2,\ldots,t\},$$

then $k2^n+1$ cannot be prime.

The original system of triples considered by Sierpiński [10] (see also [4]) is

$$\{(1,2,3),(2,4,5),(4,8,17),(8,16,257),(16,32,65537),(32,64,641),\\ (0,64,6700417)\}. \tag{2}$$

In the following lemma, we exhibit a family of systems generalizing the above system of triples.

Lemma 1. *Given a composite Fermat number F_m, there exists a covering system of congruences $\{(a_j,b_j,p_j)\}_{j=0}^{m+1}$, such that the solution k of the system of congruences $2^{a_j}k\equiv -1 \mod p_j$, $j=0,1,\ldots,m+1$, has $k\equiv 1 \pmod{p_j}$ for $j=1,\ldots,m$ and $k\equiv -1 \pmod{p_{m+1}}$.*

The proof of the above lemma can be found in Section 4.

3. Proof of Theorem 1

Choose some m such that $F_m=2^{2^m}+1$ is a Fermat number having at least two distinct prime factors. For example, by a recent computation, $m=2747497$ has this property because $p=57\cdot 2^{2747499}+1 \mid F_m$, and certainly $F_m>p$. We fix n and search for solutions to the equation

$$2^n k=\varphi(N), \tag{3}$$

where

$$N=r^\ell q_1\cdots q_{s-1} \tag{4}$$

with $r,q_1,\ldots,q_{s-1}$ primes and ℓ some suitable positive integer. For this, we first write $n=1+\lambda_1+\cdots+\lambda_{s-1}$ with positive integers $\lambda_1,\ldots,\lambda_{s-1}$, which is possible since $n\ge s$. We fix $j=0,\ldots,m+1$, and choose

$$\frac{q_i-1}{2^{\lambda_i}}\equiv 1 \mod p_j \qquad (i=1,\ldots,s-1).$$

These lead to $q_i\equiv 2^{\lambda_i}+1 \mod p_j$, which is a valid choice (namely the congruence class is nonzero) as long as $p_j\nmid 2^{\lambda_i}+1$. In the unfortunate case when $p_j\mid 2^{\lambda_i}+1$, we change our mind and ask instead that

$$\frac{q_i-1}{2^{\lambda_i}}\equiv -1 \mod p_j,$$

which leads to $q_i \equiv -(2^{\lambda_i} - 1) \mod p_j \equiv 2 \mod p_j$. This fixes nonzero congruence classes of $q_1, \ldots, q_{s-1}$ modulo p_j for $j = 0, \ldots, m+1$. We also choose $q_i \equiv 1 + 2^{\lambda_i} \pmod{2^{\lambda_i+1}}$, which ensure that $(q_i - 1)/2^{\lambda_i}$ is an odd integer for $i = 1, \ldots, s-1$. By the Chinese Remainder theorem, this fixes the congruence classes of q_i modulo $2^{\lambda_i+1} p_0 \cdots p_{m+1}$ and the fact that one may choose $s-1$ distinct primes in the above congruence classes is a consequence of Dirichlet's theorem on primes in arithmetical progressions. Now it remains to comment on r and ℓ. Equation (3) yields

$$2^n k = \varphi(N) = r^{\ell-1}(r-1)(q_1 - 1) \cdots (q_{s-1} - 1),$$

which implies

$$k = \frac{r^{\ell-1}(r-1)}{2} \prod_{i=1}^{s-1} \left(\frac{q_i - 1}{2^{\lambda_i}} \right). \tag{5}$$

Reduced modulo p_j, the left–hand side is ± 1 and the product in the right hand side over $i = 1, \ldots, s-1$ is also ± 1. Thus, it remains to show that we can find r and ℓ such that each of the two congruences

$$\frac{r^{\ell-1}(r-1)}{2} \equiv \pm 1 \mod p_j \tag{6}$$

has a nonzero solution $r_j \mod p_j$. An obvious choice is to choose

$$\ell = \mathrm{lcm}[p_0 - 1, \ldots, p_{m+1} - 1].$$

Then the above equations via Fermat's little theorem imply that congruences (6) become $(r-1)/2r \equiv \pm 1 \mod p_j$, leading to $r \equiv -1, 3^{-1} \mod p_j$. This works except when $j = 0$, since when $j = 0$ we have $p_0 = 3$, and we cannot invert 3 modulo p_0. In this case $k \equiv 1 \mod 3$, and $(q_i - 1)/2^{\lambda_i} \equiv 1 \mod 3$ for all $i = 1, \ldots, s-1$, except when λ_i is odd (case in which $3 \mid 2^{\lambda_i} + 1$), in which case the sign in the right–hand side of the last congruence above is -1. Thus, the unsolvable congruence

$$\frac{r-1}{2r} \equiv -1 \mod 3$$

is a consequence of relation (5) and of our previous choices only when there are exactly an odd number of $i \in \{1, \ldots, s-1\}$ such that λ_i is odd. Since $\sum_{i=1}^{s-1} \lambda_i = n - 1$, it follows that our construction so far fails when n is even but is successful when n is odd.

So, from now on we only work with even n. If $n \geq s+2$, then we write $3 + \sum_{i=1}^{s-1} \lambda_i = n$ with some positive integers $\lambda_1, \ldots, \lambda_{s-1}$. We take $\ell = 1$, write

$$k = \frac{(r-1)}{8} \prod_{i=1}^{s-1} \left(\frac{q_i - 1}{2^{\lambda_i}} \right),$$

and choose $q_1, \ldots, q_{s-1}$ as before. We are then led to solving

$$\frac{r-1}{8} \equiv \pm 1 \mod p_j \qquad \text{for} \qquad j = 0, \ldots, m+1. \tag{7}$$

The solutions are $r \equiv -7, 9 \mod p_j$, and these nonzero modulo p_j except when $j = 0$ and the sign in the right–hand side of the above congruence (7) is 1 (note that 7 is not one of the primes p_j for $j = 0, \ldots, m+1$). However, when $j = 0$, since n is even, it follows that $n - 3$ is odd, therefore there are exactly an odd number of $i \in \{1, \ldots, s-1\}$ such that λ_i is odd. So, at $j = 0$, the congruence to be solved is in fact $(r-1)/8 \equiv -1 \mod 3$, whose solution is the convenient $r \equiv 2 \mod 3$. We now choose $r \equiv 9 \mod 16$ to insure that $(r-1)/8$ is odd, leading to $r \equiv 41 \mod 48$, which is acceptable. Then we find one (or infinitely many) such r using Dirichlet's theorem on primes in arithmetical progressions.

Finally, we are left with the cases in which n is even and $n = s,\ s+1$. Suppose that $n = s$. Then $\lambda_1 = \cdots = \lambda_{s-1} = 1$, we take $\ell = 1$, and we work with

$$k = \left(\frac{r-1}{2}\right) \prod_{j=1}^{s-1} \left(\frac{q_j - 1}{2}\right).$$

Since n is even, it follows that s is even. So, when $j = 0$, modulo $p_0 = 3$, we can take $r \equiv q_i \equiv 2 \mod 3$ for $i = 1, \ldots, s-1$ and we obtain $k \equiv 1 \mod 3$, as desired. For $j \geq 1$, we need to solve $(r-1)/2 \equiv \pm 1 \mod p_j$, which has the nonzero solutions $-1,\ 3 \mod p_j$.

Suppose finally that $n = s+1$. We then take $\lambda_1 = \cdots = \lambda_{s-1} = 1$, $\ell = 1$, and work with

$$k = \frac{(r-1)}{4} \prod_{i=1}^{s-1} \left(\frac{q_i - 1}{2}\right).$$

For $j = 0$, since n is even, we get that s is odd, so $s - 1$ is even. So, we need to solve

$$\frac{r-1}{4} \equiv 1 \mod 3,$$

which leads to the convenient solution $r \equiv 2 \mod 3$. For $j = 1$, we have $p_1 = 5$ and $5 \nmid 2^1 \pm 1$. So, with our choices, we may choose q_i such that $(q_i - 1)/2 \equiv 1 \mod 5$ for all $i = 1, \ldots, s-1$, except for one of them, say the first one, for which we choose $(q_1 - 1)/2 \equiv -1 \mod 5$. This works if $s - 1 \geq 1$, which is our case because $s \geq 2$. Now we only need to solve

$$\frac{r-1}{4} \equiv -1 \mod 5,$$

which has the convenient solution $r \equiv 2 \pmod 5$. Finally, for $j \geq 2$, we need to solve $(r-1)/4 \equiv \pm 1 \mod p_j$, which lead to $r \equiv -3, 5 \mod p_j$ which are both nonzero congruence classes modulo p_j because $j \geq 2$. Now we fix as before congruence classes for q_i modulo 2^{λ_i+1} for $i = 1, \ldots, s-1$ to ensure that the amounts $(q_i - 1)/2^{\lambda_i}$ are odd, as well as for r modulo 8 to ensure that $(r-1)/2$ (when $n = s$) and $(r-1)/4$ (when $n = s+1$) are odd and proceed as before via the Chinese Remainder theorem and Dirichlet's theorem on primes in arithmetical progression to justify the existence of infinitely many primes $r, q_1, \ldots, q_{s-1}$ with all the congruence properties specified above.

This finishes the proof of the theorem.

4. Proof of Lemma 1

It is well-known that F_m cannot be a perfect power of integer exponent larger than 1 of some other integer. Hence, since F_m is not prime, it follows that it has at least two distinct prime factors. We choose for every $j = 0, 1, \ldots, m$ a prime factor p_j of the Fermat number F_j. Since F_m is composite with at least two distinct prime factors, we choose a second prime factor of F_m which we denote by p_{m+1}. Then, we consider the system of triples

$$(a_j, b_j, p_j) = \begin{cases} (2^j, 2^{j+1}, p_j), & \text{if} \quad j \leq m, \\ (0, 2^{m+1}, p_{m+1}), & \text{if} \quad j = m+1. \end{cases} \tag{8}$$

By considering the binary expansion $n = \sum_{i=0}^{\infty} a_i 2^i$ of a positive integer n, we see that either $n \equiv 0 \pmod{2^{m+1}}$, or $n \equiv \sum_{i=0}^{m+1} a_i 2^i \equiv 2^{j_0} \pmod{2^{j_0+1}}$, where j_0 is the smallest index $0 < j \leq m$ for which $a_j \neq 0$. This shows that the system of triples (8) fulfils condition **cov**. On the other hand, the fact that $p_j | F_j = 2^{2^j} + 1$, for $j = 0, 1, \ldots, m$, tells us that $2^{2^j} \equiv -1 \pmod{p_j}$. This congruence implies that $2^{2^{j+1}} \equiv 1 \pmod{p_j}$ and consequently $\text{ord}_{p_j}(2) = 2^{j+1}$. Here, $\text{ord}_p(2)$ is the multiplicative order of 2 modulo the odd prime p. Similarly, $\text{ord}_{p_{m+1}}(2) = 2^{m+1}$. The fact that the prime numbers p_j, for $j = 0, 1, \ldots, m, m+1$, are pairwise distinct follows because the orders of 2 modulo these primes are all different except for p_m and p_{m+1} which are distinct as well. Therefore, the system of triples (8) also fulfils condition **ord**. Finally, let us solve for k. For $j = 0, 1, \ldots, m$, we have that $2^{2^j} k \equiv -1 \equiv 2^{2^j} \pmod{p_j}$ and consequently $k \equiv 1 \pmod{p_j}$, while $2^{2^m} k \equiv -1 \equiv -2^{2^m} \pmod{p_m}$ and consequently $k \equiv -1 \pmod{p_{m+1}}$.

This finishes the proof of the lemma.

Acknowledgements. We thank the referee for comments which improved the quality of this paper and for pointing out several useful references. This paper started during a pleasant visit of the first author at the Mathematical Institute of the UNAM in Morelia, Mexico in September of 2009. He thanks the people of this Institute for their hospitality. During the preparation of this paper, V. J. M. H. was supported by Grant UAM-A 2230316.

References

[1] P. Berrizbeitia, J.G. Fernandes, M. J. González, F. Luca, V. J. Mejía Huguet, On Cullen numbers which are both Riesel and Sierpiński numbers, *J. Number Theory* **132** (2012), 2836–2841.

[2] C. K. Caldwell and T. Komatsu, Powers of Sierpinski Numbers Base B, *Integers* **10** (2010), A36, 423–436.

[3] P. Erdös, On integers of the form $2^k + p$ and some related problems, *Summa Brasil. Math.* **2** (1950), 113–123.

[4] M. Filaseta, C. Finch, M. Kozek, On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture, *J. Number Theory* **128** (2008), 1916–1940.

[5] L. Jones and D. White, Sierpiński Numbers in Imaginary Quadratic Fields, *Integers* **12A** (2012), A10.

[6] M. Křížek, F. Luca, L. Somer, 17 *Lectures on Fermat Numbers: From Number Theory to Geometry*, CMS Books in Mathematics, 10, New York, Springer, 2001.

[7] F. Luca and V. J. Mejia Huguet, Some remarks on Sierpiński numbers and related problems, *Bol. Soc. Mat. Mexicana*, **15** (2009), 11–22.

[8] F. Luca, C. G. Moreira and C. Pomerance, On integers which are the sum of a power of 2 and a polynomial value, *Bull. Brazilian Math. Soc.* **45** (2014), 559–574.

[9] Seventeen or bust, `http://www.seventeenorbust.com`.

[10] W. Sierpiński, Sur un problème concernant les nombres $k2^n + 1$, *Elem. Math.* **15** (1960), 73–74.