JTN 2015
Universidad de Valladolid
June 29-July 3, 2015

Acerca de números de Sierpiński que son de la forma $\varphi(N)/2^n$

Marcos J. González[1], Florian Luca[2], V. Janitzio Mejía Huguet[3]

[1] *Universidad Simón Bolívar, Venezuela mago@usb.ve*
[2] *University of the Witwatersrand, South Africa, fluca@matmor.unam.mx*
[3] *Universidad Autónoma Metropolitana, México, vjanitzio@yahoo.com.mx*

Expositor: V. Janitzio Mejía Huguet.

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 [7]). Shortly after, in 1962, John Selfridge found the Sierpiński number $k = 78557$, which is conjectured to be the smallest Sierpiński number (see [6]). 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 [2]). We review this method in Section 1.

Now, if k is a Sierpiński number, it follows that $2^n k \neq q-1$ for any prime q. Since $q-1 = \varphi(q)$, where φ is the Euler function, it makes sense to ask about Sierpiński numbers k such that $2^n k$ is in the image of the Euler function. In this direction it is known the following (see [5, Theorem 1]): *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. On the other hand, there exist infinitely many Sierpiński numbers k such that for each one of them, $2^n k = \varphi(N)$ holds for some positive integers n and N.*

It is natural to ask whether or not we can fix both $n \geq 1$ and the number of distinct prime factors s 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.

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 [5, Theorem 1, (i)].

1 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 $n \equiv a_j b_j$;

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

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

Since the primes p_j are all odd for $j = 1, 2, \ldots, t$, it follows that for each j, the above congruence sier1 is solvable and puts k into a certain arithmetic progression modulo p_j. The fact that the congruences sier1 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

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

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

The original system of triples considered by Sierpiński [7] (see also [3]) 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.

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 $2^{a_j} k \equiv -1 p_j$, $j = 0, 1, \ldots, m+1$, has $k \equiv 1 \pmod{p_j}$ for $j = 1, \ldots, m$ and $k \equiv -1 \pmod{p_{m+1}}$.

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*, Journal of Number Theory, 12 (2012), 2836–2841.

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

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

[4] 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.

[5] F. Luca and V. J. Mejia Huguet, *Some remarks on Sierpiński numbers and related problems*, Boletín de la Sociedad Matemática Mexicana, 15 (2009), 11–22.

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

[7] W. Sierpiński, *Sur un problème concernant les nombres* $k2^n + 1$, Elemente der Mathematik, 15 (1960), 73–74.