A NOTE ON SIERPINSKI NUMBERS

Anatoly S. Izotov
Mining Institute, Novosibirsk, Russia
7 Dostoevsky Str., Apt. 12, Novosibirsk, 630104, Russia
(*Submitted September 1993*)

In [5], W. Sierpinski proved that there are infinitely many odd integers k (Sierpinski numbers) such that $k \cdot 2^n + 1$ is composite for all $n \geq 0$. In his proof, Sierpinski used as a covering set the set of primes $\{3, 5, 17, 257, 641, 65537, 6700417\}$. A "covering set" for any k means here a finite set of primes such that every integer $k \cdot 2^n + 1$, $n \geq 0$, is divisible by at least one of them. There are other covering sets (see [4], [6]). In 1962, J. L. Selfridge (unpublished manuscript) discovered that $\{3, 5, 7, 13, 19, 37, 73\}$ is a covering set for 78557.

In this note, we prove that there are infinitely many Sierpinski numbers of the new kind. We find those k such that $k \cdot 2^n + 1$, for n of the form $n = 4m + 2$, has an easy algebraic decomposition while, for other n, we have the covering set $\{3, 17, 257, 641, 65537, 6700417\}$ from Sierpinski's set.

Theorem 1: Let the positive integer t be any solution of the system of congruences

$$\begin{cases} t \equiv 1 \pmod{2}, \\ t \equiv 1 \text{ or } 2 \pmod{3}, \\ t \equiv 0 \pmod{5}, \\ t \equiv 1, 4, 13, \text{ or } 16 \pmod{17}, \\ t \equiv 1, 16, 241, \text{ or } 256 \pmod{257}, \\ t \equiv 1, 256, 65281, \text{ or } 65536 \pmod{65537}, \\ t \equiv 1, 65536, 6634881, \text{ or } 6700416 \pmod{6700417}, \\ t \equiv 256, 318, 323, \text{ or } 385 \pmod{641}. \end{cases} \tag{1}$$

Then $k = t^4$ is a Sierpinski number.

Proof: By (1),

$$\begin{cases} k \equiv 1 \pmod{2}, \\ k \equiv 1 \pmod{3}, \\ k \equiv 0 \pmod{5}, \\ k \equiv 1 \pmod{17}, \\ k \equiv 1 \pmod{257}, \\ k \equiv 1 \pmod{65537}, \\ k \equiv 1 \pmod{6700417}, \\ k \equiv -1 \pmod{641}. \end{cases} \tag{2}$$

So we have

$$k \cdot 2^{2m+1} + 1 \equiv 0 \pmod{3},$$
$$k \cdot 2^{8m+4} + 1 \equiv 0 \pmod{17},$$
$$k \cdot 2^{16m+8} + 1 \equiv 0 \pmod{257},$$

$$k \cdot 2^{32m+16} + 1 \equiv 0 \pmod{65537},$$
$$k \cdot 2^{64m+32} + 1 \equiv 0 \pmod{6700417},$$
$$k \cdot 2^{64m} + 1 \equiv 0 \pmod{641},$$

for $m \geq 0$. For $n = 4m+2$, we have

$$\begin{aligned} k \cdot 2^n + 1 &= t^4 \cdot 2^{4m+2} + 1 \\ &= 4(t \cdot 2^m)^4 + 1 \\ &= (t^2 \cdot 2^{2m+1} + t \cdot 2^{m+1} + 1)(t^2 \cdot 2^{2m+1} - t \cdot 2^{m+1} + 1). \end{aligned}$$

Since $t > 1$, $t^2 \cdot 2^{2m+1} - t \cdot 2^{m+1} + 1 > 1$ for $m \geq 0$. Therefore, $k \cdot 2^{4m+2} + 1$ is composite for all $m \geq 0$. Note that $k \cdot 2^{4m+2} + 1 \equiv 1 \pmod 5$, so $\{3, 5, 17, 257, 641, 65537, 6700417\}$ is not a covering set for k.

Are there other Sierpinski numbers analogous to Theorem 1?

The problem of determining the least value k_0 of k such that $k \cdot 2^n + 1$ is always composite was posed by Sierpinski [5], again by Guy [2], and was considered in [1] and [3]. The least known k is Selfridge's $k = 78557$ with covering set $\{3, 5, 7, 13, 19, 37, 73\}$. Perhaps k_0 has no covering set.

REFERENCES

1. R. Baillie, G. Cormack, & H. C. Williams. "The Problem of Sierpinski Concerning $k \cdot 2^n + 1$." *Math. Comput.* **37** (1981):229-31; *Corrig. Math. Comp.* **39** (1982):308.
2. R. K. Guy. "Some Unsolved Problems." In *Computers in Number Theory*, pp. 415-22. Ed. A. O. L. Atkin and B. J. Brich. New York: Academic Press, 1971.
3. G. Jeaschke. "On the Smallest k Such That All $k \cdot 2^N + 1$ Are Composite." *Math. Comput.* **40.101** (1983):361-64.
4. J. L. Selfridge. "Solution to Problem 4995." *Amer. Math. Monthly* **70** (1963):101.
5. W. Sierpinski. "Sur un probleme concernant les nombres $k \cdot 2^n + 1$." *Elem. Math.* **15** (1960): 73-74; *Corrig.* **17** (1962):85.
6. R. G. Stanton. "Future Results on Covering Integers of the Form $1 + k \cdot 2^N$ by Primes." *Lecture Notes in Math.* **884** (1980):107-14.

AMS Classification Numbers: 11B25, 11B83