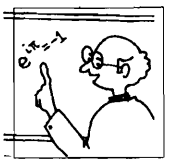
Classroom



In this section of *Resonance*, we invite readers to pose questions likely to be raised in a classroom situation. We may suggest strategies for dealing with them, or invite responses, or both. "Classroom" is equally a forum for raising broader issues and sharing personal experiences and viewpoints on matters related to teaching and learning science.

Shailesh A Shirali
Amber Valley Residential School, Chikmagalur
Karnataka 577 101, India.
Email:
Shailesh_Shirali@rediffmail.com

The Sierpiński Problem

In this article, we describe briefly a number-theoretic problem first studied by Sierpiński, now known as the *Sierpiński problem*. The problem remains open.

Waclav Sierpiński (1882-1969)

The name of Waclav Sierpiński will surely be familiar to all lovers of number theory – they would likely have read his delightful book, *250 problems in elementary number theory*. Not many know, however, of some of the significant problems on which he worked. He lived through a dark chapter in Polish history, when Poland was overrun by the Nazis, and in spite of huge obstacles, he managed to sustain an extraordinary output of papers and books. Among the topics that he worked on, the following should be mentioned: the *Gauss circle problem* (in lattice point theory), *point set topology*, *curves that fill the plane* (early examples of today's fractal sets), the *axiom of choice*, and the *continuum hypothesis*.

Keywords
Sierpiński numbers, Fermat numbers, Chinese remainder theorem, covering set.

Sierpiński Numbers

To see how the problem might arise, recall the *Fermat numbers* F_n ($n \in \mathbb{N}$) given by

$$F_n = 2^{2^n} + 1. \tag{1}$$

Fermat had rather rashly conjectured that all these numbers are primes. This is true for the numbers

$$F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537.$$

Sadly, for $n > 4$, not even one prime F_n is known. So the conjecture has been a rather spectacular miss!

The demolition of the conjecture was accomplished by Euler, who showed that F_5 is divisible by 641 and hence composite. This may seem a 'completely out of the blue' finding (laymen may be excused for wondering whether mathematicians go around carrying '641 times' tables in their heads!), but in fact it is not, because of the following result first shown by Euler himself.

> *If F_n is not prime, then each of its prime factors is of the form* $1 \pmod{2^{n+1}}$.

The proof is as follows. Let p be a prime factor of $F_n = 2^{2^n} + 1$; then

$$2^{2^n} \equiv -1, \qquad 2^{2^{n+1}} \equiv 1 \pmod{p}.$$

We know from the Little Fermat Theorem (LFT) that $2^{p-1} \equiv 1 \pmod{p}$. Let d be the order of 2 modulo p. Then d divides every integer $x > 0$ for which $2^x \equiv 1 \pmod{p}$. In particular, therefore, d divides 2^{n+1} and $p-1$, but not 2^n, because $2^{2^n} \equiv -1 \pmod{p}$. It follows that $d = 2^{n+1}$, and therefore, that 2^{n+1} divides $p-1$; that is, p is of the form $1 \pmod{2^{n+1}}$. Stated otherwise, p is of the form $k \cdot 2^{n+1} + 1$ for some positive integer k.

The result implies that potential prime factors of $F_5 = 2^{32} + 1$ are all of the form 1 (mod 64). The primes of this form are

193, 257, 449, 577, 641, 769, 1153, 1217, 1409, 1601,

Trial division of F_5 by these primes quickly reveals that 641 is a divisor.

Remark. A short proof of the divisibility of F_5 by 641 is the following. It rests on two lucky numerical 'coincidences', namely, (i) $641 = 5^4 + 2^4$, and (ii) $641 = (5 \times 2^7) + 1$. From these we get $(5 \times 2^7) \equiv -1$, therefore $5^4 \times 2^{28} \equiv 1$, the congruences being modulo 641. Since $5^4 \equiv -2^4$, this yields $(-2^4) \times 2^{28} \equiv 1$. This is the same as saying that 641 divides $2^{32} + 1$.

It is possible that this result motivated Sierpiński to study numbers of the form $k \ \ 2^n + 1$ for various values of k. Whatever be the precise source, at some point he asked the following question:

> *Does there exist a positive integer k such that $k \ \ 2^n + 1$ is composite for every positive integer n?*

Offhand, there does not seem to be much reason for supposing that such an integer should exist; but in fact, there are infinitely many such integers, as shown by Sierpiński himself. One way of demonstrating their existence is by using the Chinese Remainder Theorem (CRT). The following proof is due to Subhash Khot, a two-time IMO silver medalist and the JEE 1995 first ranker. (He found the proof in the course of an examination! I believe that a similar proof was given by Don Zagier.)

Khot notes that any positive integer n can be written uniquely in the form $2^h q$ where q is odd and h is a non-negative integer. He proposes to choose k so that

$$k > 1, \quad k \equiv 1 \pmod{F_h}, \tag{2}$$

where $F_h = 2^{2^h} + 1$ is the hth Fermat number. Then $2^{2^h} \equiv -1 \pmod{F_h}$, so

$$k \;\; 2^n + 1 = k\, 2^{2^h q} + 1 \equiv (-1)^q + 1 \equiv 0 \pmod{F_h},$$

since q is odd, implying that $k \;\; 2^n + 1$ is composite.

Obviously, here, h depends on n, so how does he get around this? (Naturally, k is to be chosen in advance – it cannot depend on n.) Khot starts by choosing k so that

$$k > 1, \quad k \equiv 1 \pmod{F_h}, \quad \text{for } h = 0, 1, 2, 3, 4. \quad (3)$$

This choice is possible by the CRT, since the five moduli are the first five Fermat primes, and it takes care of all n of the form $2^h q$ (q odd, $h < 5$). But he still has to take care of the n's for which $h \geq 5$; that is, the n's which are divisible by 32. Let $n = 2^5 m$, where m may be odd or even. Let the factorization of F_5 be PQ, where $P = 641$ and $Q = 6700417$. Khot chooses k so that

$$k \equiv -1 \pmod{P} \quad \text{and} \quad k \equiv 1 \pmod{Q}. \quad (4)$$

This choice is possible by the CRT, and it implies the following:

$$k \;\; 2^n + 1 = k \;\; 2^{2^5 m} + 1 \equiv (-1)^{m+1} + 1 \pmod{P},$$
$$k \;\; 2^n + 1 = k \;\; 2^{2^5 m} + 1 \equiv (-1)^m + 1 \pmod{Q}.$$

So $k \;\; 2^n + 1$ is divisible by P if m is even, and by Q if m is odd. It follows that $k \;\; 2^n + 1$ is composite for all positive integers n. Khot's answer is, therefore: select k so that

$$\left.\begin{array}{l} k \equiv \;\; 1 \pmod{x}, \\ \text{for } x \in \{3, 5, 17, 257, 65537, 6700417\}, \\ k \equiv -1 \pmod{641}. \end{array}\right\} \quad (5)$$

Using *Mathematica*, or some other such package, the least integer k satisfying these congruences is found to be

The least odd natural number k so that $k.2^n+1$ is composite for every natural number n is unknown, as yet.

$k = 2935363331541925531$. This thus yields an integer with the desired property.

The following observations may be made at this point.

- The proof is *constructive*; it actually exhibits an integer with the required property, rather than only showing that it must exist.
- While the congruences in the above proof suffice for an integer to have the required property, they are by no means necessary.
- No claim has been made that the value of k obtained above is the least one with the required property.

In view of the result proved above, the following definitions arise naturally.

> A **Sierpiński number** is an odd positive integer k with the property that $k \cdot 2^n + 1$ is composite for every positive integer n. The set of all Sierpiński numbers is denoted by $\mathcal{S}$.

The Sierpiński Problem

The problem of finding the least number in $\mathcal{S}$ has become known as the *Sierpiński problem.* It is conjectured (and widely believed by researchers) that 78557 is the desired number.

The fact that $78557 \in \mathcal{S}$ may be shown as follows, using the 'covering set' of moduli

$$\{3, 5, 7, 13, 19, 37, 73\}. \tag{6}$$

We prove below that the integer $A_n := 78557 \times 2^n + 1$ is divisible by at least one of these moduli for each $n \in \mathbb{N}$ (hence the name, 'covering set').

- *Divisibility by* 3. Since $78557 \equiv 2 \pmod 3$, we get:

  3 divides $A_n \iff 2^n \equiv 1 \pmod 3 \iff n \equiv 0 \pmod 2$,

  because the powers of 2, reduced modulo 3, go through the cycle $\langle 2, 1 \rangle$, with a cycle length of 2.

- *Divisibility by* 5. Since $78557 \equiv 2 \pmod 5$, we deduce that

  5 divides $A_n \iff 2^n \equiv 2 \pmod 5 \iff n \equiv 1 \pmod 4$,

  because the powers of 2, reduced modulo 5, go through the cycle $\langle 2, 4, 3, 1 \rangle$, with a cycle length of 4.

- *Divisibility by* 7. Since $78557 \equiv 1 \pmod 7$, we deduce that

  7 divides $A_n \iff 2^n \equiv 2 \pmod 7 \iff n \equiv 1 \pmod 3$,

  because the powers of 2, reduced modulo 7, go through the cycle $\langle 2, 4, 1 \rangle$, with a cycle length of 3.

- *Divisibility by* 13. Since $78557 \equiv 11 \pmod{13}$, and the inverse of 11 modulo 13 is 6, we deduce that

  13 divides $A_n \iff 2^n \equiv 7 \pmod{13} \iff n \equiv 11 \pmod{12}$,

  because the powers of 2, reduced modulo 13, go through the cycle

  $$\langle 2,\ 4,\ 8,\ 3,\ 6,\ 12,\ 11,\ 9,\ 5,\ 10,\ 7,\ 1 \rangle,$$

  with a cycle length of 12 (observe that 2 is a primitive root modulo 13).

- *Divisibility by* 19. Since $78557 \equiv 11 \pmod{19}$, we deduce that

19 divides $A_n \iff 2^n \equiv 12 \pmod{19} \iff n \equiv 15 \pmod{18}$,

because the powers of 2, reduced modulo 19, go through the cycle of length 18, with 12 occurring in the 15th place.

- *Divisibility by* 37. Since $78557 \equiv 17 \pmod{37}$, we deduce that

  37 divides $A_n \iff 2^n \equiv 13 \pmod{37} \iff n \equiv 11 \pmod{36}$,

  because the powers of 2, reduced modulo 37, go through the cycle of length 36, with 11 occurring in the 11th place.

- *Divisibility by* 73. Since $78557 \equiv 9 \pmod{73}$, we deduce that

  73 divides $A_n \iff 2^n \equiv 8 \pmod{13} \iff n \equiv 3 \pmod{9}$,

  because the powers of 2, reduced modulo 73, go through a cycle of length 9, namely $\langle 2, 4, 8, 16, 32, 64, 55, 37, 1$, with 8 occurring in the 3rd place.

But now we find, pleasingly, that the congruences

$n \equiv 0 \pmod{2}$, $n \equiv 1 \pmod{4}$, $n \equiv 1 \pmod{3}$, $n \equiv 11 \pmod{12}$

$n \equiv 15 \pmod{18}$, $n \equiv 11 \pmod{36}$, $n \equiv 3 \pmod{9}$,

neatly exhaust all the integers. It follows that A_n is divisible by at least one of the moduli $3, 5, 7, 13, 19, 37, 73$ for every positive integer n. Since $A_n > 73$ for all n, it follows that A_n is composite for all $n \in \mathbb{N}$.

Remark. Observe that the role played in this proof by the number 78557 is only in terms of its residues when

divided by the moduli 3, 5, 7, 13, 19, 37, 73. This being so, it follows that all numbers of the following form:

$$78557 \pmod{2 \times 3 \times 5 \times 7 \times 13 \times 19 \times 37 \times 73}, \quad (7)$$

i.e., 78557 (mod 140100870), are Sierpiński numbers. So we have found an infinity of Sierpiński numbers in a single congruence class! It follows that $\mathcal{S}$ has positive density in $\mathbb{N}$.

Update on the Sierpiński Problem

As noted earlier, it is conjectured that the least number in $\mathcal{S}$ is 78557. Over the decades, the task of proving this came down to proving that the following seventeen numbers are *not* in $\mathcal{S}$:

$$\left.\begin{array}{rrrrr} 4847, & 5359, & 10223, & 19249, & 21181, \\ 22699, & 24737, & 27653, & 28433, & 33661, \\ 44131, & 46157, & 54767, & 55459, & 65567, \\ 67607, & 69109. & & & \end{array}\right\} \quad (8)$$

Attempts to prune this list have included internet based "distributed computing", with findings reported on the website http://www.seventeenorbust.com/. For each k in the list, if a prime number of the form $k \ 2^n + 1$ is found (by whatever means – but this is obviously no mean task), then that k is immediately removed from the list.

By and by, the list has been whittled down. Recently (December 2004), it was reported that 28433 is not a Sierpiński number; specifically, that the number $28433 \times 2^{7830457} + 1$ is prime! (This makes it currently the fourth largest known prime. As may well be imagined, sophisticated software is needed for such computations.) The finding knocks 28433 out of potential membership in $\mathcal{S}$. As of now, the list given above has been pruned to the

Recently (December 2004), it was reported that 28433 is not a Sierpiński number; specifically, that the number $28433 \times 2^{7830457} + 1$ is prime!

An odd positive integer k with the property that $k \cdot 2^n - 1$ is composite for every positive integer n is called a 'Riesel number' It is conjectured that the smallest Riesel number is 509203.

following:

$$\left.\begin{array}{lllll} 4847, & 10223, & 19249, & 21181, & 22699, \\ 24737, & 27653, & 33661, & 55459, & 67607. \end{array}\right\} \quad (9)$$

Readers may want to try reducing the list further!

Combinatorial Aspects of the Sierpiński Problem

In Ribenboim's delightful book [5], we read of the following result proved by Erdős and Odlyzko (it was reported in *Journal of Number Theory* in 1979, under the title "On the Density of Odd Integers of the Form $(p-1)/2^k$ and Related Questions"):

> *For any real number $x \geq 1$, let $N(x)$ denote the number of odd positive integers k, not exceeding x, such that there exists a positive integer n for which $k \cdot 2^n + 1$ is prime. Then there exists a positive number C_1 such that $N(x) \geq C_1 x$ for all $x \geq 1$.*

In the other direction, it is also true that $N(x) \square C_2 x$ for all sufficiently large values of x, where C_2 is a positive constant less than $\frac{1}{2}$. Erdős and Odlyzko have conjectured that $N(x)$ is of the form Cx for large x, where C is a positive constant; but this remains open.

Remark. Similar questions to those asked above may be asked of numbers of the form $k \cdot 2^n - 1$. An odd positive integer k with the property that $k \cdot 2^n - 1$ is composite for every positive integer n is called a 'Riesel number' It is conjectured that the smallest Riesel number is 509203.

Tailpiece

Questions invariably breed further questions. One such question which occurs at this stage is:

Does there exist an integer k such that $2^n + k$ is composite for every $n \in \mathbb{N}$?

A possible connection of this query with the Sierpiński problem is the following. (It was pointed out by my colleague B Sury.) Let k be a Sierpiński number; then $k \ 2^n + 1$ is composite for all $n \in \mathbb{N}$. So for each $n \in \mathbb{N}$, the number $k \ 2^n + 1$ has a prime divisor, say q_n. This means that $k \ (-2^n) \equiv 1 \pmod{q_n}$, implying that k is invertible modulo q_n, and that its inverse k' satisfies the relation $2^n + k' \equiv 0 \pmod{q_n}$. We see here an occurrence of the form $2^n + k'$.

Suggested Reading

Readers who wish to know more about this problem are referred to the following:

[1] **http://www.seventeenorbust.com/+**

[2] **http://primes.utm.edu/glossary/page.php?sort=SierpinskiNumber+**

[3] **R Baillie, G Cormack, and H C Williams, The problem of Sierpinski concerning $k \cdot 2^n + 1$', *Math. Comp.*, Vol. 37, pp.229-231, 1981.**

[4] **W Keller, Factors of Fermat numbers and large primes of the form k $2^n + 1$, *Math. Comp.*, Vol. 41, pp. 661-673, 1983.**

[5] **P Ribenboim, *The New Book of Prime Number Records*, Springer Verlag, 1996.**

[6] **W Sierpinski, Sur un probleme concernant les nombres $k \cdot 2^n + 1$, *Elem. Math.*, Vol.15, pp.73-74, 1960.**

The great Polish mathematician Waclaw Sierpinski was coincidentally also absent-minded and coincidentally also had to move house. His wife knew of his fallibility as they stood on the street with all their belongings, said to him, "Now, you stand here and watch our ten cases, while I go and get a taxi." She left him there, eyes glazed and humming absently. Some minutes later she returned, a taxi having been called. Sierpinski challenged her (possibly with a glint in his eye): "I thought you said there were ten cases, but I've only counted to nine." His wife insisted there were ten. "No, count them," replied Sierpinski, "0, 1, 2, ...".