Math-Magic Generalized Fermat Numbers

YATHIRAJ

Some of you might have come across the following 'Magic' of numbers. Take a three-digit number, say 123. Repeat the same sequence of digits to make a six-digit number (in our case 123123). Now divide this by 7. To your surprise you get an integer again, i.e., 7 completely divides 123123 (in our case we get the quotient 17589). Next, divide the quotient by 11. Again, to your surprise, the resulting number is an integer (in our case, 1599). Finally, divide the new quotient by 13. Magic! You get back 123, i.e., you have extracted the original number. Oh! Is it really magic? I mean, does it work for all three-digit numbers? Readers may stop at this point to explore whether the magic holds for other such numbers (say 516516). Not just that, readers may try to find out whether this 'magic' works for all six-digit numbers. (For instance, does it work for 237765?)

Now, take a four-digit number, say 1234, and repeat the sequence of digits to get an eight-digit number (12341234 in our case). Now, dividing by 7, 11 and 13 does not work. Can we now find a sequence of prime divisors such that dividing by them in turn, we recover our original number 1234? The answer is yes, and the primes are 73 and 137. That is, dividing 12341234 by 73 we get 169058. Divide this by 137. Magic! – we get back 1234. If we now want to extend this technique to five-digit sequences of numbers, what primes do we need to choose? The answer is simple and relies on the structure of the place value system.

Keywords: Exploration, conjecture, place value, divisibility, primes, algebra, identities, parity.

Observe that carrying out the division by 7, 11 and 13 one after the other is the same as dividing the given number by their product that is by $7 \times 11 \times 13 = 1001$. Notice that, if $\boxed{abc}$ represents a three-digit number, then

$$\boxed{abc} \times 1001 = \boxed{abc} \times (1000 + 1) = \boxed{abc000} + \boxed{abc} = \boxed{abcabc}.$$

Therefore:

$$\frac{\boxed{abcabc}}{7 \times 11 \times 13} = \boxed{abc}.$$

Thus, to see the analog of this magic for five-digit sequences of numbers, one should observe that

$$\boxed{abcdeabcde} = 100001 \times \boxed{abcde} \Longrightarrow \frac{\boxed{abcdeabcde}}{100001} = \boxed{abcde}.$$

Thus, it is enough to look for the prime factorization of 100001 which is 11×9091. Hence the primes to be used for the divisions are 11 and 9091.

Once the trick is known, the task seems uninteresting and the thrill in the magic is lost. But the game is not over yet! We have many observations to make here. The first is that most numbers of the form $10^n + 1$ (which has $n - 1$ zeroes between two 1's) are composite (i.e., they have at least two prime divisors, so we can carry out the sequential division process to recover the original number). We have seen this till $n = 5$. It is an easy task for a computer to give us the factorization of $10^n + 1$, at least for small values of n . But even a computer has limitations: it cannot factorize $10^n + 1$ beyond some n.

Then how do we know that for most natural numbers n, $10^n + 1$ is composite? Consider$10^{25} + 1$. It is easy to observe that any prime divisor of $10^5 + 1$ is also a divisor of $10^{25} + 1$. How? Simple:

$$10^{25} + 1 = \left(10^5\right)^5 + 1 = \left(10^5 + 1\right)\left(10^{20} - 10^{15} + 10^{10} - 10^5 + 1\right),$$

which is based on the following identity which is true for all odd n:

$$a^n + 1 = (a + 1)\left(a^{n-1} - a^{n-2} + a^{n-3} - + \ldots + 1\right).$$

This gives us a general way of dealing with numbers of the form $10^n + 1$, where n is multiple of some odd number greater than 1. Suppose $n = mk$, where $m > 1$ is odd and $k > 1$ is any integer. Then

$$10^n + 1 = 10^{mk} + 1 = \left(10^k\right)^m + 1 = \left(10^k + 1\right)\left(\left(10^k\right)^{m-1} - \left(10^k\right)^{m-2} + \ldots + 1\right).$$

Obviously, a factor of $10^k + 1$ is also a factor of $10^n + 1$. We deduce that $10^n + 1$ is composite if n is a multiple of an odd number greater than 1.

Challenge for the reader. Suppose $n = 10^9 + 1 = 1000000001$. Can you find at least three prime divisors of n without the help of a computer?

However, what happens if n is not a multiple of any odd number greater than 1? For example, $n = 4$ is such a number. We know that any natural number greater than 1 can be written as a product of primes in a unique manner; this is the *fundamental theorem of arithmetic*. If n is not divisible by any odd number, then n must not be divisible by any odd prime. Hence the prime factorization of n must contain only even primes. The only even prime is 2. It follows that n is of the form 2^k. Since $n > 2$, we must have $k > 1$. Can we now say that in such a case $10^n + 1$ is composite? The answer is: 'we do not know.'

At present, we do not know the primality status of all the numbers $10^{2^k} + 1$ for natural numbers k; there are both prime numbers and composite numbers in the set of all such numbers. In exploring this question, we are led into the serious business of number theory!

Explorations of this kind were started with Pierre De Fermat when he wrote a letter to his friend Frenicle in 1640. Fermat expressed his belief that numbers of the form $F_n = 2^{2^n} + 1$ are primes for all integers $n \geq 0$. Although he had no proof, he believed it was true. There was a reason for Fermat to believe in it as for the first few values of n, that is for $n = 0, 1, 2, 3$ and 4,

$$F_0 = 3; F_1 = 5; F_2 = 17; F_3 = 257; F_4 = 65537,$$

which are all primes. If it were true that F_n is prime for all non-negative integers n, we then would have a sequence generating only primes. This belief of Fermat was supported by another great mathematician, Mersenne. But when this problem was brought to the notice of Euler by Goldbach, Euler was able to show that F_5 is a composite number with 641 as one of its prime factors.

Challenge. Suppose that (like Fermat) we had no calculator or electronic computer. How could we check whether 65537 is prime or composite?

Do you know how big is F_5? It is 4294967297. Oh! Did Euler divide F_5 by every prime number less than or equal to the square root of F_5 to find its factors? That sounds extremely unlikely! Then how could he have shown that 4294967297 is composite? We shall not describe in detail the method of Euler. We shall simply give a road map. Interested readers may go through Chapter 10 of the book *Journey through genius* by William Dunham for a detailed proof by Euler.

Outline of Euler's proof

Euler proved the following statement which can be generalized easily.

Euler's statement. If a is an even number and p is a prime number that divides $a^{32} + 1$, then p must be of the form $64k + 1$ for some k.

Generalization. If a is an even number and p is a prime number that divides $a^{2^n} + 1$, then p must be of the form $2^{n+1}k + 1$ for some positive integer k.

In the above, replacing a by 2, Euler listed the possible candidates for the prime factors of $2^{2^5} + 1$; they are 65, 129, 193, 257, 321, 385, 449, 513, 577, 641, …. From this we eliminate candidates that are themselves not prime; we are left with the list 193; 257; 449; 577; 641; … Using the familiar long division method, Euler found that 641 divides $2^{2^5} + 1$ and thus showed that

$$2^{2^5} + 1 = 641 \times 6700417.$$

On numbers of the form $a^{2^n} + 1$

Numbers of the form $2^{2^n} + 1$ are called *Fermat numbers*, and numbers of the form $a^{2^n} + 1$ are called *generalized Fermat numbers*. If they are primes, then they are called *Fermat primes* or *generalized Fermat primes* (respectively). Here are some interesting facts about these numbers.

1. A prime factor of $a^{2^n} + 1$ is of the form $k2^m + 1$ for some integers k and $m > n$.
2. Every prime of the form $k2^m + 1$ (with $m > 1$), is a factor of $a^{2^n} + 1$ for at least one even a.

3. The largest known generalized Fermat prime is the number

$$1963736^{2^{20}} + 1.$$

See https://t5k.org/primes/page.php?id=134423.

4. Fermat had a connection with the Greeks. The connection is seen in the topic of geometric constructions. The Greeks were keenly interested in constructing regular polygons using only the compass and ruler. (Here, the term 'ruler' refers to a straight edge with no markings on it.) They knew how to construct a regular triangle (i.e., an equilateral triangle), a square, a regular pentagon, a regular hexagon, etc. They wondered: Is it possible to construct all such regular polygons using compass and ruler? They did not have an answer to this question.

   It took almost 2000 years before a complete answer to this question became known, through the work of Gauss and Wantzel. It turns out that the answer is 'No; only some regular polygons can be so constructed.' Their famous result is that the only regular polygons which can be constructed using compass and ruler are those with number of sides of the form $2^k p_1 p_2 \ldots p_n$, where $k \geq 0$, $n \geq 1$, and $p_1, p_2, \ldots, p_n$ are unequal Fermat primes. Hence, it is not possible to construct a regular polygon with 7 sides or 9 sides or 11 sides or 13 sides or 19 sides; but it is possible to construct a regular polygon with 15 sides or 17 sides! What an astonishing conclusion to a 2000-year-old problem!

YATHIRAJ currently works in the department of Mathematics, Sarada Vilas College, Mysuru. Prior to this, he worked in Azim Premji Foundation, Mandya as a Teacher Educator for nearly four years. He is doing research in the areas of special functions and number theory. He is also interested in understanding the patterns, connections and thought processes which one employs during problem solving. He may be contacted at yathirajsharma@gmail.com.