Learning from mistakes

Fermat Numbers

A false conjecture leading to fun and fascination

feature

Interspersed with historical and biographical details, this article has rich nuggets of information. These don't just exercise a student's understanding of exponents, they also provide solvable proofs for school students. Best of all, the article weaves random results into a coherent whole, giving direction to ideas, conjectures and proofs.

B. A. Sethuraman

Introduction

The French mathematician Pierre de Fermat (1601–1665) was a veritable giant of number theory whose discoveries, and especially, whose conjectures and unproven assertions, kept mathematicians hard at work for several centuries that followed. Indeed, the first two issues of this magazine both featured his work: the first issue reviewed a book ([1]) on the history of what is known as "Fermat's Last Theorem," while the second issue, in an article on the four squares theorem ([2]), describes Fermat's work on primes that are representable as sums of two squares.

Besides these two well known contributions, Fermat is known for a whole host of other theorems in mathematics. He was a lawyer by training, but his passion was mathematics. He shone in arithmetic (which in its more advanced form is what we call number theory today), but made seminal contributions in other parts of mathematics as well, and even in physics.

Keywords: *Fermat, Fermat number, Fermat prime, infinity, regular polygons, constructibility*

Great mathematicians, and Fermat was squarely in that league, are characterized by deep intuition that enables them to see mathematical truths that others are not yet able to see. But great mathematicians are also human, and occasionally, they are wrong. Fermat himself was wrong on at least one mathematical matter: the issue of whether numbers of the form $2^{2^n}+1$ are prime. These numbers are the subject of this article.

Recall first the convention when interpreting numbers written with repeated exponents: $2^{2^n}+1$ is to be interpreted as $2^{(2^n)}+1$ (and *not* $(2^2)^n+1$). Let us write F_n for the number $2^{2^n}+1$, so that $F_0 = 2^{2^0}+1 = 2^1+1 = 3$, $F_1 = 5$, $F_2 = 17$, etc. Fermat claimed that the numbers F_n are prime for all integers $n = 1, 2, \ldots$. In fact, he first claimed to have a proof, but later discovered an error in it ([3, Foreward]). However, he appeared to still believe in the truth of his claim. It is thus fair to rename his claim as a conjecture.

Indeed, F_0, F_1, and F_2 above are clearly prime. So is $F_3 = 2^8+1 = 257$ and $F_4 = 2^{16}+1 = 65537$. *But there the list is broken!* Euler, who lived approximately a century after Fermat (1707–1783) showed that F_5, a ten-digit integer, is not prime: it is divisible by 641. Thus, Fermat's conjecture on the numbers $2^{2^n}+1$ was false!

But there is another characterization of great mathematicians that is relevant here—the very objects they think about turn out to be fascinating and deep, even if these mathematicians occasionally make false assertions about them! Such is indeed the case with numbers of the form $2^{2^n}+1$, now appropriately called *Fermat Numbers.* (Numbers of the form $2^{2^n}+1$ that are prime are now referred to as *Fermat primes.*) Fermat numbers have many charming properties, and have turned out to have intriguing connections to other parts of mathematics, as well as to computer science.

Identities and the infinitude of primes

Let us start with some pretty identities that Fermat numbers satisfy. Their proofs are fun exercises for high school students, involving nothing more than simple algebra and induction.

1. $F_n = (F_{n-1}-1)^2+1$, for $n \geq 1$.
2. $F_n = F_0 \times F_1 \times F_2 \times \cdots \times F_{n-1} + 2$, for $n \geq 1$.
3. $F_n = 2^{2^{n-1}} \cdot F_0 \cdot F_1 \cdot F_2 \cdot \cdots \cdot F_{n-2} + F_{n-1}$, for $n \geq 2$.
4. $F_n = F_{n-1}^2 - 2(F_{n-2}-1)^2$, for $n \geq 2$.

We will prove the first one here: Note that

$$2^{2^n} = 2^{2^{n-1+1}} = 2^{2^{n-1}\cdot 2} = (2^{2^{n-1}})^2 = (F_{n-1}-1)^2.$$

Adding one everywhere, we find
$F_n = 2^{2^n}+1 = (F_{n-1}-1)^2+1$, as desired.

There is an immediate consequence of the second identity above: the last digit of every Fermat number (for $n \geq 2$) must be 7. This is because for $n \geq 2$, we have

$$F_n = 3\cdot 5\cdot F_2 \cdot \cdots \cdot F_{n-1} + 2 = 5(3\cdot F_2 \cdot \cdots \cdot F_{n-1}) + 2.$$

So F_n is of the form 2 plus an odd multiple of 5 and hence has last digit 7. Pretty!

The second consequence is that the Fermat numbers are pairwise relatively prime; that is, for distinct non-negative integers i and j, $\gcd(F_i, F_j) = 1$. This is attributed to Christian Goldbach (who is well known for a conjecture that is as yet unproven: Every even integer greater than 2 is expressible as a sum of two primes). As noted in a companion article in this issue, *There are Infinitely many Primes*, this property leads to another proof of the infinitude of primes.

Fermat numbers and constructibility of polygons

Recall the problems of constructibility handed to us by the Greeks: using only straight-edge and compass, construct line segments of specified lengths, and angles of specified measures. It was an open problem for a very long time, for instance, (i) whether one could trisect an arbitrary angle using straight-edge or compass, (ii) whether one could "square the circle," that is, construct the side of a square whose area is that of a given circle, and (iii) whether one could "double the cube," that is, construct the side of a cube whose volume is twice that of a given cube. These problems are easy to solve once one has at one's command techniques from Field Theory (known earlier as the 'Theory of Equations'); but this theory was not known to the Greeks. We now know that the answer all three questions is: No!

A specific problem in this context was the constructibility of regular n-gons for various

values of n. Thus, a regular 3-gon is an equilateral triangle, a regular 4-gon is a square, a regular 5-gon is a regular pentagon, and so on. Whether a regular n-gon can be constructed using a straight-edge and compass quickly reduces to the question of whether the angle $360^\circ/n$ can be constructed using straight-edge and compass.

This problem was investigated by the Great Master, Carl Friedrich Gauss. (Gauss ranks among the greatest mathematicians ever, when measured not just by his own productivity but by the new areas of mathematics he initiated; his results to this date are a source of joy and wonder. His influence on mathematics and indeed all sciences ranks with that of Newton.) Gauss showed that the regular 17-gon is constructible (note that 17 is F_2), and went on to show that a regular n-gon ($n \geq 3$) can be constructed if the prime factorization of n is of the form $2^k p_1 p_2 \cdots p_l$, where the p_i are distinct primes of the form $2^{2^t} + 1$; Fermat numbers again! This is an instance of how questions about objects considered by great mathematicians (in this case Fermat) can turn out to have deep significance in mathematics, far from apparent at first. Thus, the question of whether for a given k the k^{th} Fermat number $2^{2^k} + 1$ is prime turns out to be more than just a curiosity: it is vitally connected to whether an n-gon can be constructed.

The reason why a regular n-gon with the stated prime factorization of n is constructible, lies in Field Theory. For the case where n is a prime—call it p instead—the theory tells us that the regular p-gon is constructible *if and only if* $p - 1$ is a power of 2. Thus, a regular p-gon is constructible if and only if $p = 2^k + 1$ for some integer k.

Now one can see quite easily that $2^k + 1$ cannot be prime unless k is itself a power of 2. For, suppose $k = 2^l b$ for some odd integer $b > 1$. Then

$$2^k + 1 = 2^{2^l b} + 1 = (2^{2^l})^b + 1.$$

Now it is a fact (it can be proven as a high school exercise) that $x^b + 1$ is divisible by $x + 1$ if b is odd. Hence if $b > 1$, $p = (2^{2^l})^b + 1$ would have the strictly smaller divisor $2^{2^l} + 1$, contradicting the fact that p is prime. Hence, the condition from Field Theory becomes: for prime $p \geq 3$, a regular p-gon is constructible if and only if p is a Fermat prime!

The condition for the constructibility of a regular n-gon for a general n follows from the condition just described for the case where n is prime, using standard reductions also furnished by Field Theory. Indeed, the condition for a general n-gon is also an *if and only if* statement: a regular n-gon is constructible if and only if n is of the form described by Gauss. Gauss proved the 'if' part of the condition, but his proof of the 'only if' part had a gap that was filled only later ([3, Chap. 16]).

Primality of the Fermat numbers

Let us turn to the original conjecture of Fermat, that the numbers $2^{2^n} + 1$ are prime for all $n = 0, 1, \ldots$. We know, thanks to Euler, that while F_0 through F_4 are prime, F_5 is not. For what other values of n is F_n known to be prime? The answer, more than three hundred and fifty years after Fermat made his first conjecture, is: None!

That does not mean that no F_n is prime for $n \geq 5$. All it means is that no one has as yet found a prime F_n for $n \geq 6$. What has been established are many results in the opposite direction (similar to the case of F_5): the numbers F_6 through F_{32} have all been shown to be composite ([4]). Besides these, F_n is known to be composite for other sporadic values of n, such as $n = 36, 71, 99, 517, 2059, 6390, 17748$, to select just a sample ([4]).

What makes determination of the primality of F_n so difficult is that, thanks to the presence of the double exponent, the number of digits in F_n grows very rapidly as n becomes large. In fact, Exercise (2) shows that the growth in the number of digits is exponential.

On the other hand, there is a very pretty result on the possible prime factors of F_n: Euler showed that any prime that divides F_n must be of the form $k \cdot 2^{n+1} + 1$, for some positive integer k. (The proof of this itself involves another famous theorem of Fermat known as Fermat's Little Theorem: for any prime p and any integer a, the number $a^p - a$ is divisible by p.) Euler's result was further sharpened by Lucas, who showed

Figure 1. Stamp commemorating the 400th birth anniversary of Fermat; perhaps one day there will be another stamp depicting the next Fermat prime after F_4? Source for image: [8] and [9].

that the k in Euler's result must be even. Thus we have Lucas's result that any prime divisor of F_n must be of the form $l \cdot 2^{n+2} + 1$ for some positive integer l. This result is the basis of certain attempts at showing F_n is prime for various n: run through all possible integers of the form $l \cdot 2^{n+2} + 1$ that are less than $\sqrt{F_n}$ and check if they divide F_n. Though easy to state, the computational power required to perform these calculations, even allowing for various tricks used to speed up the process, is stupendous for large n, because the numbers F_n are so large. There are distributed searches currently taking place over the internet: various groups of people fascinated by Fermat primes collectively divide the work among themselves by looking for divisors in restricted ranges of l (see [5]). Anybody with a computer and access to the internet can join these searches: we encourage the reader to do so too!

Further readings and exercises

We have only touched on some aspects of Fermat numbers: there are many more charming features of these numbers, and many more connections with other parts of mathematics and computer science that we have not described. A wonderful reference for Fermat numbers is [3] (note the pun in its title!). Although quite advanced for a high school student, it conveys the fun and the fascination of these numbers, and students will profit by simply thumbing through the book. We also recommend the Wikipedia article ([6]) for another overview of some features of these numbers, as well as the MacTutor ([7]) biography of Fermat.

We end with some more exercises that can be tackled by high school students.

Exercises

(1) Prove Identities (3) and (4) in Section . (Hint: Use Identities (1) and (2).)

(2) Show that the number of digits in F_n is approximately $\lfloor 2^n \log_{10}(2) + 1 \rfloor$ (here, $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x).

(3) Show that for $n \geq 1$, F_n is of the form $6k - 1$ for some integer k. (Hint: You may find Identity (2) in the text helpful.)

(4) Show that no F_n ($n \geq 2$) is a sum of two primes. (Hint: If it were, then one prime would have to be 2.)

(5) Show that every F_n is the difference of two square integers. (Hint: Show that every odd integer is the difference of two squares.)

(6) Using Euler's theorem on the possible prime factors of F_n, show that no F_n is a perfect square. (Hint: assume that F_n is a perfect square. First show that if integers a and b both leave a remainder of 1 when divided by a certain integer m, then so does the integer ab. Now combine this results with Euler's description of the possible prime factors of F_n to describe $\sqrt{F_n}$.)

References

[1] Tanuj Shah, *Book Review: Fermat's Enigma*, At Right Angles, Vol. 1, Number 1, June 2012.

[2] Anuradha S. Garge, *Lagrange's Four Squares Theorem*, At Right Angles, Vol. 1, Number 2, December 2012.

[3] Michal K˘rížek, Florian Luca, Lawrence Somer, 17 *Lectures on Fermat Numbers*, CMS Books in Mathematics, Springer, 2001.

[4] http://www.prothsearch.net/fermat.html

[5] http://www.fermatsearch.org/index.html

[6] http://en.wikipedia.org/wiki/Fermat_number

[7] http://www-history.mcs.st-andrews.ac.uk/Biographies/Fermat.html

[8] http://www-history.mcs.st-andrews.ac.uk/PictDisplay/Fermat.html

[9] http://jeff560.tripod.com/stamps.html

B. A. SETHURAMAN got his B.Tech in Mechanical Engineering from IIT Madras, and subsequently switched to pure mathematics. He got his Ph.D at the University of California at San Diego, and is now a professor of mathematics at California State University Northridge. He has several research publications in various areas of mathematics and its applications to wireless communication. He has also written a textbook for future high-school teachers titled *Rings, Fields, and Vector Spaces*, published by Springer-Verlag. He visits India often, both to teach and for research collaboration. In India he has taught both at IIT Bombay and ISI Bangalore.