A Brief Introduction to Fermat Numbers

LEUNG Tat-Wing

Consider a positive integer of the form $2^m + 1$. If it is a prime number, then m must be a power of 2. Otherwise, let $m = 2^n s$, where s is an odd number greater than or equal to 3. We have $2^m + 1 = 2^{2^n s} + 1 = (2^{2^n})^s + 1 = (2^{2^n} + 1)\big((2^{2^n})^{s-1} - (2^{2^n})^{s-2} + \cdots \pm 1\big)$, from which it is easily seen that $2^m + 1$ decomposed into a product of two positive divisors. The amateur mathematician Fermat (1601-1665) have considered the following "Fermat" numbers. Let $F_n = 2^{2^n} + 1,\ n = 0, 1, 2, \ldots$. Fermat observed $F_0 = 2^{2^0} + 1 = 3, F_1 = 2^{2^1} + 1 = 5, F_2 = 2^{2^2} + 1 = 17, F_3 = 2^{2^3} + 1 = 257, F_4 = 2^{2^4} + 1 = 65537$ are prime numbers (that the last number is a prime takes a bit of work to prove). Because of these, he conjectured all positive integers of the form $2^{2^n} + 1$ are prime numbers.

Unfortunately, about a hundred years later, Euler (1707-1783) discovered F_5 is not a prime number. In fact, up to now, all known $F_n, n \geq 5$ are not prime numbers. For F_5 not prime, there is a simple proof. Since $641 = 5^4 + 2^4 = 5 \times 2^7 + 1$, so 641 divides $(5^4 + 2^4)2^{28} = 5^4 \times 2^{28} + 2^{32}$. Also, since $641 = 5 \times 2^7 + 1$, so 641 divides $(5 \times 2^7 + 1)(5 \times 2^7 - 1) = 5^2 \times 2^{14} - 1$. Hence, we get 641 divides $(5^2 \times 2^{14} - 1)(5^2 \times 2^{14} + 1) = 5^4 \times 2^{28} - 1$. Finally, 641 divides the difference of $5^4 \times 2^{28} + 2^{32}$ and $5^4 \times 2^{28} - 1$, which is $2^{32} + 1 = F_5$.

This proof is very concise, but not natural. First, it is not known how to get 641 is a positive divisor. Second, that 641 can be written as the two sums above is quite fortunate. Let us investigate how Euler discovered F_5 was not a prime number. We believe the process may have been like this. Euler observed that if p is a prime divisor of $F_n = 2^{2^n} + 1$, then p must be of the form $k \cdot 2^{n+1} + 1$. Using the language of modulo arithmetic, if p divides $2^{2^n} + 1$, then $2^{2^n} \equiv -1 (\text{mod } p)$. Squaring yield $2^{2^{n+1}} \equiv 1 (\text{mod } p)$. Next, using Fermat's little theorem (known at Euler's time), we see $2^{p-1} \equiv 1 (\text{mod } p)$. If d is the smallest positive integer such that $2^d \equiv 1 (\text{mod } p)$, it can be proved (check please) that d divides $p - 1$ and 2^{n+1}, but not 2^n (as $2^{2^n} \equiv -1 (\text{mod } p)$). Hence $d = 2^{n+1}$. Also, since d divides $p - 1$, so $p - 1 = k \cdot 2^{n+1}$ or $p = k \cdot 2^{n+1} + 1$. (If the so-called law of quadratic reciprocity is used, it can even be proved that p is of the form $k \cdot 2^{n+2} + 1$.)

For example, consider F_4. Its prime divisor must be of the form $32k + 1$. Taking $k = 1, 2, \ldots$, the possible divisors are 97, 193 (the prime numbers of the form $32k + 1$ and less than $\sqrt{65537}$). However, 97 and 193 do not divide 65537, so 65537 is prime. Next, the prime divisors of F_5 must be of the form $64k + 1$. Taking $k = 1, 2, \ldots$, the possible divisors are 193, 257, 449, 577, 641, $\cdots$. After a few trials, we get $2^{2^5} + 1 = 4294967297 = 641 \times 6700417$. With a bit of luck, very quickly we found a prime divisor of F_5. In fact, the second factor is also prime, but proving that is a bit more tedious.

However, if we try to use this method to find the divisors of the other Fermat numbers, we will run into problem very quickly. For example, $F_6 = 2^{2^6} + 1$ is a twenty-digit number. Its square root is a ten-digit number ($\approx 4.29 \times 10^9$). There are over three million numbers of the form $k \cdot 2^7 + 1 = 128k + 1$. To find a divisor of F_6 among them is not simple. The readers can think about this. In 1732 Euler found the complete factorization of F_5. It took one hundred years for Landry and Le Lasseur (1880) to find the complete factorization of F_6. Another one hundred years passed before Morrison and Brillhart (1970) discovered the complete factorization of F_7. So to find the prime factorizations of Fermat numbers must not be easy. In another direction, as finding Fermat numbers is not easy, Pepin in 1877 obtained a criterion for a Fermat number to be prime, namely for a Fermat number $N > 3$ of the form $2^{2^n} + 1$, a necessary and sufficient condition for N to be prime is $3^{\frac{N-1}{2}} \equiv -1 (\text{mod } N)$. Considering $\dfrac{N-1}{2} = 2^{2^n - 1}$, we should start with 3 and keep on squaring, then take (mod N). In recent years, this is the starting point for determining if Fermat numbers are primes or not. Also, for a long time since F_7 was shown to be not prime, nothing was known about any of its divisors.

Briefly we mention some recent results. It is now known that F_5 to F_{11} are composite numbers and their complete factorizations are found. F_{12}, F_{13}, F_{15} and F_{19} are known to be composite with only some divisors found. F_{14}, F_{20} and F_{22} are known to be composite with no divisors found.The largest composite Fermat number with one divisor known is F_{382447}. The reader can imagine if this number is written in base ten how many digits it will have. Next, for F_{33}, F_{34}, F_{35}, nothing is known whether they are composite or prime numbers. For those who are interested, please consult the webpage http:// www.fermatsearch.org/status.htm.

As Fermat numbers and related numbers are of special forms and have many interesting properties, they often appeared in many competitions. Here are some examples.

Example 1. The Fermat numbers $F_0, F_1, \ldots, F_n$ are given. We have the following relation $F_0 F_1 \cdots F_{n-1} + 2 = F_n$.

Proof. In fact, $F_n = 2^{2^n} + 1 = 2^{2^n} - 1 + 2 = 2^{2^{n-1}2} - 1 + 2 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) + 2 = (2^{2^{n-1}} - 1)F_{n-1} + 2$. For $2^{2^{n-1}} - 1$, we can factor further to get the required result. Of course, a rigorous proof can be given bu using mathematical induction.

Example 2. Fermat numbers F_m, F_n, $m > n$, are given. Then F_m, F_n are relatively prime.

Proof. Since $F_m = F_{m-1} \cdots F_n \cdots F_0 + 2$, let d divide F_m and F_n. Then d also divides 2. So $d = 1$ or 2. However, $d \neq 2$ as F_m, F_n are odd. So $d = 1$, i.e. F_m, F_n are relatively prime. (Hence $F_0, F_1, F_2, \ldots$ are pairwise relatively prime. That is, they include infinitely many prime divisors. Consequently, there are infinitely many prime numbers.)

Example 3. There are infinitely many n such that $F_n + 2$ is not prime.

Proof. Experimenting a few times it can be seen that $F_1 + 2 = 7, F_3 + 2 = 259$ are multiple of 7. In fact, for $n = 0, 1, 2, \ldots$, $2^{2^n} \equiv 2, 4, 2, 4, \ldots (\text{mod } 7)$. Since for odd n, $F_n + 2 \equiv 2^{2^n} + 1 + 2 \equiv 4 + 1 + 2 \equiv 0 (\text{mod } 7)$, so it is not prime.

Here is another fact.

Example 4. For $n > 1$, the units digit of F_n is 7.

Proof. For $n > 1$, 2^n is a multiple of 4. Let $2^n = 4k$, then $F_n = 2^{2^n} + 1 = 2^{4k} + 1 = (2^4)^k + 1 \equiv 1^k + 1 \equiv 2 (\text{mod } 5)$. So the units digit of F_n is 2 or 7. It cannot be 2 as F_n is not even.

Example 5. Prove that there exists a positive integer k such that for every positive integer n, $k \cdot 2^n + 1$ is not prime.

(If n is fixed and k is allowed to vary among positive integers, then from an important theorem (Dirichlet), it is known that the series will contain infinitely many primes. However, if k is fixed and n varies, then in general, it is not clear how many primes, infinite or not, there are in the series. In fact, one can find a k such that for every positive integer n, $k \cdot 2^n + 1$ is not prime. Originally this was a result of the Polish mathematician Sierpinski (1882-1969). Later it became a problem on the USA Math Olympiad (1982). Up to now, there is only one method of proving it and it is related too Fermat numbers.)

Proof. (The starting point of the proof is the Chinese remainder theorem. Let $m_1, m_2, \ldots, m_r$ be pairwise relatively prime positive integers and $a_1, a_2, \ldots, a_r$ are arbitrary integers. Then the