Factorization of Fermat Numbers

By Rushil Saha

Fermat enjoyed proposing conjectures and leaving the proofs to his readers. Fermat analyzed numbers of the form $2^{2^n}+1$ hence their name "Fermat numbers." When Fermat looked at the first four of these numbers and realized that they were all prime, he proposed that all Fermat numbers were prime. When Euler examined this, he believed that this was not true. To prove this result, he tried to find a prime divisor for the fifth Fermat number or $2^{2^5}+1$. In order to find a prime divisor, he tries to limit his search by finding a specific form for the divisor. He finds this result with the aid of several theorems which are each built upon each other.

Theorem 1

If p is a prime number, then every number of the form $(a+b)^p-a^p-b^p$ is divisible by p.

Proof: If we expand the binomial and simplify the terms, we find that it is equal to

$$\frac{p(ab)(a^{p-2}+b^{p-2})}{1}+\frac{p(p-1)(a^2b^2)(a^{p-4}+b^{p-4})}{1*2}+\frac{p(p-1)(p-2)(a^3b^3)(a^{p-6}+b^{p-6})}{1*2*3}+\frac{p(p-1)(p-2)(p-3)(a^3b^3)(a^{p-8}+b^{p-8})}{1*2*3*4}+..$$

In each of the fractions in the sum, each of the numerators has a factor of p, and the only thing that can cancel out the p is the factorial in the bottom. However, the fractions never reach half of p and since p is prime, it won't cancel out.

Theorem 2

If either a^p-a or b^p-b is divisible by a prime p, then $(a+b)^p-a-b$ is also divisible by the same prime p.

Proof: By Theorem 1, we have that $(a+b)^p-a^p-b^p$ is divisible by p, if p is prime, and since both a^p-a and b^p-b are divisible by p, then adding all of them together yields that $(a+b)^p-a-b$ is divisible by p.

Theorem 3

If p is a prime number, then all numbers of the form c^p-c is divisible by p.

Proof: If we let a be 1 in Theorem 2, we have that $(b+1)^p-b-1$ is divisible by a prime p. Then, we can let b+1 be equal to any c so we have that c^p-c is divisible by the same prime p.

Theorem 4

If neither a nor b is divisible by a prime number p, then every number of the form $a^{p-1} - b^{p-1}$ is divisible by p.

Proof: Since neither a nor b is divisible by p, and since p is prime, from Theorem 3, we have that $a^{p-1} - 1$ and $b^{p-1} - 1$ are divisible by p. Then the difference of those 2 numbers or $a^{p-1} - b^{p-1}$ is also divisible by p.

Now we have the basic groundwork to start the proof. We start with Fermat numbers when n=1 and then Euler expands the proof to larger n.

Theorem 5

The sum of 2 squares $a^2 + b^2$ can never be divided by any prime number of the form $4n - 1$, unless both a and b are divisible by $4n - 1$

Proof: If $4n - 1$ is a prime number,and neither a nor b is divisible by it, then by Theorem 4, we have that $a^{4n-2} - b^{4n-2}$ is divisible by $4n - 1$. Now to get $a^{4n-2} + b^{4n-2}$, we have to add $2b^{4n-2}$. Since b^{4n-2} is not divisible by $4n - 1$, then $a^{4n-2} + b^{4n-2}$ will not be divisible by $4n - 1$. Now we have to relate this result with $a^2 + b^2$. Since $4n - 2 = 2(2n - 1)$ or is equal to the product of an even and an odd number, then $a^{4n-2} + b^{4n-2}$ is divisible by $a^2 + b^2$. This means that $a^2 + b^2$ is also not divisible by $4n - 1$.

Theorem 6

All divisors of the sum of two relatively prime numbers to the fourth power are either 2 or have the form 8n+1.

Proof: We let a^4 and b^4 be two primes to the fourth power. If, both of them are odd, than 2 is a divisor of the sum $a^4 + b^4$. Now we look at when one is odd and the other is even. In that case, the odd divisors must be of the form $4n + 1$ because fourth powers can also be expressed as squares. Numbers of the form $4n + 1$ can be expressed as either $8n + 1$ or $8n - 3$ depending on the parity of n. Now we can prove that no number of the form $8n - 3$ can a divisor of the sum $a^4 + b^4$. Since $8n - 3$ is assumed to be a prime number, then from Theorem 4 again, we have that the difference $a^{8n-4} - b^{8n-4}$ is divisible by the prime $8n - 3$ from which it follow that the sum $a^{8n-4} + b^{8n-4}$ is not divisible by the prime $8n - 3$ using the same logic as above unless both a and b are separately divisible by it. This cannot be the case since a and b are assumed to be relatively prime. Then, since $8n - 4 = 4(2n - 1)$ or is the product of an even and odd number, it is divisible by $a^4 + b^4$. This means that $a^4 + b^4$ cannot be divided by $8n - 3$ as well.

Theorem 7

If a and b are relatively prime, every divisor of $a^8 + b^8$ is 2 or of the form $16n + 1$.

Proof: If a and b are both odd, then the sum would have be divisible by 2. Now we look at when one is even and the other is odd. Using the same logic as the previous two theorems, since a^8 and b^8 are also fourth powers, $a^8 + b^8$'s divisors must be of the form $8n + 1$. Depending on the parity of n, it can be expressed as either $16n + 1$ or $16n - 7$. If $16n - 7$ is a prime number, then from Theorem 4, we have that $a^{16n-8} - b^{16n-8}$ is divisible by $16n - 7$. Then as above, we find that $a^{16n-8} + b^{16n-8}$ is not divisible by $16n - 7$. Furthermore, since $16n - 8 = 8(2n - 1)$, it is divisible by $a^8 + b^8$. This means that $a^8 + b^8$ cannot be divisible by divisors of the form $16n - 7$. Then $a^8 + b^8$ can only divisors of the form $16n + 1$ or 2.

Theorem 8

The sum $a^{2^m} + b^{2^m}$ can only have divisors of the form $2^{m+1}n + 1$

Proof: Using the same process as before, we see that an induction argument can be made based on the previous n-1. Following this procedure, we find that the sum of two numbers $a^{2^m} + b^{2^m}$ can only divisors of the form $2^{m+1}n + 1$. The reason the argument Euler created to prove that certain numbers cannot be divisors of the Fermat numbers does not apply to $2^{m+1}n + 1$ is because $2^{m+1}n + 1 - 1$ or $2^{m+1}n$ can never be a prime which collapses the proof.

From this, we have that the divisors of $2^{2^n} + 1$ must be of the form $64a + 1$. Keeping this is mind, Euler starting testing different a and looked only at the divisors that were prime. After doing this, Euler founded that $64(10) + 1$ or 641 divides the fifth Fermat Number. This wrapped up the proof that the fifth Fermat number was composite.