**Topic:** The Great Theorem, Euler’s Refutation of Fermat

//the final great theorem we will examine :(

**Notes on Topic:**

As in the past, Goldbach tickled Euler’s curiosity when he asked, “Is Fermat’s observation known to you, that all numbers are primes? He said he could not prove it, nor has anyone else done so to my knowledge.”

Fermat thought that he has generated a formula to produce primes.

This rings true for n=1, n=2, n=3, n-4, and then we get to n=5, so .

Fermat likewise suggested that this was a prime.

Given his track record, there was no reason to doubt his statement. To prove him incorrect a mathematician would have to search for a way to factor this into two smaller numbers, and if Fermat was correct, the search would prove fruitless.

That is, until Euler, he focused on this number and ultimately was able to factor it, proving Fermat wrong.

How perverse, that ultimately what Euler used to refute Fermat’s statement was none other than the little fermat theorem itself. “Fermat had sown the seeds of his own downfall.”

“...as we watch Euler reason his way through the great theorem below, we cannot help but admit that, in the right hands, a little Fermat goes a long way” JTG 230.

We will examine three preliminaries building to the great theorem.

**Theorem A:** Suppose a is an even number, and p is a prime that is not a factor of a, but does divide evenly into a+1. Then for some whole number k, p=2k+1.

**Proof:** If a is even, then a+1 is odd. Since we assumed that p divides evenly a+1, p itself must be odd. Hence, p-1=2k for some integer k. In other words, p=2k+1.

**Q.E.D.**

**Theorem B:** Suppose a is an even number and p is prime that is not a factor of a, but such that p does divide evenly into , then for some integer k, p=4k+1.

**Proof:**  Since a is even, so is , so we know that any prime factor of must be odd. That is p is one more than a multiple of 2.

What happens when we divide p by 4. Obviously any odd number is either one more or three more than a multiple of 4, so either p=4k+1 or p=4k+3.

Euler wanted to eliminate the latter possibility, so for the sake of eventual contradiction, assume p=4k+3 for some integer k. By the hypothesis, p is not a factor of a, so by the little Fermat theorem, p does divide evenly into,

On the other hand, we have assumed that p is a divisor of and consequently is a divisor of the product,

It can be checked algebraically that, upon multiplying out and cancelling terms, this complicated product reduces to the relatively simple, .

We have now concluded that p divides both and , so it is necessary that p divides their difference,

But this is a contradiction since p is assumed to be odd, so cannot possibly divide 2. Thus the contradiction must imply that our assumption that p=4k+3 is false, and in fact p=4k+1 for some integer k.

**Q.E.D.**

**Theorem C:** Suppose a is an even number and p is prime that is not a factor of a but such that p does divide evenly into . Then for some whole number k, p=8k+1.

**Proof:** First note that, so from Theorem B, we know that p=4k+1, with this in mind, Euler wanted to know what would happen if he divided p by 8, where he encountered eight possibilities.

It is easy to rule out a few possibilities right away, since p is odd, we know that we must rule out, 8k, 8k+2, 8k+4, 8k+6.

Moreover, 8k+3=4(2k)+3 which we know cannot be p. And 8k+7=4(2k+1)+3 which cannot be p.

So the only possibilities are 8k+1 and 8k+5. Euler eliminated the latter by assuming p=8k+5 and reaching a contradiction. Since p is not a divisor of a, by the little Fermat theorem, p does divide evenly into,

Since p divides evenly into , it surely divides evenly into,

By a similar argument as Theorem B, that implies

This is a contradiction since p is odd and cannot divide 2. That implies that the original assumption that p=8k+5 is false, which means p=8k+1.

**Q.E.D.**

At last we reach the great theorem.

**The Great Theorem:** is not prime.

**Proof:** Since a=2 is certainly even, the preceding work tells us that any prime factor of must take on the form p=64k+1, for some integer k. We can thus check the highly specialized numbers for different values of k, and check to see if they are (1) prime and (2) divide evenly into 4,294,967,297 .

.

.

.

Euler did this, checking all number k=1,..,9 and when he hit k=10 p=64(10)+1=641. 641, a prime and does indeed divide .

**Q.E.D.**

By Euler’s previously mentioned theorem, primes that come in the form p=4k+1 have one and only one way to write them as the sum of two squares. Notice,

So indeed it can be written as p=4k+1. But it is straightforward to check numerically,

While simultaneously,

Therefore the way it can be written as the sum of two squares is not unique, hence cannot be prime.

Fermat primes, have been debunked for n=5, then for n=6, and n=7.

As of 1988, mathematicians know that , , and are all composite.

The assumption by Fermat that *all* number of this form are prime is clearly false and for no primes of this form have been found.

**Additional Suggested Reading**: Epilogue, Chapter 10

**Assignment:** None