



## Fermat's Little Theorem

November, 2003

If  $p$  is a prime number and if  $p$  does not divide  $a$ , then  $a^{p-1} \equiv 1 \pmod{p}$ . This fact is sometimes known as Fermat's Little Theorem. There is a generalization: if  $\mathbf{j}(n)$  is the number of positive integers less than  $n$  and relatively prime to  $n$ , and if  $a$  and  $n$  are relatively prime, then  $a^{\mathbf{j}(n)} \equiv 1 \pmod{n}$ . This is a generalization because  $n$  is prime exactly when  $\mathbf{j}(n) = n-1$ . The generalization is sometimes known as the Euler-Fermat Theorem.

Fermat was not the first to discover Fermat's Little Theorem, and Euler was not the first to prove it. Both Fermat and Leibniz proved it first, though Euler seems to have been the first one to *publish* a proof. In fact, over the course of forty years, Euler published at least three different proofs; more than that depending on how "different" you think proofs have to be to be called "different." Here, we are going to look at the first of those three proofs, and at how Euler came to discover it.

Our story begins, appropriately, with Fermat, though not with Fermat's Little Theorem. While he described the result in a letter to Marin Mersenne in 1640 and he said he had a proof, he never published the result or the proof. Instead, we begin with a conjecture Fermat mentioned in several letters in the 1640's and 1650's, to Frenicle de Bessy, Pascal, Carcavi and others, claiming that all numbers of the form  $F_n = 2^{2^n} + 1$  were prime. These numbers are now known as Fermat numbers. All of these people tried their hands at a proof. Frenicle de Bessy claimed a proof, but it does not survive.

Let us jump forward about sixty years to 1729, when a 22-year old Leonhard Euler works at the Imperial Academy of Sciences in St. Petersburg. Christian Goldbach is Secretary of the Academy, and one of Euler's superiors. Euler and Goldbach exchange letters for more than 35 years. At the end of his very first letter of this long series, Goldbach remarks

P. S. Notane Tibi est *Fermatiani* observatio omnes numeros hujus formulae  $2^{2^n} + 1$ , nempe 3, 5, 17, etc. esse primos, quam tamen ipse fatebatur se demonstrare non posse et post eum nemo, quod sciam, demonstravit.

P. S. Note the observation of Fermat that all numbers of this form  $2^{2^x} + 1$ , that is 3, 5, 17, etc., are primes, which he himself admits that he was not able to prove, and, as far as I know, nobody else has proved it either.

Three years later, in a five-page paper that now bears the index number E26, Euler shows that the  $F_5 = 4,294,967,297 = 641 \cdot 6,700,417$ . That is, Fermat was wrong. At the end of the paper, Euler adds six “theorems” of his own, things he believes to be true but cannot prove. Yet.

The first of these six “theorems” is exactly Fermat’s Little Theorem, though the “(mod  $n$ )” notation has not yet been introduced. Three of the other “theorems” are special cases of the Euler-Fermat Theorem. At the time, Euler can’t prove any of them.

By 1736, Euler makes great progress in discovering ways to prove theorems in number theory. In another five-page paper, he states and proves Fermat’s Little Theorem. In describing his proof, we will use his notation, though some of it could be simplified a bit by using modern notation, and, where possible, we will use his words, though translated from Latin into English. He states the theorem thus:

*With  $p$  signifying a prime number, the formula  $a^p - 1$  will always be able to be divided by  $p$ , unless  $a$  itself is divisible by  $p$ .*

Euler plans to prove this by mathematical induction on  $a$ , but he does not expect his readers necessarily to be familiar with the technique, so he explains his steps carefully and breaks the steps into a number of lemmas. He feels it safe to omit the cases  $p = 2$  and also  $a = 1$ , and begins with  $a = 2$ . He claims

*With  $p$  signifying an odd prime number, then any formula  $2^{p-1} - 1$  will always be able to be divided by  $p$ .*

For his proof, he wrote 2 as  $1 + 1$  to get

$$(1+1)^{p-1} = 1 + \frac{p-1}{1} + \frac{(p-1)(p-2)}{1 \cdot 2} + \frac{(p-1)(p-2)(p-3)}{1 \cdot 2 \cdot 3} + \frac{(p-1)(p-2)(p-3)(p-4)}{1 \cdot 2 \cdot 3 \cdot 4} + \text{etc.}$$

where, Euler reminds us, the number of terms here is  $= p$ , which is an odd number. Note that Euler does not have a modern notation for the binomial coefficients, nor does he have the modern  $\sum$  - notation.

Next, Euler subtracts 1 from both sides, to get  $(1+1)^{p-1} - 1$  on the left and an even number of terms on the right. Those terms on the right form pairs of consecutive binomial coefficients. Euler applies the well-known identity on binomial coefficients that we now write as  $\binom{p-1}{k-1} + \binom{p-1}{k} = \binom{p}{k}$ .

This gives him

$$2^{p-1} - 1 = \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-2)(p-3)}{1 \cdot 2 \cdot 3 \cdot 4} + \frac{p(p-1)(p-2)(p-3)(p-4)(p-5)}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6} + \text{etc.}$$

On the right, there are  $\frac{p-1}{2}$  terms, the last of which is  $p$ . Each term on the right is divisible by  $p$ , so the left hand side must also be divisible by  $p$ . Q. E. D.

Euler offers an alternate proof that is simpler. He begins with

$$2^p = (1+1)^p = 1 + \frac{p}{1} + \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} + \dots + \frac{p}{1} + 1$$

Subtracting  $2 = 1 + 1$  from both sides leaves

$$2^p - 2 = \frac{p}{1} + \frac{p(p-1)}{1 \cdot 2} + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} + \dots + \frac{p}{1}.$$

Obviously,  $p$  divides the right hand side, hence  $p$  divides  $2^p - 2$ . Since  $p$  is odd, it must divide  $2^{p-1} - 1$ . Q. E. D.

Euler also proves the case  $a = 3$  separately.

*With  $p$  denoting any prime number except 3, any formula  $3^{p-1} - 1$  will always be able to be divided by  $p$ .*

Euler patterns his proof after his second proof of the case  $a = 2$ , and writes

$$3^p = (1+2)^p = 1 + \frac{p}{1} \cdot 2 + \frac{p(p-1)}{1 \cdot 2} \cdot 4 + \frac{p(p-1)(p-2)}{1 \cdot 2 \cdot 3} \cdot 8 + \dots + \frac{p}{1} \cdot 2^{p-1} + 2^p$$

Now, Euler subtracts  $1 + 2^p$  from both sides, and juggles the left hand side a bit to get

$$3^p - 2^p - 1 = 3^p - 3 - 2^p + 2 = (3^p - 3) - (2^p - 2).$$

This leaves a factor of  $p$  in every term of the right hand side, hence  $p$  must divide the right hand side.

The previous theorem showed that  $p$  divides  $2^p - 2$ , hence  $p$  must also divide  $3^p - 3$ . Since  $p$  is not 3, this leaves that  $p$  divides  $3^{p-1} - 1$ . Q. E. D.

Euler is now ready to do his general induction step.

*With  $p$  denoting any prime number, if  $a^p - a$  can be divided by  $p$ , then that same prime  $p$  will divide any formula  $(a+1)^p - a - 1$ .*

Euler's calculations are identical to those in the case  $a = 3$ , with the 3's replaced with  $a$ 's.

For his readers who are not familiar with mathematical induction, Euler concludes by explaining why the hard work is finished. His explanation is complete, but not all that clear. He showed that if  $a^p - a$  is divisible by  $p$ , then so also is  $(a+1)^p - a - 1$ . It follows that  $(a+2)^p - a - 2$  is also divisible by  $p$ , as is  $(a+3)^p - a - 3$ , and, in general  $(a+b)^p - a - b$ . Since the theorem is true for  $a = 2$ , then any formula of the form  $(b+2)^p - b - 2$ , whatever value is substituted for  $b$ . This shows that  $a^p - a$  is always divisible by  $p$ .

Euler finishes with a brief remark that this implies that if  $p$  does not divide  $a$ , then  $p$  divides  $a^{p-1} - 1$ , as promised.

Fermat's Little Theorem has been proved in many ways. Probably only the Pythagorean Theorem has been proved in more ways. Over the course of his career, Euler himself will give at least two other proofs, and those may be topics for future columns.

As a final note, Euler refers, at various times, to at least ten different results as "a theorem of Fermat," but the result we now call "Fermat's Little Theorem" was not one of them. When he first discovered the theorem in 1732, he apparently did not know of Fermat's work on the subject.

---

Ed Sandifer ([SandiferE@wcsu.edu](mailto:SandiferE@wcsu.edu)) is Professor of Mathematics at Western Connecticut State University in Danbury, CT. He is an avid marathon runner, with 31 Boston Marathons on his shoes, and he is Secretary of The Euler Society ([www.EulerSociety.org](http://www.EulerSociety.org))

---

*How Euler Did It* is updated each month.

Copyright ©2003 Ed Sandifer