
	<h1>How Euler Did It</h1> <p>by Ed Sandifer</p>	
---	---	---

Factoring F_5

March 2007

Two names stand large in the history of number theory, Pierre de Fermat (1601-1665) and Leonhard Euler (1707-1783). Fermat, sometimes called The Great Amateur, was a part-time mathematician, a contemporary and rival of Descartes. His “real job” was as a judge in Toulouse, France. At the time, judges were expected to avoid the company of people on whom they might be required to pass judgment, so Fermat lived in comparative isolation, away from the people of Toulouse, with plenty of time to work on his mathematics. He kept in touch with current developments through his correspondence with Marin Mersenne.

Fermat worked on many of the same problems as René Descartes (1596-1650). They independently discovered analytic geometry, but since Fermat seldom published anything, *Cartesian coordinates* bear the name of Descartes, not Fermat. Both tried to “restore” the lost books of Apollonius, and when Fermat discovered a pair of amicable numbers, Descartes retaliated by finding another pair.¹ Both discovered techniques for finding the line tangent to a given curve at a given point, and Fermat showed how to find the area under a curve given by the equation $y = x^n$, as long as n was not equal to -1 . All of this was very important in setting the stage for the discovery of calculus, later in the 1600’s. Fermat and Descartes did not like each other very much. In fact, some people describe their relationship as a “feud,” but it seems that Descartes resented Fermat more than Fermat disliked Descartes. They probably never met.

Fermat followed many of the mathematical traditions of the 17th century. Rather than provide proofs, he more often simply announced results and left the proofs of his claims as challenges to his readers. Others he wrote in the margins of his books. Those margin notes became known to the mathematical world when his son, Samuel, published his notes and papers in 1666, just after Pierre’s death. This is how the conjecture we call Fermat’s Last Theorem² became known to the rest of the mathematical world. Most of Fermat’s conjectures were neither as difficult nor as influential as the Last Theorem. For example, in another of his margin notes, he claimed

Theorem: No triangular number other than 1 can be a fourth power.

¹ To be fair, both pairs had been known to Arab mathematicians for a few hundred years, but the discoveries were new to Europe.

² The conjecture was that $x^n + y^n = z^n$ has no non-trivial integer solutions if $n > 2$. Its proof eluded mathematicians for over 300 years until Andrew Wiles solved it in the 1990’s.

This is interesting, but it can hardly be considered important.

In 1738, Euler proved this particular claim to be true, [E98] and over the course of his career, Euler also proved (or disproved) almost all of Fermat's other conjectures, including Fermat's Little Theorem and Fermat's Last Theorem for the cases $n = 3$ and $n = 4$. Fermat's Last Theorem is called the "Last" not because it was the last conjecture Fermat ever made, but because after Euler got through with them, it was the last important one that remained to be proved or disproved.

Euler's interest in number theory was first sparked by another Fermat conjecture, that for all values of n , the number $F_n = 2^{2^n} + 1$ is a prime number. Fermat had made his conjecture in several of his letters during the 1630's and 1640's. These numbers are now called *Fermat numbers*, and, indeed, for small values of n , they give us 3, 5, 17, 257 and 65537, all of which are prime numbers. The next Fermat number, taking $n = 5$, is 4,294,967,297.

Euler's mentor in St. Petersburg, Christian Goldbach, alerted Euler to the conjecture in 1729. Euler responded almost immediately that he could make no progress on the problem, but by 1732, close to a hundred years after Fermat had originally made the conjecture, Euler had a solution: Fermat was wrong. In Euler's first paper on number theory [E26] Euler announced that 641 divides 4,294,967,297. Later in that same paper, Euler added six of his own conjectures, some equivalent to Fermat's Little Theorem, that if p is prime and if p does not divide a , then p divides $a^{p-1} - 1$, and others that would turn out to be consequences of the Euler-Fermat theorem. See [S1] or [S2] for details.

What Euler did *not* tell us in E26 was how he thought to try to divide 4,294,967,297 by 641. He hadn't simply been dividing by prime numbers until he got to 641. He had a much better way, but he waited about fifteen years, until E134, to reveal that secret.

The main purpose of E134, "Theoremata circa divisores numerorum," (Theorems about divisors of numbers) is to give Euler's first proof of Fermat's Little Theorem, but we will be looking at some of the other contents of this paper. After the main result of the paper, he proves a slightly more general version of Fermat's Little Theorem:

Theorem 4: If neither of the numbers a and b is divisible by the prime number p , then every number of the form $a^{p-1} - b^{p-1}$ will be divisible by p .

He uses this to prove a theorem about the divisors of numbers that are the sum of two squares:

Theorem 5: The sum of two squares $aa + bb$ will never be divisible by a prime number of the form $4n - 1$ unless both of the roots a and b are divisible by $4n - 1$.

Euler is really interested in the contrapositive of Theorem 5, that if a and b do not have a common prime factor of the form $4n - 1$, then all of the odd prime factors of $aa + bb$ must have the form $4n + 1$.

Euler's Theorems 6 and 7 extend the contrapositive of Theorem 5 to sums of two 4th powers (divisible only by odd primes of the form $8n + 1$) and 8th powers (prime divisors of the form $16n + 1$) before giving the general theorem in the form:

Theorem 8: The sum of two such powers $a^{2^m} + b^{2^m}$, in which the exponents are powers of two, will not admit any divisors except those that are contained in the form $2^{m+1}n + 1$

When Euler writes “two such powers,” he is being just a little bit sloppy, and may be overlooking a condition. He probably means that a and b are relatively prime, but the claim is true if a and b have no common factors except those of the form $2^{m+1}n + 1$.

As Euler then tells us, this gives us a way to try to factor $2^{2^5} + 1$, or 4,294,967,297. Since both 4,294,967,296 and 1 are 32^{nd} powers, and since they are relatively prime, and since $32 = 2^5$, Euler’s Theorem 8 tells us that any prime divisors of 4,294,967,297 must have the form $64n + 1$. We can simply try different values of n , until we find a divisor, reach the square root of 4,294,967,297 or give up. Let’s try it:

$n = 1$	$64n + 1 = 65$	65 is not prime.
$n = 2$	$64n + 1 = 129$	129 is not prime.
$n = 3$	$64n + 1 = 193$	193 is prime, but does not divide 4,294,967,297.
$n = 4$	$64n + 1 = 257$	257 is prime, but does not divide 4,294,967,297.
$n = 5$	$64n + 1 = 321$	321 is not prime.
$n = 6$	$64n + 1 = 385$	385 is not prime.
$n = 7$	$64n + 1 = 449$	449 is prime, but does not divide 4,294,967,297.
$n = 8$	$64n + 1 = 513$	513 is not prime.
$n = 9$	$64n + 1 = 577$	577 is prime, but does not divide 4,294,967,297.
$n = 10$	$64n + 1 = 641$	641 divides 4,294,967,297 with quotient 6,700,417.

We find the factor 641 after just six divisions.

Euler did not speculate in print on whether the other factor, 6,700,417, is prime. It is prime, but there is no evidence that Euler ever tried to find out.

How much more work would it have been to show that 6,700,417 is prime? Not that much. If 6,700,417 has a prime factor, it has to have one less than its square root, which is a bit over 2588, and, by Theorem 8, any such factors also would have to be of the form $64n + 1$. There are 40 integers less than 2588 of the form $64n + 1$, and we’ve already checked ten of them. Thirty remain, of which only six, 769, 1153, 1217, 1409, 1601, 2113 are prime, and none of which divide 6,700,417. Euler had already done half the work. Knowing this, we could finish the proof that 6,700,417 is prime with pencil and paper in only a few minutes.

The number 6,700,417 would have been the largest known prime number in Euler’s day. When he prepared a table of large prime numbers [E283] in 1762, the largest prime number he mentioned was 2,232,037. Some experts think that Euler knew that 6,700,417 was prime, because it would have been so easy for him prove it. Others think that Euler never thought to use those tools on this particular number, because if he had, he would have told somebody and mentioned it in E283. Experts disagree.

References:

- [E26] Euler, Leonhard, *Observationes de theoremate quodam Fermatiano aliisque ad numeros primos spectantibus, Commentarii academiae scientiarum Petropolitanae* 6 (1732/33), 1738, pp. 103-107. Reprinted in *Opera Omnia* I.2, pp. 1-5. Available online at EulerArchive.org.

- [E98] Euler, Leonhard, Theorematum quorundam arithmeti-
corum demonstrationes, *Commentarii academiae scientiarum
Petropolitanae* **10** (1738), 1747, pp. 125-146. Reprinted in *Opera Omnia* I.2, pp. 38-58. Available online at
EulerArchive.org.
- [E134] Euler, Leonhard, Theoremata circa divisores numerorum, *Novi commentarii academiae scientiarum Petropolitanae* **1**
(1747/48), 1750, pp. 20-48. Reprinted in *Opera Omnia* I.2, pp. 62-85. Available online at EulerArchive.org.
- [S1] Sandifer, Ed, "Fermat's Little Theorem," *How Euler Did It*, MAA Online, November 1993.
- [S2] Sandifer, C. Edward. *The Early Mathematics of Leonhard Euler*, MAA, 2007.

Ed Sandifer (SandiferE@wcsu.edu) is Professor of Mathematics at Western Connecticut State University in Danbury, CT. He is an avid marathon runner, with 34 Boston Marathons on his shoes, and he is Secretary of The Euler Society (www.EulerSociety.org). His new book, *The Early Mathematics of Leonhard Euler*, was published by the MAA in December 2006, as part of the celebrations of Euler's tercentennial in 2007. The MAA will be publishing a collection of the *How Euler Did It* columns during the summer of 2007.

How Euler Did It is updated each month.
Copyright ©2007 Ed Sandifer