

Fermat's Method of Infinite Descent

Although Fermat never communicated what he believed his proof of this fact to be, he did was one of the first to make use of a method of proof—the method of infinite descent—by which many facts in number theory can be proved, including the case of fourth powers in Fermat's last theorem. The basis of the method can be explained in the abstract by sketching a proof of the case of a fourth power, a proof given by Euler in 1738. Actually the proof shows that there can be no positive integers x, y, z , such that $x^4 + y^4 = z^2$. Supposing that such numbers do exist, we assume that z is the smallest positive integer for which there exist positive integers x and y satisfying this equation. Then no two of x, y , and z have a common prime factor (otherwise the fourth power of this factor could be divided out, producing a smaller z). This means that two of the numbers are odd and one is even, and in particular that z is odd. (If x and y were both odd, their fourth powers would both leave a remainder of 1 when divided by 4, implying that the square of z leaves a remainder of 2 when divided by 4. But obviously the square of an even number leaves no remainder when divided by 4.) Assume that x is odd and y is even. Then $x^4 = (z + y^2)(z - y^2)$. Since z and y have no common factor, it follows that the odd numbers $z + y^2$ and $z - y^2$ also have no common factor. Since they are relatively prime and their product is a fourth power, each of the factors is a fourth power, that is, there exist (odd) integers u, v , such that $z - y^2 = u^4$, $z + y^2 = v^4$, and $uv = x$. Now $(v^2 - u^2)(v^2 + u^2) = v^4 - u^4 = 2y^2$, and since $v^2 - u^2$ and $v^2 + u^2$ have no common prime factor except 2, there exists a factorization of y ($y = \omega\zeta$) such that either

$$\begin{aligned}v^2 + u^2 &= \zeta^2 \\v^2 - u^2 &= 2\omega^2\end{aligned}$$

or

$$\begin{aligned}u^2 + \omega^2 &= v^2 \\u^2 + v^2 &= 2\zeta^2\end{aligned}$$

The first possibility can be ruled out, since the sum of two odd square integers cannot be a perfect square, for the same reason as given above: it leaves a remainder of 2 when divided by 4. It then follows from the first equation in the second pair that u, ω , and v form a Pythagorean triple, and as shown in Problem 7.18, this means there exist integers ξ and η such that $u = \xi^2 - \eta^2$, $\omega = 2\xi\eta$, and $v = \xi^2 + \eta^2$. Then the second equation says that $\xi^4 + \eta^4 = \zeta^2$. Since $\zeta < y < z$, this contradicts the assumed minimality of z .