The *second case* holds for the exponent p when there do not exist integers x, y, z, all different from 0, such that $p|xyz$, $\gcd(x,y,z) = 1$ and $x^p + y^p = z^p$.

2. Early Attempts

It was already known in antiquity that a sum of two squares of integers may well be the square of another integer. Pythagoras was supposed to have proven that the lengths a, b, c of the sides of a right-angle triangle satisfy the relation

$$a^2 + b^2 = c^2;$$

so the above fact just means the existence of such triangles with sides measured by integers.

But the situation is already very different for cubes, biquadrates and so on. Fermat's proof for the case of biquadrates is very ingenious and proceeds by the method which he called *infinite descent*. Roughly, it goes as follows: Suppose a certain equation $f(X,Y,Z) = 0$ has integral solutions a, b, c, with $c > 0$, the method just consists in finding another solution in integers a', b', c' with $0 < c' < c$. Repeating this procedure a number of times, one would reach a solution a'', b'', c'', with $0 < c'' < 1$, which is absurd. This method of infinite descent is nothing but the well-ordering principle of the natural numbers.

Little by little Fermat's problem aroused the interest of mathematicians and a dazzling array of the best minds turned to it.

Euler considered the case of cubes. Without loss of generality, one may assume $x^3 + y^3 = z^3$ where x, y, z are pairwise relatively prime integers, x, y are odd, so $x = a - b$, $y = a + b$. Then $x + y = 2a$, $x^2 - xy + y^2 = a^2 + 3b^2$ and $z^3 = x^3 + y^3 = 2a(a^2 + 3b^2)$, where the integers $2a$, $a^2 + 3b^2$ are either relatively prime or have their greatest common divisor equal to 3. Euler was led to studying odd cubes $a^2 + 3b^2$ (with a, b relatively prime), and forms of their divisors; he concluded the proof by the method of infinite descent. The properties of the numbers $a^2 + 3b^2$ which were required had to be derived from a detailed study of divisibility, and therefore were omitted from the proof published in Euler's book on algebra (1822). This proof, with the same gap, was reproduced by Legendre. Later, mathematicians intrigued by the missing steps were able without much difficulty, to reconstruct the proof on a sound basis. In today's language, numbers of the form $a^2 + 3b^2$ are norms of algebraic integers of the quadratic extension $\mathbb{Q}(\sqrt{-3})$ of the rational field $\mathbb{Q}$ and the required properties can be deduced from the unique factorization theorem, which is valid in that field.

Gauss gave another proof for the case of cubes. His proof was not "rational" since it involved complex numbers, namely those generated by the cube root of unity $\zeta = (-1 + \sqrt{-3})/2$, i.e., numbers from the quadratic field $\mathbb{Q}(\sqrt{-3})$. He consciously used the arithmetic properties of this field. The

underlying idea was to call "integers" all numbers of the form $(a + b\sqrt{-3})/2$ where a, b are integers of the same parity; then to define divisibility and the prime integers, and to use the fact that every integer is, in a unique way, the product of powers of primes. Of course some new facts appeared. First, the integers $\pm\zeta$, $\pm\zeta^2$ that divide 1 are "units" since $\zeta\zeta^2 = 1$ and therefore should not be taken into account so to speak, in questions of divisibility. Thus, all the properties have to be stated "up to units". Secondly, the unique factorization, which was taken for granted, was by no means immediate—in fact it turned out to be false in general. I shall return to this later.

Gauss's proof was an early incursion into the realm of number fields, i.e., those sets of complex numbers obtained from the roots of polynomials by the operations of addition, subtraction, multiplication, and division.

In the 1820s a number of distinguished French and German mathematicians were trying intensively to prove Fermat's theorem.

In 1825, G. Lejeune Dirichlet read at the Académie des Sciences de Paris a paper where he attempted to prove the theorem for the exponent 5. In fact his proof was incomplete, as pointed out by Legendre, who provided an independent and complete proof. Dirichlet then completed his own proof, which was published in Crelle Journal, in 1828.

Dirichlet's proof is "rational", and involves numbers of the form $a^2 - 5b^2$. He carefully analyzed the nature of such numbers which are 5th powers when either a, b are odd, or a, b have different parity, and 5 does not divide a, 5 divides b, and a, b are relatively prime. Nowadays the properties he derived can be obtained from the arithmetic of the field $\mathbb{Q}(\sqrt{5})$. In this field too, every integer has a unique factorization. Moreover every unit is a power of $(1 + \sqrt{5})/2$, which is of crucial importance in the proof. Of course, for Dirichlet this knowledge took the form of numerical manipulations which lead to the same result.

In 1832 Dirichlet settled the theorem for the exponent 14.

The next important advance was due to Lamé, who, in 1839 proved the theorem for $n = 7$. Soon after, Lebesgue simplified Lamé's proof considerably by a clever use of the identity,

$$\begin{aligned}(X + Y + Z)^7 - (X^7 + Y^7 + Z^7) &= 7(X + Y)(X + Z)(Y + Z) \\ &\quad \times [(X^2 + Y^2 + Z^2 + XY + XZ + YZ)^2 + XYZ(X + Y + Z)]\end{aligned}$$

already considered by Lamé.

While these special cases of small exponents were being studied, a very remarkable theorem was proved by Sophie Germain, a French mathematician.

Previously Barlow, and then Abel, had indicated interesting relations that x, y, z must satisfy if $x^p + y^p = z^p$ (and x, y, z are not zero). Through clever manipulations, Sophie Germain proved:

If p is an odd prime such that $2p + 1$ is also a prime then the first case of Fermat's theorem holds for p.