which has one variation in sign, hence exactly one positive root. It follows that equation (1) has exactly one negative root. Descartes's rule of signs is a special case of what logicians call *elimination of quantifiers.* Descartes wrote two other books, the *Meditations* (1641) and *Principia Philosophicae* (1644). The latter deals with physical science and proposes the theory of vortices to explain planetary motion. This theory was later refuted by Newton.

The *Meditations* contains a 'geometrical proof' of the existence of God:

> existence can no more be separated from the essence of God than the idea of a mountain from that of a valley, or the equality of its three angles to two right angles, from the essence of a triangle (Meditation V).

In other words, God exists because existence is just one of the defining properties of God.

Fermat was a councillor for the parliament of Toulouse, and only did mathematics in his spare time. He published almost nothing during his lifetime; his contributions to mathematics are contained in his correspondence (e.g., with Mersenne) and in the papers that were found after his death. Nonetheless, he is considered to be the greatest amateur mathematician of all times.

Fermat introduced his version of analytic geometry in his *Ad Locos Planos et Solidos Isagoge.* He also collaborated on probability theory with Pascal. In addition, Fermat studied tangents to curves, maxima and minima, and areas under curves, coming very close to discovering calculus. Fermat's methods were influenced by those of his contemporaries, Cavalieri and Wallis, whom we shall meet in the next Chapter.

Today Fermat is best known for his contributions to the theory of numbers. Diophantus knew that a prime number of the form $4n - 1$ is never the sum of two squares. Fermat went further and proved that every prime of the form $4n + 1$ can be written as the sum of two squares in exactly one way. He also noted that every odd prime $p$ can be written as the difference of two squares in one and only one way.

The last statement is easy to prove. Indeed, $p = (\frac{1}{2}(p+1))^2 - (\frac{1}{2}(p-1))^2$ where $\frac{1}{2}(p+1)$ and $\frac{1}{2}(p-1)$ are both integers, since $p$ is odd. On the other hand, if $p = x^2 - y^2 = (x+y)(x-y)$, then $x + y = p$ and $x - y = 1$ (since $p$, being prime, has no factors except 1 and $p$). This gives $x = \frac{1}{2}(p+1)$ and $y = \frac{1}{2}(p+1)$ as before.

Fermat's so-called 'Little Theorem' asserts that, if $p$ is a prime and $a$ is an integer which is not a multiple of $p$, then $a^{p-1} - 1$ is a multiple of $p$. There are many proofs of this theorem. One of them depends on the

Binomial Theorem (known to the Chinese centuries before Fermat):

$$(x+1)^p = x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + 1,$$

where

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 1}$$

is an integer. If $0 < k < p$, then $p$ is not a factor of $k(k-1)\cdots 1$. Since $p$ is a factor of

$$\binom{p}{k}k(k-1)\cdots 1 = p(p-1)\cdots(p-k+1)$$

it follows that $p$ is a factor of $\binom{p}{k}$ when $0 < k < p$. Hence

$$(x+1)^p = x^p + 1 + mp$$

for some integer $m$. If $x = 1$, we obtain $2^p = 2 + mp$, so that $p$ is a factor of $2^{p-1} - 1$. If $x = 2$, we get $3^p = 2^p + 1 + m'p = 2 + mp + 1 + m'p = 3 + (m + m')p$, so that $p$ is a factor of $3^{p-1} - 1$. Continuing in the same way (using mathematical induction), we see that, for all $a$, $a^p = a + np$ for some integer $n$. Thus $p$ divides $a^p - a = a(a^{p-1} - 1)$ and the theorem follows (since $p$ does not divide $a$).

More famous still is Fermat's 'Last Theorem'. This was proved in 1994 by Andrew Wiles.

What is Fermat's 'Last Theorem'? In reading Bachet's translation (from Greek into Latin) of the work of Diophantus, Fermat came across the equation $x^2 + y^2 = z^2$ with its solutions (e.g., $x = 3, y = 4$ and $z = 5$). Fermat wrote in the margin of the book that he had been able to prove that the equation

$$x^n + y^n = z^n$$

has no positive integer solutions for $n > 2$, but that the margin was too small for him to write the proof there. (Of course, $0^3 + 7^3 = 7^3$, but here one of the integers is 0; this is called a 'trivial' solution.)

It is quite possible that Fermat had a proof of the nonexistence of the positive integer solutions for $n = 3$. We still have his proof of the 'Last Theorem' for the special case $n = 4$. However, it is unlikely that he ever had a proof for the complete theorem.

Legendre disposed of the case when $n = 5$ in 1823, and Dirichlet handled the case when $n = 14$ in 1832. In 1849 Kummer made a big step forward and was able to vindicate Fermat's statement for all $n < 100$ except 37, 59 and 67. Before 1994, thanks to the help of the computer, we knew that Fermat was right for all $n < 10^8$ or so, but a proof of the general theorem still escaped us. In 1994, however, Wiles gave a complete proof, for all $n$.