The Proof of Fermat's Last Theorem by R. Taylor and A. Wiles

Gerd Faltings

The proof of the conjecture mentioned in the title was finally completed in September of 1994. A. Wiles announced this result in the summer of 1993; however, there was a gap in his work. The paper of Taylor and Wiles does not close this gap but circumvents it. This article is an adaptation of several talks that I have given on this topic and is by no means about my own work. I have tried to present the basic ideas to a wider mathematical audience, and in the process I have skipped over certain details, which are in my opinion not so much of interest to the nonspecialist. The specialists can then alleviate their boredom by finding those mistakes and correcting them.

Elliptic Curves

For our purposes an elliptic curve E is given as the set of solutions (x, y) of an equation $y^2 = f(x)$, where $f(x) = x^3 + \dots$ is a polynomial of degree three. Usually E is defined over the rational numbers $\mathbb{Q}$; that is, the coefficients of f are in $\mathbb{Q}$. We also demand that all three zeros of f are distinct (E is "nonsingular"). We may consider E as those solutions in $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, denoted, respectively, $E(\mathbb{Q})$, $E(\mathbb{R})$, and $E(\mathbb{C})$. One usually includes in this set an infinitely distant point, denoted ∞. With this addition, the solution set has the structure of an abelian group, with ∞ as the neutral element. The inverse of (x, y) is $(x, -y)$, and the sum of three points vanishes if they lie on a line. The group addition is given by algebraic functions. As a group $E(\mathbb{Q})$ is finitely generated (Mordell's Theorem), $E(\mathbb{R})$ is isomorphic to $\mathbb{R}/\mathbb{Z}$ or to $\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and $E(\mathbb{C}) \cong \mathbb{C}/\text{lattice}$ (for example, $y^2 = x^3 - x$ yields the lattice $\mathbb{Z} \oplus \mathbb{Z}i$). For an integer n let $E[n]$ denote the n-division points, that is, the kernel of multiplication by n. Over $\mathbb{C}$ these are isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$, and the coordinates are algebraic numbers. For example, the 2-division points are exactly ∞ and the three zeros of f (where $y = 0$). The absolute Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on

Gerd Faltings is affiliated with the Max-Planck-Institute für Mathematik in Bonn, Germany.

Translated from Testausdruck DMV Mitteilungen 27. März 1995 für 2/95 *by Uwe F. Mayer, University of Utah.*