Summary of the Proof of Fermat's Last Theorem

BY DEREK BUCHANAN

Theorem. *There are no positive integers a, b, c, n with $n > 2$ such that $a^n + b^n = c^n$.*

Proof. An **elliptic curve** E is given by $y^2 = c_3x^3 + c_2x^2 + c_1x + c_0 = g(x)$, no repeated roots, $c_0, c_1, c_2, c_3, x \in \mathbb{R}$. E is over $\mathbb{Q}$ if $c_0, c_1, c_2, c_3 \in \mathbb{Q}$. If Fermat's Last Theorem is false, there is a elliptic **Frey curve** $y^2 = x(x - A^n)(x - B^n)$, where A and B are solutions for a and b in Fermat's equation. This is defined over $\mathbb{Q}$. By change of coordinates, one can change the equation to a **normal form** $g'(x') = y'^2 = x'^3 + a'x' + b'$. For this to not have repeated roots, its discriminant $\Delta = -16(27b'^2 + 4a'^3) \neq 0$. The discriminant Δ_M with fewest prime factors, is called the **minimal discriminant**. There are prime numbers p such that $\Delta_M \equiv 0 (\text{mod } p)$.

p is called **bad** if $\begin{cases} g'(x') (\text{mod } p) \text{ has 2 different zeros, in which case } \gamma_p = 1, \text{ or} \\ g'(x') (\text{mod } p) \text{ has 3 zeros coincide, in which case } \gamma_p = 2. \end{cases}$

The **conductor** $\prod_{p \text{ bad}} p^{\gamma_p}$ of E is denoted N_E. If N_E is squarefree E is called **semistable**. For Frey curves, $N_E = \prod_{p|ABC} p \Rightarrow N_E$ is squarefree $\Rightarrow$ Frey curves are semistable.

For $s \in \mathbb{C}$ the **L-function** of E is $L(E, s) = \sum_{p \text{ prime}} \frac{a_p}{p^s}$, $a_p = p + 1 - A_p$, $A_p =$ the number of $\mathbb{Q}$-points on E mod p.

For $z \in \mathbb{C}$, a function f is **modular of weight** k if $f\left(\frac{\alpha z+\beta}{\gamma z+\zeta}\right) = (\gamma z + \zeta)^k f(z)$ for $\Im(z) > 0$ $(\mathcal{H})$ and any $\alpha, \beta, \gamma, \zeta \in \mathbb{C}$, and some $k \in \mathbb{N}$. f is a **modular form** if it is analytic (differentiable). For a modular form f, $f(z + 1) = f(z)$ and $f(z) = \sum_{m=0}^{\infty} b_m e^{2\pi imz}$, $z \in \mathcal{H}$, for some $b_m \in \mathbb{C}$. The **L-function** of f is $L(f, s) = \sum_{m=1}^{\infty} \frac{b_m}{m^s}$.

E is **modular** if there exists a modular form f such that $L(E, s) = L(f, s)$ for all s. All Frey curves are nonmodular and all semistable elliptic curves over $\mathbb{Q}$ are modular. (In fact all elliptic curves over $\mathbb{Q}$ are modular.) A Frey curve exists if an only if Fermat's Last Theorem is false. If Frey curves exist, they are nonmodular semistable elliptic curves over $\mathbb{Q}$. But all such curves are modular - contradiction. Therefore Frey curves do not exist and therefore Fermat's Last Theorem is true! $\square$

References.

http://www4.tpgi.com.au/nanahcub/flt.pdf

http://math.stanford.edu/~lekheng/flt/bcdt.pdf

Updated April 3, 2006