An Introduction to the Proof of Fermat's Last Theorem

Jason Swanson

Fall 1998

It seems an undisputed fact in the mathematical community that the long sought after proof of Fermat's Last Theorem has indeed been found. Though a member of the mathematical community myself, I am in the unfortunate position of being unable to either dispute or attest to the validity of this claim. I have been told that the amount of time required to obtain knowledge enough to critique the proof would be measured in years. After my brief survey of the mathematics involved, I'm reasonably convinced that this is true. It's unfortunate that the solution to such a classic problem as this has come to us in a way understandable by only the most learned experts. It is for this reason that I write this paper. My hope is that it will serve as an initial guide to anyone interested in learning what is necessary to verify for themselves the validity of the proof of Fermat's Last Theorem.

Fermat's Last Theorem, until recently, was not a theorem at all, but a conjecture. The challenge was to prove or disprove the claim that there are no non-zero integers x, y, z such that $x^n + y^n = z^n$ when $n \geq 3$. A proof of this claim has been provided by Andrew Wiles. This claim is actually a corollary to a larger theorem that Wiles proved, namely that all semistable elliptic curves are modular. This paper will provide a very brief sketch of what this means and how it implies Fermat's Last Theorem.

I. The Projective Plane

Let K be a field and define a relation on $K^3 - \{0\}$ by

$$(x, y, z) \sim (x', y', z') \text{ iff } \exists\, l \in K^* \text{ such that } (x, y, z) = l\,(x', y', z')$$

It can be easily verified that this is an equivalence relation and the **projective plane**, $\mathbf{P}_K^2$, is defined to be the set of equivalence classes in $K^3 - \{0\}$ under this relation. Now define $P \subset \mathbf{P}_K^2$ to be

$$P = \left\{a \in \mathbf{P}_K^2 \colon \exists\, (x, y, z) \in a,\ z \neq 0\right\}$$

Since if $(x, y, z) \sim (x', y', z')$, then $z = 0$ if and only if $z' = 0$, it follows that, equivalently,

$$P = \left\{a \in \mathbf{P}_K^2 \colon \forall (x, y, z) \in a,\ z \neq 0\right\}$$

Now let $p : P \to K^2$ be defined as

$$p(a) = \left(\frac{x}{z}, \frac{y}{z}\right), \text{ where } (x, y, z) \in a$$

To see that this is a well defined function, let $(x, y, z), (x', y', z') \in a$ and $l \in K^*$ such that $(x, y, z) = l\,(x', y', z')$. Since $z' \neq 0$, $l = \frac{z}{z'}$. If $x' \neq 0$, then $l = \frac{x}{x'} = \frac{z}{z'}$. If $x' = 0$, then $x = lx' = 0$. In either case, $\frac{x}{z} = \frac{x'}{z'}$. Similarly, $\frac{y}{z} = \frac{y'}{z'}$. Hence, $p\,(a)$ is defined independently of the choice of $(x, y, z) \in a$. Now suppose $p\,(a) = p\,(b)$. Then $\exists\, (x, y, z) \in a$, $(x', y', z') \in b$ such that

$\left(\frac{x}{z},\frac{y}{z}\right)=\left(\frac{x'}{z'},\frac{y'}{z'}\right)$. Since $z, z' \neq 0$, let $l=\frac{z}{z'}\in K^*$. Then $x=\frac{zx'}{z'}=lx'$. Similarly $y = ly'$, i.e. $a = b$ and p is injective. Now let $(p, q)\in K^2$. If a denotes the equivalence class of $(p, q, 1)$ in P, then $p(a) = (p, q)$ and p is surjective. Thus there is a one-to-one correspondence between K^2 and the proper subset, $P \subset \mathbf{P}_K^2$. It is for this reason that $\mathbf{P}_K^2$ is thought of as an extension of K^2 and the points in $\mathbf{P}_K^2 - P$ are called "the points at infinity".

II. Curves in the Projective Plane

The degree of a monomial is the sum of the powers of its variables. The total degree of a polynomial is the maximum degree of the monomials of which it is a sum. If the total degree of a polynomial is equal to the degree of each of the monomials of which it is a sum, then that polynomial is said to be **homogeneous**.

Let $f(x, y)$ be a polynomial with coefficients in K. The **corresponding homogeneous polynomial** is defined to be

$$\tilde{f}(x,y,z)=z^n f\left(\frac{x}{z},\frac{y}{z}\right),$$

where n is the total degree of f. If cx^iy^j is a monomial in f, then the corresponding term in $\tilde{f}$ is $cx^iy^jz^{n-(i+j)}$. Since $n \geq i + j$, $\tilde{f}$ is indeed a polynomial and since $i + j + n - (i + j) = n$, $\tilde{f}$ is indeed homogeneous and of degree n.

The equation $f(x, y) = 0$ defines a curve $C = \{(x, y)\in K^2 : f(x, y) = 0\}$. The **projective completion** of C is the curve

$$C'=\left\{a\in\mathbf{P}_K^2:\exists\,(x,y,z)\in a,\ \tilde{f}(x,y,z)=0\right\}$$

Since $\forall\, l\in K^*,\ \tilde{f}(lx, ly, lz) = l^n\tilde{f}(x,y,z)$, it follows that, equivalently,

$$C'=\left\{a\in\mathbf{P}_K^2:\forall(x,y,z)\in a,\ \tilde{f}(x,y,z)=0\right\}$$

Now consider the function, p, given above. Let $a \in C' \cap P$ and $(x, y, z)\in a$. Then $\tilde{f}(x,y,z)=0=z^n f(p(a))$. Since $z \neq 0$, it follows that $p(a) \in C$ and, thus, $p(C' \cap P) \subset C$. Now let $(p, q)\in C$ and a denote the equivalence class of $(p, q, 1)$ in $\mathbf{P}_K^2$. Since $\tilde{f}(p, q, 1) = f(p, q) = 0$, $a\in C'$. Thus $C \subset p(C' \cap P)$, i.e. $p(C' \cap P) = C$. Since p is a bijection, we consider $C' \cap P$ to be equivalent to C, with the equivalence class of $(x, y, 1)$ in $C' \cap P$ associated with the point $(x, y)\in C$. The remaining points on C' are points at infinity.

III. Elliptic Curves

Let

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6, \qquad a_i \in \mathbf{Z}.$$

The curve $f(x, y) = 0$ is **singular** if there is a simultaneous solution in $\mathbf{C}^2$ to the equations

$$f(x,y) = 0 \qquad \frac{\partial f}{\partial x}(x,y) = 0 \qquad \frac{\partial f}{\partial y}(x,y) = 0.$$

Any such solution is called a **point of singularity**. The curve is **nonsingular** if it is not singular. If $f(x, y) = 0$ is nonsingular, then the curve

$$E(\mathbf{Q}) = \left\{a \in \mathbf{P}_{\mathbf{Q}}^2 : \forall (x,y,z) \in a,\ \tilde{f}(x,y,z) = 0\right\}$$

is called an **elliptic curve**.

IV. The Discriminant

Let $f(x, y)$ be as in section III and let $g(x,y) = 4f(x, \frac{y - a_1x - a_3}{2})$. It follows that

$$g(x,y) = y^2 - 4x^3 - b_2x^2 - 2b_4x - b_6, \text{ where}$$
$$b_2 = a_1^2 + 4a_2$$
$$b_4 = 2a_4 + a_1a_3$$
$$b_6 = a_3^2 + 4a_6$$

Now let $h(x,y) = 11664g(\frac{x - 3b_2}{36}, \frac{y}{108}) = 46656f(\frac{x - 3b_2}{36}, \frac{y - 3a_1x + 9a_1b_2 - 108a_3}{216})$. Then

$$h(x,y) = y^2 - x^3 + 27c_4x^2 + 54c_6, \text{ where}$$
$$c_4 = b_2^2 - 24b_4$$
$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

It follows that $h(x, y) = 0$ is singular if and only if $f(x, y) = 0$ is singular.

PROOF

Let $u(x,y) = \frac{x - 3b_2}{36}$ and $v(x,y) = \frac{y - 3a_1x + 9a_1b_2 - 108a_3}{216}$. Note that

$$\frac{\partial h}{\partial x}(x,y) = 1296\frac{\partial f}{\partial x}(u(x,y), v(x,y)) - 648a_1\frac{\partial f}{\partial y}(u(x,y), v(x,y))$$

and

$$\frac{\partial h}{\partial y}(x,y) = 216\frac{\partial f}{\partial y}(u(x,y),v(x,y))$$

Now suppose the curve $h(x, y) = 0$ is singular. Let (x_0, y_0) be a simultaneous solution to

$$h(x,y)=0 \qquad \frac{\partial h}{\partial x}(x,y)=0 \qquad \frac{\partial h}{\partial y}(x,y)=0$$

It follows from the above equations that $(u(x_0, y_0), v(x_0, y_0))$ is a simultaneous solution to

$$f(x,y)=0 \qquad \frac{\partial f}{\partial x}(x,y)=0 \qquad \frac{\partial f}{\partial y}(x,y)=0$$

and $f(x, y) = 0$ is singular.

Now suppose $f(x, y) = 0$ is singular and let (x_0, y_0) be a simultaneous solution to

$$f(x,y)=0 \qquad \frac{\partial f}{\partial x}(x,y)=0 \qquad \frac{\partial f}{\partial y}(x,y)=0$$

Let $u'(x, y) = 36x + 3b_2$ and $v'(x, y) = 108a_2x + 216y + 108a_3$. Note that

$$\begin{pmatrix} u'(x,y) \\ v'(x,y) \end{pmatrix} = 36\begin{pmatrix} 1 & 0 \\ 3a_2 & 6 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} + 3\begin{pmatrix} b_2 \\ 36a_3 \end{pmatrix}.$$

Thus,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \frac{1}{216}\begin{pmatrix} 6 & 0 \\ -3a_1 & 1 \end{pmatrix}\begin{pmatrix} u'(x,y) \\ v'(x,y) \end{pmatrix} - \frac{1}{24}\begin{pmatrix} 2b_2 \\ 12a_3 - a_1b_2 \end{pmatrix}.$$

Now let $(x_1, y_1) = (u'(x_0, y_0), v'(x_0, y_0))$. Then $h(x_1, y_1) = 46656 f(u(x_1, y_1), v(x_1, y_1))$. But

$$\begin{pmatrix} u(x_1,y_1) \\ v(x_1,y_1) \end{pmatrix} = \frac{1}{216}\begin{pmatrix} 6 & 0 \\ -3a_1 & 1 \end{pmatrix}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} - \frac{1}{24}\begin{pmatrix} 2b_2 \\ 12a_3 - a_1b_2 \end{pmatrix} = \begin{pmatrix} x_0 \\ y_0 \end{pmatrix},$$

so $h(x_1, y_1) = 46656 f(x_0, y_0) = 0$. Similarly, $\frac{\partial h}{\partial x}(x_0, y_0) = 0$ and $\frac{\partial h}{\partial y}(x_0, y_0) = 0$. Thus, $h(x, y) = 0$ is singular. □

Now write

$$h(x,y) = y^2 - (x-r_1)(x-r_2)(x-r_3), \quad r_1, r_2, r_3 \in \mathbf{C}.$$

It follows that $h(x, y) = 0$ is nonsingular if and only if r_1, r_2, r_3 are distinct.

PROOF
Suppose r_1, r_2, r_3 are distinct and $h(x, y) = 0$ is singular. Let (x_0, y_0) be a point of singularity. Then $\frac{\partial h}{\partial y}(x_0, y_0) = 2y_0 = 0$. Since $h(x_0, 0) = 0$, it follows that $x_0 \in \{r_1, r_2, r_3\}$. Without loss of generality, assume $x_0 = r_1$. Then

$$\frac{\partial h}{\partial x}(r_1, 0) = -(r_1 - r_2)(r_1 - r_3) = 0.$$

But this cannot be since r_1, r_2, r_3 are distinct.

Now suppose $h(x, y) = 0$ is nonsingular and, without loss of generality, that $r_1 = r_2$. Let $(x_0, y_0) = (r_1, 0)$. Then $h(r_1, 0) = 0$, $\frac{\partial h}{\partial y}(r_1, 0) = 0$, and $\frac{\partial h}{\partial x}(r_1, 0) = -(r_1 - r_2)(r_1 - r_3) = 0$, since $r_1 = r_2$. But this cannot be since $h(x, y) = 0$ is nonsingular. □
Let $d = (r_1 - r_2)^2(r_1 - r_3)^2(r_2 - r_3)^2$. Then $h(x, y) = 0$ is singular if and only if $d = 0$. It can be verified that

$$\det\begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix} = (r_3 - r_2)(r_3 - r_1)(r_2 - r_1),$$

so that

$$d = \det\begin{pmatrix} 1 & 1 & 1 \\ r_1 & r_2 & r_3 \\ r_1^2 & r_2^2 & r_3^2 \end{pmatrix}\begin{pmatrix} 1 & r_1 & r_1^2 \\ 1 & r_2 & r_2^2 \\ 1 & r_3 & r_3^2 \end{pmatrix} = \det\begin{pmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{pmatrix}$$

where $s_i = r_1^i + r_2^i + r_3^i$ for $1 \le i \le 4$. If $a = r_1 + r_2 + r_3$, $b = r_1r_2 + r_1r_3 + r_2r_3$, and $g = r_1r_2r_3$, then it can be verified algebraically that

$$\begin{aligned} s_1 &= a \\ s_2 &= a^2 - 2b \\ s_3 &= a^3 - 3ab + 3g \\ s_4 &= a^4 - 4a^2b + 2b^2 + 4ag. \end{aligned}$$

Now since

$$x^3 - 27c_4x - 54c_6 = (x - r_1)(x - r_2)(x - r_3) = x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_1r_3 + r_2r_3)x - r_1r_2r_3,$$

it follows that $a = 0$, $b = -27c_4$, and $g = 54c_6$. Hence,

$$d = \det\begin{pmatrix} 3 & 0 & 54c_4 \\ 0 & 54c_4 & 162c_6 \\ 54c_4 & 162c_6 & 1458c_4^2 \end{pmatrix} = 78732(c_4^3 - c_6^2).$$

The **dicriminant** Δ of the curve $f(x, y) = 0$ is defined to be

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6$$

where $b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2$. It can be verified that $4b_8 = b_2 b_6 - b_4^2$. Using this equality, it can be verified that

$$1728\Delta = c_4^3 - c_6^2.$$

Hence, $f(x, y) = 0$ is singular iff $h(x, y) = 0$ is singular iff $d = 0$ iff $\Delta = 0$.

V. Types of Singularities

Let $f(x, y)$ be as in section III and $h(x, y)$ be as in section IV. Suppose $h(x, y) = 0$ is singular. Let $P = (x_0, y_0)$ be a point of singularity. From section IV, we may state, without loss of generality, that $P = (r_1, 0)$, where

$$h(x, y) = y^2 - (x - r_1)^2 (x - r_2)$$

If $P' = (x_1, y_1)$ is another, distinct, point of singularity, then, since $\frac{\partial h}{\partial y}(x_1, y_1) = 2y_1 = 0$, $P' = (x_1, 0)$. Since, $h(x_1, 0) = -(x_1 - r_1)^2 (x_1 - r_2) = 0$ and $x_1 \neq r_1$, $P' = (r_2, 0)$. But, then, since

$$\frac{\partial h}{\partial x}(r_2, 0) = -(r_2 - r_1)^2 = 0,$$

we find that $r_2 = r_1$ and $P = P'$. Thus, $h(x, y) = 0$ has at most one point of singularity.

If $f(x, y) = 0$ has two points of singularity, say (x_1, y_1) and (x_2, y_2), then $u'(x_1, y_1) = u'(x_2, y_2)$ and $v'(x_1, y_1) = v'(x_2, y_2)$, where u', v' are as in section IV. But from the vector equations in section IV, this implies that $(x_1, y_1) = (x_2, y_2)$ and $f(x, y) = 0$ has at most one point of singularity.

Now let $f(x, y) = 0$ be singular and (x_0, y_0) its point of singularity. Let $g(x, y) = f(x + x_0, y + y_0)$. Then

$$g(x, y) = y^2 + a_1' xy + a_3' y - x^3 - a_2' x^2 - a_4' x - a_6'$$

Since (0, 0) is the point of singularity for $g(x, y)=0$, we have $g(0, 0) = -a_6' = 0$, $\frac{\partial g}{\partial y}(0,0) = a_3' = 0$, and $\frac{\partial g}{\partial x}(0,0) = -a_4' = 0$. Hence,

$$g(x,y) = y^2 + a_1'xy - x^3 - a_2'x^2 = (y - ax)(y - bx) - x^3, \quad a, b \in \mathbf{C}.$$

If $a = b$, then the singular point (x_0, y_0) is a **cusp**, otherwise it is a **node**. In the case of a node, if $a, b \in \mathbf{Q}$, then the node is a **split case**, otherwise it is a **nonsplit case**.

VI. The Group Operation on Elliptic Curves

Let $E(\mathbf{Q})$ be an elliptic curve given by an equation $f(x, y) = 0$ as in section III and denote the point at infinity on the elliptic curve by O. The following method will be used to add points in $E(\mathbf{Q})$:

(i) $P + O = O + P = P$, for all $P \in E(\mathbf{Q})$

(ii) if $P_1, P_2 \in E(\mathbf{Q}) - \{O\}$, then let $l = \overline{P_1P_2}$ if $P_1 \neq P_2$ and let l be the line tangent to the curve at P_1 if $P_1 = P_2$. If l is vertical, then $P_1 + P_2 = O$. Otherwise, $P_1 + P_2 = (x, -y)$ where (x, y) is the point of intersection of l and $E(\mathbf{Q})$ distinct from P_1 and P_2.

Under this operation, it can shown that $E(\mathbf{Q})$ forms an abelian group. The point O is the identity element and if $P = (x, y)$, then $-P = (x, -y)$. Given a prime p, let $E[p]=\{P \in E(\mathbf{Q}): pP = O\}$.It can be shown that $|E[p]| = p^2$ and that $E[p]$ is a subgroup of $E(\mathbf{Q})$ isomorphic to $\mathbf{Z} / p\mathbf{Z} \times \mathbf{Z} / p\mathbf{Z}$.

VII. Reduction Modulo *p*

Let p be a prime and $f(x, y)$ be as in section III. Since each $a_i \in \mathbf{Z}$, we can reduce the coefficients modulo p and consider $f(x, y)$ as a polynomial in $\mathbf{F}_p = \mathbf{Z} / p\mathbf{Z}$. The curve $f(x, y) = 0$ is nonsingular if there are no simultaneous solutions in $\overline{\mathbf{F}_p}^2$ to the equations

$$f(x,y) = 0 \qquad \frac{\partial f}{\partial x}(x,y) = 0 \qquad \frac{\partial f}{\partial y}(x,y) = 0.$$

Any such solution is called a point of singularity and it can be shown that there exists at most one such point. When

$$g(x,y) = (y - ax)(y - bx) - x^3, \quad a, b \in \overline{\mathbf{F}_p}$$

is constructed as in section V, the point of singularity is a cusp if $a = b$ and is a node if $a \neq b$. If it is a node and $a, b \in \mathbf{F}_p$, the node is a split case, otherwise it is a nonsplit case.

The curve

$$E(\mathbf{F}_p) = \left\{ a \in \mathbf{P}^2_{\mathbf{F}_p} : \forall (x,y,z) \in a, \tilde{f}(x,y,z) = 0 \right\}$$

is an elliptic curve if the curve $f(x, y) = 0$ is nonsingular. It can be shown by methods similar to those used in section IV (care must be taken for the case $p \in \{2,3\}$) that $E(\mathbf{F}_p)$ is an elliptic curve if and only if $p \nmid \Delta$.

If $E(\mathbf{F}_p)$ is an elliptic curve, then $E(\mathbf{Q})$ is said to have **good reduction** at p. If $E(\mathbf{F}_p)$ is not an elliptic curve, then the curve $f(x, y) = 0$ in $\mathbf{F}_p^2$ has a point of singularity. If this point is a node, E is said to have **multiplicative reduction** at p. If it is a cusp, E has **additive reduction** at p.

VIII. Minimal Equations

Let $r \in \mathbf{Q}$. If $r \neq 0$, write $r = p^n u / v$, where GCD (p, u) = GCD $(p, v) = 1$. Then the p-**adic norm** of r is defined to be $|r|_p = p^{-n}$. We define $|0|_p = 0$. A number $r \in \mathbf{Q}$ is p-**integral** if $|r|_p \leq 1$.

Let $E(\mathbf{Q})$ be an elliptic curve given by an equation $f(x, y) = 0$ in the form shown in section III. An **admissible change of variables** is one of the form

$$x = u^2 x' + r \qquad y = u^3 y' + s u^2 x' + t$$

where $u, r, s, t \in \mathbf{Q}$ and $u \neq 0$. The equation, $f(x, y) = 0$, is said to be **minimal** for the prime p if the power of p dividing Δ cannot be decreased by making an admissible change of variables with the property that the new coefficients are p-integral. The equation, $f(x, y) = 0$ is said to be a **global minimal Weierstrass equation** if it is minimal for all primes and its coefficients are integers. Two elliptic curves related by an admissible change of variables are said to be **isomorphic**.

It can be shown that for any elliptic curve, $E(\mathbf{Q})$, given be an equation $f(x, y) = 0$ of the form in section III, there exists an admissible change of variables such that the resulting equation is a global minimal Weierstrass equation.

IX. The Conductor

Let $E(\mathbf{Q})$ be an elliptic curve given by a global minimal Weierstrass equation $f(x, y) = 0$. The **conductor** of E is defined to be

$$N = \prod_{p \text{ prime}} p^{n(p)}$$

where

$$n(p) = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p \\ 1 & \text{if } E \text{ has multiplicative reduction at } p \\ \geq 2 & \text{if } E \text{ has additive reduction at } p. \end{cases}$$

There are algorithms for determining the exact value of $n(p)$ in the additive case. It should be noted that in this case, if $p > 3$, $n(p) = 2$.

X. Semistable Elliptic Curves

Let E (**Q**) be an elliptic curve given by an equation $f(x, y) = 0$ of the form in section III. Let E' (**Q**) be an isomorphic elliptic curve given by a global minimal Weierstrass equation with conductor N. If for all primes p such that $p \mid N$, $p^2 \nmid N$, i.e. N is **squarefree**, then E (**Q**) is said to be **semistable**.

XI. The *L*-function

Let E (**Q**) be an elliptic curve given by a global minimal Weierstrass equation, $f(x, y) = 0$. Let p be a prime. If $p \nmid \Delta$, define $a_p = p + 1 - |E(\mathbf{F}_p)|$. If $p \mid \Delta$, let $P \in \overline{\mathbf{F}_p}^2$ be the point of singularity on the curve $f(x, y) = 0$ and define

$$a_p = \begin{cases} 0 & \text{if } P \text{ is a cusp} \\ 1 & \text{if } P \text{ is a split case of a node} \\ -1 & \text{if } P \text{ is a nonsplit case of a node} \end{cases}$$

Let

$$e_p = \begin{cases} 0 & \text{if } p \mid \Delta \\ p & \text{if } p \nmid \Delta \end{cases}$$

The ***L*-function of *E*** is defined to be

$$L(E,s) = \prod_{p \text{ prime}} \left[\frac{1}{1 - a_p p^{-s} + e_p p^{-2s}} \right].$$

We can then write

$$L(E,s) = \prod_{p \text{ prime}} \left[\sum_{n=0}^{\infty} \left(a_p p^{-s} - e_p p^{-2s} \right)^n \right] = \prod_{p \text{ prime}} \left[\sum_{n=0}^{\infty} \sum_{m=0}^{n} \binom{n}{m} a_p^{n-m} e_p^m p^{-(m+n)s} \right].$$

Now $\forall n \in \mathbf{N}$, define

$$A_n = \left\{ (i, j) \in \mathbf{Z}^2 : i \geq j \geq 0, i + j = n \right\}$$

and

$$a_{p^n} = \sum_{(i,j) \in A_n} \binom{i}{j} a_p^{i-j} e_p^j .$$

Then

$$L(E,s) = \prod_{p \text{ prime}} \left[1 + \sum_{n=1}^{\infty} a_{p^n} p^{-ns} \right].$$

Now define $a_1 = 1$ and $\forall n \in \mathbf{N}$, with $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ being the unique factorization of n, define $a_n = a_{p_1^{m_1}} a_{p_2^{m_2}} \cdots a_{p_k^{m_k}}$. It then follows that

$$\begin{aligned} L(E,s) &= \left(1 + \frac{a_2}{2^s} + \frac{a_{2^2}}{(2^2)^s} + \frac{a_{2^3}}{(2^3)^s} + \cdots \right) \\ &\quad \times \left(1 + \frac{a_3}{3^s} + \frac{a_{3^2}}{(3^2)^s} + \frac{a_{3^3}}{(3^3)^s} + \cdots \right) \\ &\quad \times \left(1 + \frac{a_5}{5^s} + \frac{a_{5^2}}{(5^2)^s} + \frac{a_{5^3}}{(5^3)^s} + \cdots \right) \\ &\quad \times \cdots \\ &= 1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_{2^2}}{(2^2)^s} + \frac{a_5}{5^s} + \frac{a_2}{2^s}\left(\frac{a_3}{3^s} \right) + \cdots \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \end{aligned}$$

XII. Modular Forms

Let $H = \{ z \in \mathbf{C} : \operatorname{Im} z > 0 \}$ denote the complex upper half plane and

$$\Gamma = SL_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,b,c,d \in \mathbf{Z} \text{ and } ad - bc = 1 \right\}$$

denote the special linear group. If $g \in \Gamma$ and $z \in H$, define $g\,z = \dfrac{az+b}{cz+d}$. It can be verified that if $z \in H$, then $g\,z \in H$ and $g_1(g_2\,z) = (g_1 g_2)\,z$. Now for each $N \in \mathbf{N}$, define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c \equiv 0 \pmod{N} \right\}.$$

Let $k \in \mathbf{Z}$, let $N \in \mathbf{N}$, and let $f: H \to \mathbf{C}$ be a holomorphic function that satisfies the condition

$$f(g\,z) = (cz+d)^k f(z), \qquad \forall z \in H, g \in \Gamma_0(N).$$

Since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, it follows that $f(z+1) = f(z)$ and f has a Fourier expansion

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n, \qquad \text{where } q = e^{2piz}$$

If $a_n = 0$ for all $n < 0$, then f is called a **modular form of weight k on $\Gamma_0(N)$.** The number, N, is called the **level** of f. If, in addition, $a_0 = 0$, f is called a **cusp form**.

XIII. Old and New Forms

The set of modular forms of weight k and level N is denoted $M_k(N)$. Now let $f, g \in M_k(N)$ and $h(z) = f(z) + g(z)$. It follows that for all $g \in \Gamma_0(N)$

$$h(g\,z) = f(g\,z) + g(g\,z) = (cz+d)^k (f(z) + g(z)) = (cz+d)^k h(z)$$

and $h \in M_k(N)$. Also, if $f \in M_k(N)$, $w \in \mathbf{C}$, and $h(z) = wf(z)$, then for all $g \in \Gamma_0(N)$

$$h(g\,z) = wf(g\,z) = (cz+d)^k wf(z) = (cz+d)^k h(z)$$

and again $h \in M_k(N)$. Hence, the set $M_k(N)$ is a complex vector space.

Let N be fixed and $d \in \mathbf{Z}$ be given such that $1 < d < N$ and $d \mid N$. Define the set

$$O_d = M_k(d) \cup \{g(z) : g(z) = f(d'z) \text{ for some } f \in M_k(d)\}, \text{ where } dd' = N.$$

It follows that $O_d \subset M_k(N)$.

PROOF
Let $g \in O_d$. Assume $g \in M_k(d)$. Since $\Gamma_0(N) \subset \Gamma_0(d)$, it follows easily that $g \in M_k(N)$. Now assume $g \notin M_k(d)$. Let $f \in M_k(d)$ be given such that $g(z) = f(d'z)$. Let $g \in \Gamma_0(N) \subset \Gamma_0(d)$ be given. Then

$$g(g\,z) = g\left(\frac{az+b}{cz+d}\right) = f\left(\frac{ad'z+bd'}{cz+d}\right) = f\left(\frac{a(d'z)+bd'}{dd''(d'z)+d}\right), \text{ where } c = Nd''.$$

Since $ad - bd'dd'' = ad - bc = 1$, it follows that $\begin{pmatrix} a & bd' \\ dd'' & d \end{pmatrix} \in \Gamma_0(d)$. Thus,

$$g(g\,z) = (dd''(d'z)+d)^k f(d'z) = (cz+d)^k g(z)$$

and $g \in M_k(N)$.□

Now let $O = \bigcup_{1<d<N,\, d|N} O_d$. The subspace of $M_k(N)$ spanned by the vectors in O is called the space of **old forms**.

Let $G \subset \Gamma$ be a subgroup. Two points, $z_1, z_2 \in H$ are ***G*-equivalent** if $\exists g \in G$ such that $z_2 = g\, z_1$. A closed region $F \subset H$ is a **fundamental domain** for G if every $z \in H$ is G-equivalent to a point in F, but no two distinct points z_1, z_2 in the interior of F are G-equivalent.

The **Petersson inner product** on the space, $M_k(N)$, is defined as

$$\langle f, g \rangle = \int_F f(z)\overline{g(z)}y^{k-2}dxdy$$

where $z = x + iy$ and F is a fundamental domain for $\Gamma_0(N)$.

A modular form, $f \in M_k(N)$, is said to be a **new form** if there exists an old form, $g \in M_k(N)$, such that $\langle f, g \rangle = 0$.

XIV. Finite Dimensionality

Define $S_k(N) = \{f \in M_k(N)$: f is a cusp form$\}$. It can be easily verified that $S_k(N)$ is a subspace. In fact, $M_k(N)$ (and, thus, $S_k(N)$) is finite dimensional. For our purposes, we will be interested in the dimension of $S_k(N)$ when $k = 2$. There is a complex formula for computing dim $S_2(N)$, which, in the case when N is prime, reduces to

$$\dim S_2(N) = \frac{N+1}{12} - \frac{m_2}{4} - \frac{m_3}{3},$$

where

$$m_2 = \begin{cases} 2 & \text{if } N \equiv 1 (\text{mod } 4) \\ 0 & \text{if } N \equiv 3 (\text{mod } 4) \\ 1 & \text{if } N = 2 \end{cases}$$

and

$$m_3 = \begin{cases} 2 & \text{if } N \equiv 1 (\text{mod } 3) \\ 0 & \text{if } N \equiv 2 (\text{mod } 3) \\ 1 & \text{if } N = 3 \end{cases}$$

An application of this formula for the case $N = 2$ shows that dim $S_2(2) = 0$, i.e. $S_2(2) = \varnothing$.

XV. Hecke Operators

Let N and k be fixed and consider the space $M_k(N)$. The **hecke operators** are functions T_m: $M_k(N) \to M_k(N)$, $m \in \mathbf{N}$ where if $f(z) = \sum_{n=0}^{\infty} a_n q^n$, with $q = e^{2piz}$, then

$$T_m(f)(z) = \sum_{n=0}^{\infty} b_n q^n$$

where

$$b_n = \begin{cases} a_0 \sum_{d>0, d|m} d^{k-1} & \text{if } n = 0 \\ a_m & \text{if } n = 1 \\ \sum_{d|\mathrm{GCD}(n,m)} d^{k-1} a_{nm/d^2} & \text{if } n > 1 \end{cases}$$

Let $f(z) = \sum_{n=0}^{\infty} a_n q^n$ be given. If there exists a sequence of complex numbers, $\{l_m\}_{m=1}^{\infty}$, such that $T_m(f) = l_m f$, then f is an **eigenform**.

XVI. Modular Forms vs. Elliptic Curves

Let $f \in S_2(N)$ be a new eigenform. Write

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \text{ with } q = e^{2piz}.$$

By multiplying f by an appropriate constant, if necessary, we can make $a_1 = 1$. This is called **normalizing** the form f. If, after the normalization, each $a_i \in \mathbf{Z}$, then there exists an elliptic curve, E ($\mathbf{Q}$) given by an equation with integer coefficients, whose conductor is N and whose L-function has coefficients, a_i, that are precisely those in the Fourier expansion of f. An elliptic curve formed in this fashion is called **modular**.

XVII. Shimura-Taniyama-Weil

The Shimura-Taniyama-Weil conjecture is this: Let E ($\mathbf{Q}$) be an elliptic curve whose equation has integer coefficients. Let N be the conductor of E, and for each n let a_n be the number appearing in the L-function of E. Then there exists a cusp form of weight 2, level N, which is a new eigenform, and (when normalized) has Fourier expansion equal to $\sum_{n=1}^{\infty} a_n q^n$, with $q = e^{2piz}$.

Andrew Wiles proved that this conjecture is true under the added assumption that the elliptic curve in question is semistable.

XVIII. The Frey Curve

Suppose $\exists\ u, v, w \in \mathbf{Z}^*$ and prime $q \geq 5$ such that $u^q + v^q + w^q = 0$. Suppose further that u, v, w are relatively prime, $u \equiv -1 \pmod 4$ and v is even. Let

$$f(x, y) = y^2 - x(x - u^q)(x + v^q)$$

The elliptic curve given by $f(x, y) = 0$ is called the **Frey curve**. By making the admissible change of variables $x = 4x'$, $y = 8y' + 4x'$, $f(x, y) = 0$ becomes $g(x, y) = 0$, where

$$g(x, y) = y^2 + xy - x^3 - \frac{v^q - u^q - 1}{4} x^2 + \frac{(uv)^q}{16} x\,.$$

The congruences show that the coefficients are integers and, in fact, the equation $g(x, y) = 0$ is a global minimal Weierstrass equation. To compute the dicriminant Δ of $g(x, y) = 0$, we note that

$$a_1 = 1 \qquad b_2 = v^q - u^q$$

$$a_3 = 0 \qquad b_4 = -\frac{(uv)^q}{8}$$

$$a_2 = \frac{v^q - u^q - 1}{4} \qquad b_6 = 0$$

$$a_4 = -\frac{(uv)^q}{16} \qquad b_8 = -\frac{(uv)^{2q}}{256}$$

$$a_6 = 0$$

Thus,

$$\Delta = \frac{(uv)^{2q}(v^q - u^q)^2}{256} + \frac{(uv)^{3q}}{64} = \frac{(uv)^{2q}}{256}((v^q - u^q)^2 + 4(uv)^q)$$
$$= \frac{(uv)^{2q}}{256}(v^q + u^q)^2 = \frac{(uvw)^{2q}}{256}.$$

It can be shown that the Frey curve is semistable so that its conductor is

$$N = \prod_{p|uvw} p\,.$$

XIX. Ribet's Theorem

Let $f \in S_2(N)$ be a normalized, new eigenform and write

$$f(z) = \sum_{n=1}^{\infty} a_n q^n, \text{ where } q = e^{2piz}\,.$$

Let E (**Q**) be an elliptic curve with dicriminant Δ, conductor N, and L-function

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Write $\Delta = p_1^{a_{p1}} p_2^{a_{p2}} \cdots p_r^{a_{pr}}$, $N = \prod_{p|\Delta} p^{b_p}$ and fix a prime, l. As remarked in section IV, E [l] is a 2-dimensional vector space. If there is no 1-dimensional subspace of E [l] which is left fixed by the action of the Galois group G = Gal (**Q**(E [l])/**Q**), where **Q**(E [l]) is the smallest field containing the rationals and the coordinates of the points in E [l], then E[l] is said to be irreducible. If E [l] is irreducible, then Ribet's theorem states that there exists $f_1 \in S_2(N_1)$, where

$$N_1 = \frac{N}{\prod_{\substack{p|\Delta, b_p=1, \\ l|a_p}} p}.$$

XX. Fermat's Last Theorem

There are no non-zero integers x, y, z such that $x^n + y^n = z^n$ when $n \geq 3$.

PROOF
Proofs of the specific cases $n = 3$ and $n = 4$ are available elsewhere. Assume there are non-zero integers x, y, z and an integer $n \geq 3$ such that $x^n + y^n = z^n$. Since the theorem is true for the cases $n = 3$ and $n = 4$, there must be a prime $q \geq 5$ such that $q \mid n$. Let $n = qd$, so that $u^q + v^q + w^q = 0$, where $u = x^d$, $v = y^d$, $w = -z^d$. After dividing through by common factors, if necessary, we can assume u, v, w are relatively prime. Hence, exactly one of them is even. Of the other two, one must be congruent to –1 modulo 4. After renaming the variables, if necessary, we may assume $u \equiv -1 \pmod 4$ and v is even. From section XVIII, the Frey curve,

$$y^2 + xy = x^3 + \frac{v^q - u^q - 1}{4} x^2 - \frac{(uv)^q}{16} x$$

is semistable. So by section XVII, there exists a new eigenform $f \in S_2(N)$, where $N = \prod_{p|uvw} p$. It can be shown that on this curve, E [q] is irreducible. Now

$$\Delta = \frac{(uvw)^{2q}}{256} = \prod_{p|uvw} p^{b_p}, \text{ where } b_p = \begin{cases} 2q-8 & \text{if } p = 2 \\ 2q & \text{if } p \neq 2 \end{cases}.$$

Hence, by section XIX, there exists $f_1 \in S_2(N_1)$, where

$$N_1 = \frac{N}{\prod_{p|\Delta, q|b_p} p} = 2.$$

But in section XIV, it was noted that $S_2(2) = \varnothing$.□

The proof given here for Fermat's Last Theorem is hardly a proof at all. Many of the facts given in this paper were stated without proof and, more importantly, no mention has been made of the method Wiles employed to show that all semistable elliptic curves are modular. This, of course, was his major contribution and what you see here is a very brief sketch of some of the mathematics involved in determining that this fact implies Fermat's Last Theorem. This paper is meant as a guide, both for myself and the interested reader. The next step in my investigation of this topic will be to study the points of finite order on elliptic curves and their respective Galois representations.

It is undoubtedly an ominous task to try to learn all that is necessary to verify the work of the many mathematicians that have contributed to this proof, but the alternative is to simply accept that it is valid on the authority of the experts. In any intellectual discipline, especially in mathematics and the sciences, this is a dangerous habit indeed and I would encourage anyone with the drive and interest to pursue this knowledge for themselves.

BIBLIOGRAPHY

Anthony W. Knapp, *Elliptic Curves*, Princeton University Press, 1992
John B. Fraleigh, *A First Course in Abstract Algebra*, Addison-Wesley Publishing Company, 1967
Neal Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1993