How Not To Prove Fermat's Last Theorem

William M. Faucette

December 2001

The tremendous endurance of Fermat's Last Theorem in the mind of the public is at least in part due to the fact that the theorem is so easily stated:

Theorem 1 (Fermat's Last Theorem). *For any natural number $n \geq 3$, the equation*

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

has only trivial integral solutions. That is, if (x, y, z) is an integral solution, then one of the coordinates is zero.

The long search for a proof of Fermat's Last Theorem is now over with its proof by Professor Andrew Wiles of Princeton University. With the resolution of what has been one of the most famous mathematical problems for the last three centuries, this is the ideal time to revisit a rather naïve attack on this famous problem using the elementary theory of algebraic plane curves and examine the reasons why such an approach fails to work.

Background Notions.

Let $\mathbb{C}$ denote the field of complex numbers and define the affine complex plane, $\mathbb{A}^2$, to the the set of all ordered pairs (a, b) where a, $b \in \mathbb{C}$. A complex affine plane curve is the locus of zeroes in $\mathbb{A}^2$ of a nonzero polynomial $f \in \mathbb{C}[X, Y]$. The complex projective plane, $\mathbb{P}^2$, is the set of all equivalence classes $[a, b, c]$ of ordered triples $(a, b, c) \in \mathbb{C}^3 \setminus \{(0, 0, 0)\}$ under the equivalence relation $(a, b, c) \sim (a', b', c')$ if $(a, b, c) = (\lambda a', \lambda b', \lambda c')$ for some nonzero complex number λ. Notice that if $c \neq 0$, we may divide the three coordinates by c and obtain coordinates $[a, b, 1]$. A complex projective plane curve is the locus of zeroes in $\mathbb{P}^2$ of a nonzero homogeneous polynomial $F \in \mathbb{C}[X, Y, Z]$. The degree of a plane curve is the degree of its defining polynomial. Curves of degrees one, two, three, and four are called lines, conics, cubics, and quartics, respectively.

The affine plane is contained in the projective plane by the inclusion $\mathbb{A}^2 \hookrightarrow \mathbb{P}^2$ given by $(x, y) \mapsto [x, y, 1]$, with the remainder of the projective plane forming the line at infinity,

$$L_\infty = \{[x, y, 0] \in \mathbb{P}^2\}.$$

If $f(X,Y)$ is an element of $\mathbb{C}[X,Y]$ of degree d, we con homogenize f by setting $F(X,Y,Z) = Z^d f(X/Z, Y/Z)$. F is then a homogeneous polynomial of degree d. If f defines an affine plane curve C, the projective plane curve defined by F is the *projective closure* of C.

For an introduction to the basic notions of algebraic geometry, see [1], [2] or [3].

Motivation: The case $n = 2$.

Consider the Pythagorean equation

$$x^2 + y^2 = z^2, \tag{1}$$

where x, y, and z are integers. Note that this is a homogeneous polynomial in x, y, and z, so it defines a projective algebraic curve C in $\mathbb{P}^2$. Finding all the Pythagorean triples, that is, all integral solutions to equation (1), is equivalent to finding all points on C with integral coordinates. Since the coordinates of points in $\mathbb{P}^2$ are defined only up to a nonzero complex multiple, we may actually seek to determine the *rational points* on C, that is, those points with rational coordinates, since clearing denominators will then produce an integral solution to equation (1).

We seek nontrivial solutions, so we may assume that none of these integers is zero. Thus we may dehomogenize this equation by setting $X = x/z$ and $Y = y/z$, and in this way we can concentrate out attention on the affine piece given by $z \neq 0$. Thus, this equation becomes

$$X^2 + Y^2 = 1. \tag{2}$$

If we now view this equation as representing a complex affine algebraic curve, C, the question we ask can be rephrased as follows: Is there any way to determine the rational points on C? Equivalently, can we find a parameterization of C by rational functions with rational coefficients? If so, then for each rational value of the parameter (except possibly finitely many where the parameterization is undefined), we get an ordered pair of rational numbers, (X,Y), satisfying equation (1). Clearing denominators, we get a triple of integers (x,y,z) satisfying $x^2 + y^2 = z^2$.

To accomplish such a parameterization, we note that each line ℓ through the point $(-1,0)$ passes through the curve once more. If we let our parameter be the slope t of the line $\ell(t)$ through the points $(-1,0)$, then for most values of t, we can associate to t the point other than $(-1,0)$ of intersection for the line $\ell(t)$ with the curve.

The Computation.

Referring to Figure 1, setting t equal to the slope of the line through the point $(-1,0)$ and (x,y), we see that the equation of this line, $\ell(t)$, is

$$y = xt + t,$$

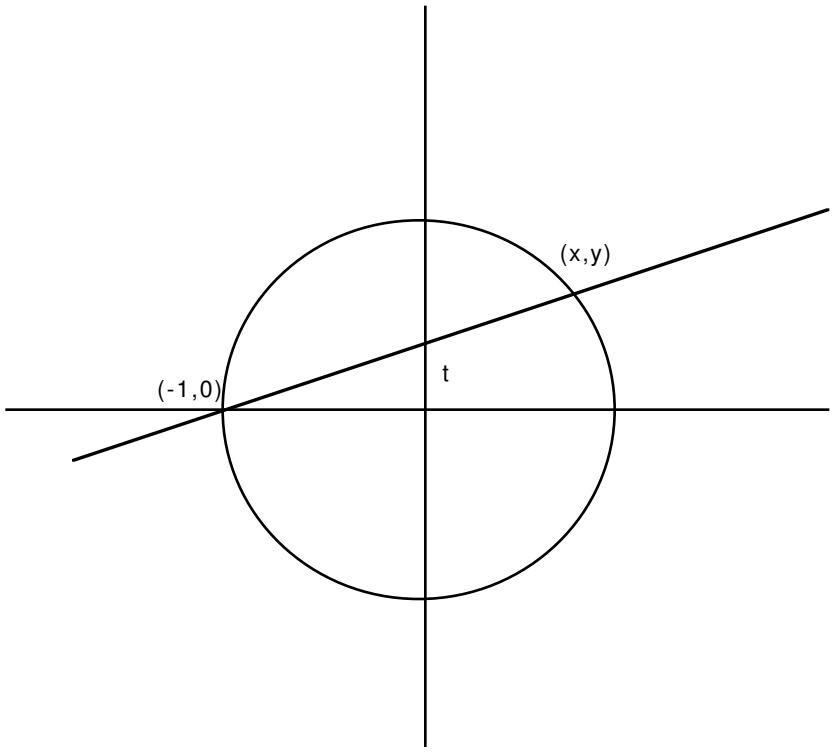

Figure 1: $X^2 + Y^2 = 1$

and substituting this value into the equation (2) yields the coordinates of the two points of intersection of $\ell(t)$ with the curve C:

$$\begin{aligned} x^2 + y^2 &= 1 \\ x^2 + (xt + t)^2 &= 1 \\ x^2 + x^2t^2 + 2xt^2 + t^2 &= 1 \\ x^2(1 + t^2) + 2xt^2 + (t^2 - 1) &= 0. \end{aligned}$$

Using the quadratic formula to solve this equation for x, we get

$$x = -1 \quad \text{or} \quad x = \frac{1 - t^2}{1 + t^2}.$$

Disregarding the root $x = -1$, which corresponds to the point $(-1, 0)$, the remaining point of intersection is

$$\left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

Now define a mapping $\phi : \mathbb{Q} \to C$ by

$$\phi(t) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2} \right).$$

We then get a map of the rational numbers into C. Clearing denominators, we get triples of points

$$\left(1 - t^2, 2t, 1 + t^2\right).$$

Of course, the affine equation $X^2 + Y^2 = Z^2$ is symmetric with respect to the coordinate planes, so we may rewrite our parameterization as

$$t \mapsto \left(t^2 - 1, 2t, 1 + t^2\right).$$

Note that if we take t to be an integer, we get integer solutions to equation (1), the so-called Pythagorean triples. In particular, for $t = 2$ we get the familiar triple $(3, 4, 5)$.

Completeness of this Solution.

Do we get all possible integral triples in this way? Equivalently, do we get all rational points on the curve C? To answer this question, define $\psi : C \setminus \{(-1, 0)\} \to \mathbb{C}$ by

$$\psi(x, y) = \frac{y}{x + 1}\ .$$

Notice that $\phi \circ \psi$ is the identity on $C \setminus \{(-1, 0)\}$ and $\psi \circ \phi$ is the identity on $\mathbb{C}$. Suppose that (x, y, z) is a Pythagorean triple with $z \neq 0$. Dividing by z, we get an ordered pair (x', y') satisfying equation (1). Assuming $x' \neq 1$, let $t = \psi(x', y')$, so that $\phi(t) = (x', y')$. This computation shows that with the

exception of the point $(-1, 0) \in C$ through which all the lines $\ell(t)$ pass, the mapping ϕ is bijective.

So Why Won't This Approach Prove Fermat's Last Theorem?

The problem arises with the existence of the parameterization ϕ. If C is a complex projective curve, we say that C is *rational* if there exists a nonconstant rational map $\phi : \mathbb{P}^1 \to C$. So, in order to find a parameterization ϕ, the question we must ask is this: Is the curve $x^n + y^n = z^n$ rational? The answer to this question in general is completely given by a discrete invariant called the *geometric genus* of C. A projective algebraic curve C is rational if and only if it has genus zero. For a smooth plane curve of degree n, the genus is $\frac{1}{2}(n-1)(n-2)$. We see that the only rational smooth plane curves are those of degrees one or two. In other words, the algebraic curves $x^n + y^n = z^n$ for $n \geq 3$ are not rational, and therefore admit no parameterization ϕ as constructed above. We give a more concrete argument in the next section.

The General Case.

In this section we show directly that the projective algebraic curve with equations $x^n + y^n = z^n$ is not rational for $n \geq 3$, following an argument taken from [3, pp. 7–8].

Suppose there exists a rational map $\phi(t) = (p(t), q(t), r(t))$ parameterizing the curve $x^n + y^n = z^n$. Then we have the relation

$$p(t)^n + q(t)^n - r(t)^n = 0.$$

Differentiating, we have

$$p(t)^{n-1}p'(t) + q(t)^{n-1}q'(t) - r^{n-1}(t)r'(t) = 0.$$

Using matrix notation, this says that the 3-tuple $\left(p(t)^{n-1}, q(t)^{n-1}, r(t)^{n-1}\right)$ is a solution of the equation

$$\begin{bmatrix} p(t) & q(t) & -r(t) \\ p'(t) & q'(t) & -r'(t) \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = 0.$$

We now assume that $p(t)$, $q(t)$, and $r(t)$ are relatively prime of degrees a, b, and c, respectively, with $a \geq b \geq c$. By standard techniques for solving matrix equations, the solution $\left(p(t)^{n-1}, q(t)^{n-1}, r(t)^{n-1}\right)$ must be proportional to the minors of the "coefficient" matrix:

$$\left(r(t)q'(t) - q(t)r'(t), p(t)r'(t) - r(t)p'(t), p(t)q'(t) - q(t)p'(t)\right).$$

Since $p(t)$, $q(t)$, and $r(t)$ are relatively prime, we must have that $p(t)^{n-1}$ divides $r(t)q'(t) - q(t)r'(t)$. This then yields that $(n-1)a \leq b + c - 1 \leq 2a - 1$, which is not possible for $n \geq 3$.

Conclusion

In this paper we have examined an approach to the proof of Fermat's Last Theorem based on the idea of parameterizing the related algebraic plane curve with homogeneous equations $X^n + Y^n = Z^n$ by rational functions, noting that such a parameterization provides infinitely many nontrivial integral solutions to this equation. The obstruction to this approach to a solution is an integral invariant called the genus of the algebraic curve. An algebraic curve admits such a parameterization if and only if it has genus zero. For our particular curve, the genus is given by $\frac{1}{2}(n-1)(n-2)$, so for $n \geq 3$, the algebraic curve with equation $X^n + Y^n = Z^n$ cannot be parameterized in such a way. However, for $n = 2$ this technique does give a constructive method for finding all but finitely many of the Pythagorean triples.

References

[1] W. Fulton. *Algebraic Curves.* Benjamin/Cummings Publishing Company, Reading, Massachusetts, 1974.

[2] J. Harris. *Algebraic Geometry: A First Course.* Springer-Verlag, New York, 1993.

[3] I. R. Shafarevich. *Basic Algebraic Geometry.* Springer-Verlag, New York, 1977.