

Fermat's Last Theorem over Polynomial Rings

Andrew Snowden

Friday, October 3rd, 2003

Let k be a field of characteristic p containing the algebraic closure of its prime subfield. Let $R = k[T_1, \dots, T_N]$ be the polynomial ring over k in N indeterminates. Consider the Fermat equation

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

over R . In this paper we investigate solutions to (1) and prove:

Theorem 1 *For $n > 2$ there are no nontrivial primitive solutions to (1).*

We now define the terms primitive and nontrivial appearing in the statement of the theorem.

A solution (x, y, z) to (1) is trivial if $x, y, z \in k$ or if one of x, y, z is zero.

A solution (x, y, z) is primitive if x, y, z are pairwise coprime. Furthermore, if the characteristic p is not zero we require that n and p be coprime (for if x, y, z satisfy $x^{np} + y^{np} = z^{np}$ then they also satisfy $x^n + y^n = z^n$).

Note that we always obtain infinitely many solutions to (1) if $n = 1, 2$. In the case $n = 1$ this is obvious. For $n = 2$, if we select any $s, t \in R$ we obtain a solution via

$$\begin{aligned} x &= s^2 - t^2 \\ y &= 2st \\ z &= s^2 + t^2. \end{aligned} \tag{2}$$

We now prove the theorem. Let $n > 2$ be coprime to p . Note that the ring R is a unique factorization domain, a fact essential to our proof. Now, assume we have a nontrivial primitive solution (x, y, z) . We then have

$$z^n = x^n + y^n = \prod_{i=0}^{n-1} x + \zeta^i y \tag{3}$$

where $\zeta \in k$ is a primitive n th root of unity. Since x and y are coprime it follows that the $x + \zeta^i y$ are coprime. By unique factorization we therefore have

$$x + \zeta^i y = q_i^n \quad (4)$$

$$z = \prod_{i=0}^{n-1} q_i \quad (5)$$

for some $q_i \in R$. Note that the q_i are pairwise coprime, none are zero, and at most one is constant.

Consider now the three equations

$$\begin{aligned} x + y &= q_0^n \\ x + \zeta y &= q_1^n \\ x + \zeta^2 y &= q_2^n. \end{aligned} \quad (6)$$

We have

$$\begin{aligned} q_0^n &= x + y \\ &= (1 + \zeta^{-1})(x + \zeta y) + (-\zeta^{-1})(x + \zeta^2 y) \\ &= (1 + \zeta^{-1})q_1^n + (-\zeta^{-1})q_2^n. \end{aligned} \quad (7)$$

Thus if we let

$$\begin{aligned} x' &= (1 + \zeta^{-1})^{1/n} q_1 \\ y' &= (-\zeta^{-1})^{1/n} q_2 \\ z' &= q_0 \end{aligned} \quad (8)$$

Then (x', y', z') is a nontrivial primitive solution to (1). Furthermore, the degrees of x', y' and z' are strictly less than the degrees of x, y, z . Continuing in this way, we obtain smaller and smaller solutions until we find a contradiction.