Parabola Volume 35, Issue 1 (1999)

FERMAT'S LAST THEOREM FOR POLYNOMIALS

by Enrico Laeng[1]

If x, y, and z are three positive integers such that

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

and the exponent n is also a positive integer, then $n \leq 2$. In other words, if $n \geq 3$, the equation $x^n + y^n = z^n$ does not have positive integer solutions. This is the statement of "Fermat's last theorem", which, despite the name, was only a conjecture until recently, when Andrew Wiles provided a proof, making it a real theorem.

Wiles' proof was announced to specialists in algebraic geometry during the summer of 1993, but it had a few gaps. It was completed in September 1994, and now appears in [5][2]. What we want to present in this article is another not so well-known theorem, apparently due to Liouville in 1879 (see [4, pp. 263–265]). We give a proof due to R.C. Mason, from the beginning of the 1980's. (see [2]; S. Lang wrote an article [1] illustrating other applications of Mason's ideas). This theorem and Mason's approach to it is strictly related to the so-called "abc conjecture" and loosely related to the circle of ideas that led to Wiles' success in proving Fermat's last theorem. It can be presented in a very elementary way, and it is interesting in itself. The only prerequisites needed to follow the proof are some high school algebra and the ability to take derivatives of products and quotients of polynomials.

Let $x(t)$, $y(t)$, and $z(t)$ be three polynomials with real coefficients (t is the independent variable, which sometimes we will not write explicitly). The polynomials $x(t)$, $y(t)$ and $z(t)$ are said to be *relatively prime* if they do not have any common factors, and said to be *nontrivial* if their degree is at least one (polynomials of degree zero are simply real constants). We have the following result.

---

[1]Professor Laeng teaches mathematics at the Milan Polytechnic, in Italy.
This is an edited and slightly revised translation of his article which first appeared in *Lettera matematica* **25**, published by Springer-Verlag Italia S.R.L. in September 1997.

[2]This proof is very long and complicated, and even university mathematicians have difficulty in understanding it. It is to be hoped that a simpler version of the proof can be found.

Theorem 0.1 *If $x(t)$, $y(t)$ and $z(t)$ are nontrivial relatively prime polynomials with real coefficients, satisfying Fermat's equality*

$$x(t)^n + y(t)^n = z(t)^n,$$

where the exponent n is a positive integer, then $n \leq 2$.

An example of a solution when $n = 2$ is $x(t) = 2t$, $y(t) = 1 - t^2$ and $z(t) = 1 + t^2$, since

$$(2t)^2 + (1 - t^2)^2 = t^4 + 2t^2 + 1 = (1 + t^2)^2.$$

Our statement is about polynomials in one variable, but can be easily extended to polynomials in two or more variables. Indeed, if there were a solution of Fermat's equation where $n > 2$ with polynomials in several variables, then we could substitute numerical values for all the variables except one, and obtain a one-variable solution that would contradict the theorem.

There is no simple procedure known for deducing Fermat's last theorem from this theorem. In fact, it is rather unlikely that such a procedure could be found. In spite of that, the theorem as it stands does give us some information about Fermat's original claim. The reason is that, when $n = 2$, the general formula for the integer solutions of Fermat's equation can be expressed using polynomials: if there were any integer solutions of Fermat's equation when $n > 2$, they could not be expressed in terms of polynomials. There are infinitely many integer solutions of the equation $x^2 + y^2 = z^2$; these are called *Pythagorean triples*, and can be obtained by substituting positive integers t and u in the following polynomials

$$\begin{aligned} x(t,u) &= t^2 - u^2; \\ y(t,u) &= 2tu; \\ z(t,u) &= t^2 + u^2. \end{aligned}$$

It is relatively easy to prove that as t and u vary over all possible relatively prime positive integers, not both odd, then the corresponding values of x, y and z vary over all the primitive Pythagorean triples, i.e., all those integer solutions of the equation $x^2 + y^2 = z^2$ which are essentially different from each other. The set of all solutions is then obtained by considering also all nonprimitive triples, i.e., integer multiples of solution triples which have been already found. All this was essentially known to Diophantus and other Greek mathematicians, who produced Pythagorean triples such as $(3, 4, 5)$, or $(5, 12, 13)$ or $(12, 35, 37)$.

Let $\delta(a)$ be the *degree* of the polynomial $a(t)$ and let $\eta(a)$ be the *number of distinct complex roots* of the polynomial $a(t)$. For example, if $a(t) = t^3 - 2t^2 + t = t(t-1)^2$, then $\delta(a) = 3$ and $\eta(a) = 2$.

Observe that

(i) $\eta(a(t)) \leq \delta(a(t))$, since the degree of the polynomial $a(t)$ is the maximum number of distinct roots that $a(t)$ could have,

(ii) $\eta(a(t)^n) = \eta(a(t))$, and

(iii) $\delta(a(t).b(t)) = \delta(a(t)) + \delta(b(t))$.

To prove the main theorem we will use the following result.

Lemma 0.2 (Mason's Lemma) *Let $a(t)$, $b(t)$, and $c(t)$ be nontrivial, relatively prime, polynomials such that $a + b = c$. Then*

$$\max\{\delta(a), \delta(b), \delta(c)\} \leq \eta(abc) - 1$$

Proof of the theorem using Mason's lemma. Let us assume that the lemma holds and that $x(t)$, $y(t)$ and $z(t)$ are three relatively prime polynomial of degree at least 1, such that

$$x(t)^n + y(t)^n = z(t)^n.$$

We want to show that $n \leq 2$.

Applying the lemma with $a = x^n$, $b = y^n$ and $c = z^n$, we get

$$\begin{aligned}\delta(x^n) &\leq \max\{\delta(x^n), \delta(y^n), \delta(z^n)\} \leq \eta(x^n y^n z^n) - 1 \\ &\leq \delta(xyz) - 1 = \delta(x) + \delta(y) + \delta(z) - 1,\end{aligned}$$

so, observing that $\delta(x^n) = n\delta(x)$, we have

$$n\delta(x) \leq \delta(x) + \delta(y) + \delta(z) - 1.$$

By the same argument we can show that

$$\begin{aligned}n\delta(y) &\leq \delta(x) + \delta(y) + \delta(z) - 1, \\ n\delta(z) &\leq \delta(x) + \delta(y) + \delta(z) - 1,\end{aligned}$$

and by adding these three inequalities together we obtain

$$n(\delta(x) + \delta(y) + \delta(z)) \leq 3(\delta(x) + \delta(y) + \delta(z)) - 3,$$

and therefore

$$n \leq 3 - \frac{3}{\delta(x) + \delta(y) + \delta(z)} < 3. \qquad \square$$

Proof of Mason's Lemma. The equation $a + b = c$, where a, b and c are nontrivial relatively prime polynomials, can also be written as $f + g = 1$, where $f = a/c$ and $g = b/c$. Both f and g are rational functions (ratios of polynomials) and they are reduced (their numerators and denominators do not have nontrivial common polynomial divisors). We differentiate the expression $f + g = 1$ with respect to t, and we obtain $f' + g' = 0$, which can also be written in the form

$$\frac{f'}{f} f + \frac{g'}{g} g = 0,$$

and from this last identity we obtain

$$-\frac{f'/f}{g'/g} = \frac{g}{f} = \frac{b}{a}. \qquad (*)$$

Any rational function $r(t)$ can be written as a product

$$r(t) = R(t-\rho_1)^{q_1}(t-\rho_2)^{q_2}\dots(t-\rho_I)^{q_I},$$

where R is a suitable constant, the numbers $\rho_1,\dots,\rho_I$ are the I distinct roots of the numerator and denominator of $r(t)$, and the numbers $q_1,\dots,q_I$ are the corresponding multiplicities, given by a positive integer for the roots of the numerator and a negative integer for the roots of the denominator. For example, if $r(t) = (2t^2-2)/(t^2-4)$, then we represent $r(t)$ by the formula

$$r(t) = 2(t-1)(t+1)(t-2)^{-1}(t+2)^{-1}.$$

Taking the logaritheorem of r and then differentiating with respect to x we have

$$\frac{r'}{r} = \sum_{i=1}^{I}\frac{q_i}{t-\rho_i} = \frac{q_1}{t-\rho_1}+\dots+\frac{q_I}{t-\rho_I}.$$

Notice that in this last expression the multiplicities have become constants and the constant R has disappeared completely. We can write the polynomials a, b, and c in the factorized form

$$\begin{aligned} a(t) &= A(t-\alpha_1)^{l_1}(t-\alpha_2)^{l_2}\dots(t-\alpha_L)^{l_L},\\ b(t) &= B(t-\beta_1)^{m_1}(t-\beta_2)^{m_2}\dots(t-\beta_M)^{m_M},\\ c(t) &= C(t-\gamma_1)^{n_1}(t-\gamma_2)^{n_2}\dots(t-\gamma_N)^{n_N}, \end{aligned}$$

where the roots and multiplicities appear explicitly. Using formula $(*)$, we have

$$\frac{b}{a} = -\frac{f'/f}{g'/g} = -\frac{\sum\frac{l_i}{t-\alpha_i}-\sum\frac{n_k}{t-\gamma_k}}{\sum\frac{m_j}{t-\beta_j}-\sum\frac{n_k}{t-\gamma_k}}.$$

We now multiply the numerator and denominator of this expression by the polynomial $h(t)$, given by the formula

$$h(t) = (t-\alpha_1)\dots(t-\alpha_L)(t-\beta_1)\dots(t-\beta_M)(t-\gamma_1)\dots(t-\gamma_N),$$

and we obtain

$$\frac{b}{a} = -\frac{hf'/f}{hg'/g}.$$

Since $\delta(h) = \eta(abc)$, both hf'/f and hg'/g are polynomials whose degree is at most $\eta(abc)-1$. Furthermore we are assuming that the polynomials a and b are relatively prime, and this last equality implies that their degrees $\delta(a)$ and $\delta(b)$ are at most $\eta(abc)-1$. Since $a+b=c$ we have $\delta(c)\le\eta(abc)-1$ as well, and this concludes the proof of the lemma. □

Another proof of this theorem, together with some further material concerned with Fermat's last theorem which is accessible to high school students, is contained in [3, Chap. 1].

References

[1] S. Lang, Old and new conjectured Diophantine inequalities, *Bull. Amer. Math. Soc. (N.S.)* **23** (1990), 37–75.

[2] R.C. Mason, *Diophantine equations over function fields*, London Math. Soc. Lecture Note Series 96, Cambridge University Press, 1984.

[3] [3] A. van der Poorten, *Notes on Fermat's Last Theorem*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley and Sons, 1996

[4] P. Ribenboim, *13 Lectures on Fermat's Last Theorem*, Springer-Verlag, 1979.

[5] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), 443–551.