The Mason-Stothers Theorem

Jeffrey Paul Wheeler, the University of Pittsburgh*

A child learns of the nonnegative numbers at an early age. Polynomials, on the other hand, demand a little more sophistication and are reserved in a U.S. child's education for middle school. Those fortunate enough to take an undergraduate abstract algebra class realize that the chasm between the integers and polynomials is not so vast. One learns there are similarities: both integers and polynomials form rings; and that there are analogies: the integers have prime factors as their basic building blocks, whereas polynomials (over $\mathbb{C}$) have linear factors. Given this, it is not that surprising that we have the following definitions:

Definition 1 (The Radical of an Integer)**.**
*For $n \in \mathbb{Z}^+$ suppose $n = {p_1}^{e_1} \cdots {p_k}^{e_k}$ where the p_i's are distinct primes and the e_i's are positive integers. We the define the **radical** of n to be:*

$$r(n) = p_1 \cdots p_k \text{ with } r(1) := 1.$$

In other words, $r(n)$ *is the greatest square-free factor of* n or, more simply, *the product of distinct prime factors of* n. As an example, $r(100) = r(2^2 \cdot 5^2) = 2 \cdot 5 = 10$.

Definition 2 (The Radical of a Polynomial)**.**
Let $p(t)$ be a polynomial whose coefficients belong to an algebraically closed field of characteristic 0. We put $\mathbf{n_0(p(t))}$ = the number of distinct zeros of $p(t)$.

(In a ring R, if there exists a $n \in \mathbb{Z}^+$ such that $na = 0$ for all $a \in R$, then the least such positive integer is called the *characteristic of the ring.*

*Department of Mathematics, the University of Pittsburgh, Pittsburgh PA 15260, USA. E-mail: `jwheeler@pitt.edu`.

Algebraically closed just means we are in the right place for all the roots of the polynomial to exist; think of polynomials with coefficients in $\mathbb{C}$ - they can be written as a product of linear factors if we allow roots from $\mathbb{C}$).

With these definitions we state

Theorem 1 (Mason-Stothers Theorem)**.**
Let $a(t), b(t)$, and $c(t)$ be polynomials whose coefficients belong to an algebraically closed field of characteristic 0. Suppose $a(t), b(t)$, and $c(t)$ are relatively prime and that $a(t) + b(t) = c(t)$. Then

$$\max \deg\{a(t), b(t), c(t)\} \leq n_0(a(t) \cdot b(t) \cdot c(t)) - 1.$$

This beautiful theorem is easily understood and it's proof requires just a little knowledge of abstract algebra. What is intriguing is that the analogous statement for the integers is still unproven[1]. This is the important open problem in Number Theory known as the *abc Conjecture*[2]:

Conjecture 1 (The abc Conjecture - Masser's Version)**.**
Consider a nontrivial triple of integers (a, b, c) such that $a + b = c$ and $\gcd(a, b, c) = 1$. Then for every $\epsilon > 0$ there exists a universal constant $\mu(\epsilon)$ such that

$$\max\{|a|, |b|, |c|\} \leq \mu(\epsilon)[r(abc)]^{1+\epsilon}.$$

Hence, the remarkable fact that we have a problem for polynomials that is much easier to establish than the analogous statement for integers. This is not the only one. We offer

Problem: Use the Mason-Strother's Theorem to establish a polynomial Fermat's Last Theorem; that is

Corollary (Polynomial Fermat's Last Theorem)**.**
Let $x(t), y(t)$, and $z(t)$ be relatively prime polynomials whose coefficients belong to an algebraically closed field of characteristic 0 such that at least one

[1] We note that Shinichi Mochizuki of Kyoto University has offered a proof in the form of a series of papers on his website [3]. A review is in process.

[2] The conjecture was originally posed in 1985 by David Masser (considering an integer analog of Mason's Theorem) [2] and in 1988 by Joseph Oesterlé (considering a conjecture of Szpiro regarding elliptic curves) [4].

of them has degree > 0. *Then*

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

has no solution for $n \geq 3$.

References

[1] Mason, R. C. (1984), *Diophantine Equations over Function Fields*, London Mathematical Society Lecture Note Series 96, Cambridge, England: Cambridge University Press.

[2] Masser, D. W. (1985). *Open problems.* In Chen, W. W. L. Proceedings of the Symposium on Analytic Number Theory. London: Imperial College

[3] Mochizuki, Shinichi. *Personal webpage.* `http://www.kurims.kyoto-u.ac.jp/~motizuki/top-english.html`

[4] Oesterlé, Joseph (1988), *Nouvelles approches du "thorme" de Fermat*, Astrisque, Sminaire Bourbaki exp 694 (161): 165186

[5] Stothers, W. W. (1981), *Polynomial identities and hauptmoduln*, Quarterly J. Math. Oxford, 2 32: 349370.