*abc*s in the Margin: Solution

Note that the degree is multiplicative: if $f(t)$ and $g(t)$ are polynomials, then

$$\deg\big[f(t)g(t)\big] = \deg f(t) + \deg g(t).$$

This means if $f(t)$ is a factor of $g(t)$ then $\deg f(t) \le \deg g(t)$.

Assume for the sake of contradiction $a(t)^n + b(t)^n = c(t)^n$ for nonconstant polynomials $a(t), b(t), c(t)$. If any two of them shared a nonconstant factor $f(t)$, then so would the third. For example, if $a(t) = f(t)u(t)$ and $c(t) = f(t)v(t)$ then $b(t)^n = f(t)^n\big[v(t) - u(t)\big]$ implies $f(t)^n$ is a factor of $b(t)^n$ so $f(t)$ must be a factor of $b(t)$. We could divide $a(t)^n + b(t)^n = c(t)^n$ by $f(t)^n$ to get another solution with smaller-degree polynomials. Without loss of generality, then, we may assume the polynomials are pairwise coprime.

Then the *abc* theorem applies to the polynomials $a(t)^n, b(t)^n, c(t)^n$:

$$\max\{\deg a(t)^n, \deg b(t)^n, \deg c(t)^n\} < \deg \operatorname{rad}\big[a(t)^n b(t)^n c(t)^n\big].$$

Since $f(t)^n$ has the same irreducible factors as $f(t)$, the radical on the right-hand side is unaffected by the power n. By multiplicativity, however, the left-hand side is affected, since $\deg f(t)^n = n \deg f(t)$ for each polynomial:

$$n \max\{\deg a(t), \deg b(t), \deg c(t)\} < \deg \operatorname{rad}\big[a(t)b(t)c(t)\big]$$

The assumption $n > 2$ implies

$$\begin{aligned} & n \max\{\deg a(t), \deg b(t), \deg c(t)\} \\ \ge\ & 3 \max\{\deg a(t), \deg b(t), \deg c(t)\} \\ \ge\ & \deg a(t) + \deg b(t) + \deg c(t) \\ =\ & \deg\big[a(t)b(t)c(t)\big]. \end{aligned}$$

But putting this inequality together with the last one yields

$$\deg\big[a(t)b(t)c(t)\big] < \deg \operatorname{rad}\big[a(t)b(t)c(t)\big],$$

which is impossible because $\operatorname{rad}\big[a(t)b(t)c(t)\big]$ is a factor of $a(t)b(t)c(t)$.

The ***abc* conjecture** is actually about integers, not polynomials. It says, effectively, that for positive coprime integers (a, b, c) satisfying $a + b = c$, the value c rarely exceeds the radical $\text{rad}(abc)$ by much. (The radical of an integer is the product of its prime factors, for example $\text{rad}\, 24 = 6$.) More precisely, it says no matter how small $\varepsilon > 0$ is, there are only finitely many exceptions to the inequality $c < \text{rad}(abc)^{1+\varepsilon}$. The version of *abc* for polynomials instead of integers is called the Mason-Stothers theorem and has a quick, (relatively) simple proof using Wronskians.

The *abc* conjecture has numerous implications in number theory, one being an alternate proof **Fermat's Last Theorem**, which says for $n > 2$ there are no nontrivial integer solutions (a, b, c) to $a^n + b^n = c^n$. This was written by Fermat (found by his son in the margin of his copy of *Arithmetic*, a 3rd century book by Diophantus about exactly these kinds of equations, now called Diophantine equations), famously adding "I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain."

While it's doubtful Fermat really had a proof, nonetheless, the mathematical community's subsequent quest for a proof is oft-touted as the birth of algebraic number theory. The first valid proof appeared three-and-a-half centuries later in the mid-90s by Andrew Wiles, by linking it to and then proving (a narrow version of) the Taniyama-Shimura conjecture, now called the **modularity theorem**, which asserts a rational correspondence between rational elliptic curves and classical modular curves.

This problem highlights similarities between integers and polynomials. Both admit factorizations into primes/irreducibles. Long division with quotients and remainders is possible for both. Relative size can be measured by absolute value or degrees. Even partial fraction decompositions are possible for rational numbers just as they are for rational functions. And as we've seen, both contexts have versions of the *abc* theorem, Fermat's Last Theorem, and many other theorems. When we use finite fields for polynomial coefficients this observation is called the **function field analogy**.