

August 2, 2007

CHAPTER EIGHT

DIOPHANTINE EQUATIONS FOR POLYNOMIALS

§1. THE abc THEOREM

Just as we can have polynomial equations that have solutions in integers, we can have polynomial equations that have solutions in polynomials. A useful result that is useful in analyzing the possibilities is the *abc Theorem* by Mason.

Theorem. *Suppose that $a(x)$, $b(x)$, $c(x)$ are pairwise coprime polynomials and nonconstant polynomials for which*

$$a(x) + b(x) + c(x) = 0 .$$

Suppose that $a(x)b(x)c(x)$ has exactly k distinct zeros. Then the degrees of each of the polynomials $a(x)$, $b(x)$ and $c(x)$ cannot exceed $k - 1$.

Proof. Let $f = a/c$ and $g = b/c$. These are rational functions for which $f + g + 1 = 0$ and $f' = -g'$. Suppose that $a(x) = \prod(x - u)^r$, $b(x) = \prod(x - v)^s$ and $c(x) = \prod(x - w)^t$ where u, v, w run through the roots of a , b and c , respectively. Because of the coprime condition, the sets of u , v and w do not overlap. Then

$$\frac{f'(x)}{f(x)} = \sum \frac{r}{x - u} - \sum \frac{t}{x - w}$$

and

$$\frac{g'(x)}{g(x)} = \sum \frac{s}{x - v} - \sum \frac{t}{x - w} .$$

Suppose that $h(x) = \prod(x - u) \prod(x - v) \prod(x - w)$. The degree of $h(x)$ is exactly k and the functions $\phi(x) = h(x)f'(x)/f(x)$ and $\psi(x) = h(x)g'(x)/g(x)$ are both polynomials of degree not exceeding $k - 1$.

We have that

$$\frac{b(x)}{a(x)} = \frac{g(x)}{f(x)} = -\frac{f'(x)/f(x)}{g'(x)/g(x)} = -\frac{\phi(x)}{\psi(x)} .$$

Thus,

$$b(x)\psi(x) = a(x)\phi(x) .$$

Since $a(x)$ and $b(x)$ are coprime, $a(x)$ must divide $\phi(x)$, and so its degree cannot exceed $k - 1$. Similarly, the degree of $b(x)$ does not exceed $k - 1$. The degree of $c(x)$ can be handled similarly. ♠

Theorem. (Davenport) *Let $f(x)$ and $g(x)$ be coprime nonconstant polynomials. Then the degree of $f^3 - g^2$ is at least $\frac{1}{2}(\deg f(x)) + 1$.*

Proof. If the degrees of f^3 and g^2 differ, then the degree of $f^3 - g^2$ is at least equal to the degree of f^3 or three times the degree of f and the result follows.

Suppose that the degrees of f^3 and g^2 are equal to $6m$, so that the degree of f is $2m$ and of g is $3m$. Since $(f^3 - g^2) + (-f^3) + g^2 = 0$ and the number of zeros of the product of f^3 , g^2 and $f^3 - g^2$ cannot exceed the sum of their degrees, we have, by the *abc theorem*,

$$6m \leq 2m + 3m + \deg(f^3 - g^2) - 1 .$$

whence

$$\deg(f^3 - g^2) \geq m - 1 = \frac{1}{2}(\deg f) - 1 .$$



Equality in Davenport's theorem is attained when $f(t) = t^2 + 2$ and $g(t) = t^3 + 3t$.

§2. FERMAT'S THEOREM FOR POLYNOMIALS

The *abc* Theorem allows for a quick proof of the following result: The equation $f(x)^n + g(x)^n = h(x)^n$ has nontrivial solutions for n a positive integer, only when $n = 1$ and $n = 2$.

The case $n = 1$ is obvious, and an example of a solution when $n = 2$ is $(f(x), g(x), h(x)) = (x^2 - 1, 2x, x^2 + 1)$. Suppose, for some value of n , the identity holds where at least one polynomial has positive degree. Then, by the *abc* Theorem, each of the degrees of $f(x)^n, g(x)^n, h(x)^n$ cannot exceed $\deg f(x) + \deg g(x) + \deg h(x) - 1$ (since a polynomial and each of its powers have the same number of distinct roots). Hence

$$n \deg f(x) \leq \deg f(x) + \deg g(x) + \deg h(x) - 1$$

$$n \deg g(x) \leq \deg f(x) + \deg g(x) + \deg h(x) - 1$$

$$n \deg h(x) \leq \deg f(x) + \deg g(x) + \deg h(x) - 1 .$$

a Adding the three inequalities yields that

$$n(\deg f(x) + \deg g(x) + \deg h(x)) \leq 3((\deg f(x) + \deg g(x) + \deg h(x)) - 1) .$$



More generally, we can analyse the diophantine equation $f^\alpha + g^\beta = h^\gamma$, where α, β and γ are positive integers exceeding 1. Wolog, we may suppose that $2 \leq \alpha \leq \beta \leq \gamma$. If a, b, c are the respective degrees of f, g, h , we have that

$$\alpha a \leq a + b + c - 1$$

$$\beta b \leq a + b + c - 1$$

$$\gamma c \leq a + b + c - 1 .$$

Adding these three inequalities yields that

$$\alpha(a + b + c) \leq \alpha a + \beta b + \gamma c \leq 3(a + b + c - 1) ,$$

whence $\alpha < 3$. Thus, $\alpha = 2$. The three inequalities become $a \leq b + c - 1$, $\beta b \leq a + b + c - 1$ and $\gamma c \leq a + b + c - 1$. Again, adding the three inequalities, yields

$$\beta(b + c) \leq \beta b + \gamma c \leq 3(b + c) + a - 3 \leq 4(b + c) - 4 ,$$

whence $\beta < 4$. Hence $\beta = 2$ or $\beta = 3$.

Solutions can be found for $(\alpha, \beta, \gamma) = (2, 2, n)$ for any integer $n \geq 2$. So, suppose that $\beta = 3$. Then $a \leq b + c - 1$ and $2b \leq a + c - 1$ lead to $b \leq 2c - 2$ and $a \leq 3c - 3$. Thus, $\gamma c \leq 6c - 5$, so that $\gamma \leq 5$.

Solutions can be found for all of the values of (α, β, γ) within these bounds.

S3. CATALAN'S EQUATION FOR RATIONAL FUNCTIONS

Finally, we show that $u(x)^m - v(x)^n = 1$ is not solvable for rational functions, unless $m = n = 2$. When $m = n = 2$, it is satisfied by $(u(x), v(x)) = ((x^2 - 1)(x^2 + 1)^{-1}, 2x(x^2 + 1)^{-1})$.

Suppose that $u(x) = f(x)/g(x)$ and $v(x) = h(x)/k(x)$, where both the pairs (f, g) and (h, k) are coprime. Then

$$f(x)^m k(x)^n + g(x)^m h(x)^n = g(x)^m k(x)^n . \quad (*)$$

Since (f, g) is coprime, $g(z) = 0$ implies that $k(u) = 0$. Since (h, k) is coprime, $k(z) = 0$ implies that $g(u) = 0$. Hence, there is a set of complex numbers z_i for which

$$g(x) = \prod (x - z^i)^{a_i}$$

and

$$k(x) = \prod (x - z^i)^{b_i},$$

where the a_i and b_i are positive integers. The multiplicity of z_i as a root of the three terms of $(*)$ respectively are nb_i , ma_i and $nb_i + ma_i$ respectively. If nb_i and ma_i differ, then the multiplicity of z_i as a root of the left side is the lesser of these, which is not possible. Hence $nb_i = ma_i$, from which we deduce that $k(x)^n = g(x)^m$. Hence $f(x)^m - h(x)^n = g(x)^m$.

From the result in Section 2, we see that $(m, n) = (2, 2)$ or $(m, n) = (3, 2)$. In the latter case, $g(x)^3 = k(x)^2 = l(x)^6$ for some polynomial $l(x)$. This yields $f(x)^3 - h(x)^2 = l(x)^6$, which is not solvable. ♣