CHAPTER ELEVEN

DIOPHANTINE EQUATIONS FOR POLYNOMIALS

§1. INTRODUCTION

In Section 10.4, we noted that the pellian equation $x^2 - dy^2 = k$ and $x^3 + cy^3 + c^2z^3 - 3cxyz = 1$ can be solved when the parameters c and d and variables x, y, z are polynomials. The solution $(x, y, z) = (s^2 - t^2, 2st, s^2 + t^2)$ for $x^2 + y^2 = z^2$ is also well-known. It is natural to consider other diophantine equations for which polynomial solutions might exist, such as the Fermat equation $x^n + y^n = z^n$. It is a deep result that, when $n \geq 3$, there are no nontrivial solutions for the Fermat equation in integers, which then rules out solutions in polynomials over **Z**. However, this latter result is obtainable more directly with the aid of a remarkable result called the "*abc* Theorem".

The *abc* Theorem for polynomials is a kind of analogue of the *abc* Conjecture in number theory formulated by Oesterlé and Masser in 1985, which states that, *if* $\epsilon > 0$ *and the integers* a, b, c *are pairwise coprime with* $a + b = c$, *then the maximum of* $|a|$, $|b|$, $|c|$ *does not exceed* $C_\epsilon \prod p^{1+\epsilon}$ *where* C_ϵ *depends only on* ϵ *and the product is taken over all primes* p *dividing* abc. Since this conjecture implies the truth of Fermat's Last Theorem for sufficiently large exponents, it is deep. However, the polynomial version, known as Mason's Theorem, is much more tractable with a brief and easily understandable proof. It was proved in 1981 by W.W. Stothers. [**4, 6**].

§2. THE abc THEOREM

Theorem 11.1. *Suppose that* $a(x)$, $b(x)$, $c(x)$ *are pairwise coprime nonconstant polynomials for which*

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

Suppose that the product $a(x)b(x)c(x)$ *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 $f + g = 1$ 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 coprimality 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 11.2. (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 $(f^3 - g^2) + g^2 = f^3$ and the number of zeros of the product of f^3, g^2 and $f^3 - g^2$ cannot exceed the sum of the degrees of f, of g and of $f^3 - g^2$, 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 $g(t) = t^3 + 3t$.

§3. 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 in polynomials f and g 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

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

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

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

Adding the three inequalities yields that

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

so that $n < 3$. ♣

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, $\gamma c \leq 6c - 6$, so that $\gamma \leq 5$.

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

S4. 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 polynomial pairs (f, g) and (h, k) are coprime. Then

$$f(x)^m k(x)^n - g(x)^m h(x)^n = g(x)^m k(x)^n \ . \tag{11.1}$$

Since (f, g) is coprime, $g(u) = 0$ implies that $k(u) = 0$. Since (h, k) is coprime, $k(u) = 0$ implies that $g(u) = 0$. Hence, there is a finite 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 (11.1) 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 3, 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. ♣

\$5. PROBLEMS AND INVESTIGATIONS

1. Determine polynomials solutions to each of the following diphantine equations:

(a) $a^3 + b^3 + c^3 = d^3$;

(b) $\frac{1}{2}a(a + 1) + b^2 = c^3$.

2. Determine polynomial solutions to the simultaneous system of diophantine equations:

$$2(b^2 + 1) = a^2 + c^2 \ ; \quad 2(c^2 + 1) = b^2 + d^2 \ .$$

Hints and references

1. (b) See [AMM #10510; 1996, 266; 105:4 (April, 1998), 375]. Two simple solutions are

$$(a, b, c) = (2x^2 - 1, x(x^2 - 1), x^2) \ ;$$

$$(a, b, c) = (32x^6 - 1, 4x^3, 8x^4) \ .$$

2. See [**2**].

References

1. E.J. Barbeau, *Polynomials.* Springer, 1989, 1995 Exploration E.10,

2. H. Davenport, On $f^3(t) - g^2(t)$. *Norske Vid. Selsk. Forh. (Trondheim)* 38 (1965), 86-87
3. R.C. Mason, *Diophantine equations over function fields.* Cambridge University Press, 1984
4. Terry Sheil-Small, *Complex polynomials.* Campbridge, 2002
Chapter XI, pp. 370-372
5. W.W. Stothers, Polynomial identities and Hauptmodulen. *Quarterly J. Math. Oxford Ser. II* 32 (1981), 349-370
6. Eric W. Weisstein, *abc* conjecture. *Mathworld - A Wolfram Web Resource*
http://mathworld.wolfram.com/abcConjecture.html
7. Eric W. Weisstein, Mason's theorem. Mathworld - A Wolfram Web resource
http://mathworld.wolfram.com/MasonsTheorem.html
8. *http://math.unicaen.fr/~nitaj/abc.html*