DIOPHANTINE EQUATIONS FOR POLYNOMIALS (MA2316, EIGHTH WEEK)

VLADIMIR DOTSENKO

In this lecture, we shall discuss some "Diophantine equations for polynomials", that is solutions to polynomial equations (in several variables) that are themselves polynomials (in one variable).

All key results here will follow from the following result, which was proved surprisingly recently (early 1980s). Let us denote by $N_0(f)$ the number of distinct complex zeros of a polynomial f, for example $N_0(x^2+1)=2$, $N_0(x^{100})=1$, $N_0(5)=0$.

Theorem 1 (Mason–Stothers Theorem)**.** *Suppose that $f(x), g(x), h(x) \in \mathbb{C}[x]$ are coprime polynomials, and not all of them are constant. If $f+g+h=0$, then*

$$\max(\deg(f), \deg(g), \deg(h)) \leq N_0(fgh) - 1.$$

The following proof is probably the shortest one known. A prominent American mathematician Serge Lang mentioned this theorem to a then high school student Noah Snyder (now a renowned mathematician himself), who came up with this elegant proof which is shorter and clearer than ones known previously.

Proof. Let us recall that each root of multiplicity k of a given polynomial $f(x)$ is a root of multiplicity $k-1$ of $f'(x)$. Indeed, if $f(x) = (x-a)^k g(x)$ where $g(a) \neq 0$, then $f'(x) = k(x-a)^{k-1}g(x) + (x-a)^k g'(x) = (x-a)^{k-1}(kg(x) + (x-a)g'(x))$, and the expression in the brackets does not vanish at $x=a$. This implies that

$$\deg \gcd(f, f') = \deg(f) - N_0(f).$$

Indeed, if $f(x) = (x-a_1)^{k_1}(x-a_2)^{k_2}\cdots(x-a_m)^{k_m}$, then our previous remark shows that $\gcd(f,f') = (x-a_1)^{k_1-1}(x-a_2)^{k_2-1}\cdots(x-a_m)^{k_m-1}$, so

$$\deg \gcd(f, f') = k_1 - 1 + k_2 - 1 + \cdots + k_m - 1 = (k_1 + \cdots + k_m) - m = \deg(f) - N_0(f).$$

Now everything is ready for our proof. Note that since $f+g+h=0$, we have $f'+g'+h'=0$, and hence $fh' - f'h = f(-f'-g') - f'(-f-g) = f'g - fg'$. Also, we remark that since not all of the f, g, h are constant, there are at least two non-constant polynomials among them. Without loss of generality, these are f and g. That implies $f'g - fg' \neq 0$, for otherwise, since f and g are coprime, we would conclude that $f \mid f'$, which is impossible. Finally, we note that $\gcd(f,f')$ and $\gcd(g,g')$ manifestly divide $f'g - fg'$, but since we know that $f'g - fg' = fh' - f'h$, we also conclude that $\gcd(h,h')$ divides $f'g - fg'$. Note that since f, g, h are coprime, the polynomials $\gcd(f,f')$, $\gcd(g,g')$, and $\gcd(h,h')$ are coprime, so $f'g - fg'$ is divisible by their product. As a consequence,

$$\begin{aligned}\deg(f) - N_0(f) + \deg(g) - N_0(g) + \deg(h) - N_0(h) = \\ = \deg(\gcd(f,f')\gcd(g,g')\gcd(h,h')) \leq \deg(f'g - fg') \leq \deg(f) + \deg(g) - 1,\end{aligned}$$

or $\deg(h) \leq N_0(f) + N_0(g) + N_0(h) - 1 = N_0(fgh) - 1$. (The latter step again uses that f, g, h are coprime). Repeating the last step but replacing $\deg(f'g - fg') \leq \deg(f) + \deg(g) - 1$ by $\deg(f'g - fg') = \deg(fh' - f'h) \leq \deg(f) + \deg(h) - 1$, we get $\deg(g) \leq N_0(f) + N_0(g) + N_0(h) - 1 = N_0(fgh) - 1$, and a similar inequality for $\deg(f)$ as well. We conclude that

$$\max(\deg(f), \deg(g), \deg(h)) \leq N_0(fgh) - 1,$$

as required. □

Corollary (Fermat's Last Theorem for polynomials)**.** *Let $f(x), g(x), h(x) \in \mathbb{C}[x]$ be coprime polynomials satisfying $f^n + g^n = h^n$ for some $n \geq 3$. Then these polynomials are constant.*

(Of course, unlike integers, we cannot say that there are no solutions, since in $\mathbb{C}$ we can extract n^{th} roots, and so for example $1^n + 1^n = (\sqrt[n]{2})^n$ is a solution).

Proof. Assume the contrary, and apply Mason–Stothers to $f^n, g^n, -h^n$:

$$\begin{aligned} n\deg(f) &\leq N_0(f^n g^n h^n) - 1 = N_0(fgh) - 1 \leq \deg(f) + \deg(g) + \deg(h) - 1, \\ n\deg(g) &\leq N_0(f^n g^n h^n) - 1 = N_0(fgh) - 1 \leq \deg(f) + \deg(g) + \deg(h) - 1, \\ n\deg(h) &\leq N_0(f^n g^n h^n) - 1 = N_0(fgh) - 1 \leq \deg(f) + \deg(g) + \deg(h) - 1. \end{aligned}$$

Adding these inequalities, we get

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

so

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

which for $n \geq 3$ is clearly a contradiction. □

Remark. *Later, if you learn some algebraic geometry, you will see another very elegant proof of this last result. Recall that when we enumerated Pythagorean triples, we first obtained a parametrisation of all rational points on the circle $x^2 + y^2 = 1$ of the form $\left(\frac{2k}{k^2+1}, \frac{k^2-1}{k^2+1}\right)$. Our result states that for higher exponents, nothing like that would work, that is the "Fermat's curve" $x^n + y^n = 1$ does not admit a rational parametrisation. Algebraic geometry explains it very clearly indeed, saying that the Fermat's curve, viewed as a complex curve, that is something of $\mathbb{R}$-dimensions 2, looks like a sphere with $\frac{(n-1)(n-2)}{2}$ handles attached to it (e.g. for $n = 3$ looks like a torus), and that existence of a rational parametrisation would imply that there can be no handles, so it must be just a sphere.*

This last result can be generalised as follows.

Corollary. *Let p, q, r be positive integers, and let $f(x), g(x), h(x) \in \mathbb{C}[x]$ be coprime polynomials satisfying $f^p + g^q = h^r$, and not all of them are constant. Then $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$.*

Proof. Assume the contrary, and apply Mason–Stothers to $f^p, g^q, -h^r$:

$$\begin{aligned} p\deg(f) &\leq N_0(f^n g^n h^n) - 1 = N_0(fgh) - 1 \leq \deg(fgh) - 1 < \deg(fgh), \\ q\deg(g) &\leq N_0(f^n g^n h^n) - 1 = N_0(fgh) - 1 \leq \deg(fgh) - 1 < \deg(fgh), \\ r\deg(h) &\leq N_0(f^n g^n h^n) - 1 = N_0(fgh) - 1 \leq \deg(fgh) - 1 < \deg(fgh), \end{aligned}$$

so we have

$$\frac{\deg(f)}{\deg(fgh)} < \frac{1}{p}, \quad \frac{\deg(g)}{\deg(fgh)} < \frac{1}{q}, \quad \frac{\deg(h)}{\deg(fgh)} < \frac{1}{r},$$

and adding these inequalities, we get

$$1 < \frac{1}{p} + \frac{1}{q} + \frac{1}{r},$$

as claimed. □

Remark. *The triples $2 \leq p \leq q \leq r$ satisfying the above inequality are $(2, 2, m)$, $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$. Solutions to the corresponding Diophantine equations are closely related to regular polyhedra in three dimensions.*

Corollary. *The elliptic curve $y^2 = x^3 - x$ does not admit a rational parametrisation $x = \frac{a(t)}{b(t)}$, $y = \frac{c(t)}{d(t)}$.*

Proof. We assume that $\frac{a(t)}{b(t)}$ and $\frac{c(t)}{d(t)}$ are written in lowest terms, that is $\gcd(a, b) = \gcd(c, d) = 1$. Clearing the denominators, we obtain

$$c^2b^3 = a^3d^2 - ab^2d^2,$$

so $b^2 \mid d^2$, implying $b \mid d$, and $d = kb$. Also, $d^2 \mid b^3$, so $k^2b^2 \mid b^3$, $k^2 \mid b$, and $b = k^2l$. So we have $d = kb = k^3l$ and $b = k^2l$. Substituting these into the original equation, we get

$$c^2k^6l^3 = a^3k^6l^2 - ak^4l^2k^6l^2,$$

or

$$c^2l = a^3 - ak^4l^2,$$

so $l \mid a^3$. But $l \mid b$ as well, so l is a constant. Rewriting the last equation as

$$(c\sqrt{l})^2 = a(a^2 - (k^4l)^2),$$

and noticing that $\gcd(a, a^2 - (k^4l)^2) = 1$ since $k \mid b$ and $\gcd(a, b) = 1$, we conclude that $a = A^2$ and $a^2 - (k^4l)^2 = B^2$ for some A, B, since the product of two coprime polynomials is a square only when both of them are squares. We observe that in that case

$$A^4 = (k^4l)^2 + B^2 = (k^2\sqrt{l})^4 + B^2,$$

and $\gcd(A, k^2\sqrt{l}) = 1$, so the polynomials $A, k^2\sqrt{l}, B$ are coprime, and the previous corollary shows that they must be constant, in which case a is a constant, k is a constant, so b is a constant, and therefore x is constant, not a rational parametrisation. □

Exercise. Analyse the proof of the last statement, where until the very final step we in fact were not using much about polynomials, mostly just divisibility. Try to use that proof to classify $\mathbb{Q}$-points on the curve $y^2 = x^3 - x$.