Runge's theorem on Diophantine equations

Martin Klazar

(lecture on the 7-th PhD conference)

Ostrava, September 10, 2013

A (binary) Diophantine equation is an equation

$$F(x,y) = 0\ ,$$

where $F \in \mathbb{Z}[x,y]$ is a polynomial, with solutions in the integers, $x, y \in \mathbb{Z}$. (We will use x, y to denote both the formal variables and their numeric values in $\mathbb{Z}$ or $\mathbb{R}$.) The 20th century saw great advances in resolution of such equations, associated with the names of A. Thue, C.-L. Siegel and A. Baker. But it was at the end of the previous century, in 1887, when C. Runge [2] in a pioneering result proved finiteness of the number of solutions for a large class of Diophantine equations; his method is still used today to solve specific equations. In this lecture we will prove, by generating functions, a particular case of Runge's theorem:

Theorem (Runge, a particular case). *Suppose that $F \in \mathbb{Z}[x,y]$ is nonzero and irreducible in $\mathbb{Q}[x,y]$, $n = \deg F = \deg_y F \geq 2$ and the polynomial $f(1,y) \in \mathbb{Z}[y]$, where $f(x,y)$ is the leading degree n form of $F(x,y)$, is reducible in $\mathbb{Q}[y]$ and has only simple roots. Then the equation*

$$F(x,y) = 0$$

has only finitely many solutions $x, y \in \mathbb{Z}$.

(We write $F(x,y) = f_n(x,y) + f_{n-1}(x,y) + \ldots + f_0(x,y)$, where $f_j(x,y)$ is zero or a homogeneous polynomial with total degree j, and set $f = f_n$.) At the end of the lecture we state Runge's theorem in its general form.

For example, the above theorem implies that any equation of the form

$$y^n = (ax)^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0\ ,$$

where $n \geq 2$, $a, a_i \in \mathbb{Z}$, $a \neq 0$ and the polynomial on the right side is not a d-th power in $\mathbb{Z}[x]$ for any divisor $d \geq 2$ of n, has only finitely many solutions $x, y \in \mathbb{Z}$.

Exercise. Check that this example satisfies assumptions of the theorem.

We prove the above theorem and start with a lemma: If $0 \neq P \in \mathbb{Z}[x,y]$ has $\deg_y P < \deg_y F (= n)$ then $F(x,y) = P(x,y) = 0$ for only finitely many $x, y \in \mathbb{Z}$. Indeed, F is irreducible also in $\mathbb{Z}(x)[y]$ (by Gauss lemma) and since P has in y a lower degree, F and P are coprime in $\mathbb{Z}(x)[y]$. By Bachet's identity in this ring, $uF + vP = 1$ for some $u, v \in \mathbb{Z}(x)[y]$. Clearing denominators in the coefficients of u and v, we get polynomials $U, V \in \mathbb{Z}[x][y]$ and $0 \neq W \in \mathbb{Z}[x]$ such that

$$UF + VP = W \ .$$

Thus $x, y \in \mathbb{Z}$ and $F(x,y) = P(x,y) = 0$ implies that $W(x) = 0$. For any fixed $x \in \mathbb{Z}$ there are at most n values $y \in \mathbb{Z}$ with $F(x,y) = 0$ (due to irreducibility of F). Hence $F(x,y) = P(x,y) = 0$ for at most $n \deg W$ values $x, y \in \mathbb{Z}$ and the lemma is proven.

We denote the real roots of $f(1,y)$ by α. We show that there is an $\varepsilon > 0$ and at most n polynomials $P_\alpha \in \mathbb{Z}[x,y]$, indexed by the real roots α, with the property that each P_α is nonzero, $\deg_y P_\alpha < n$ and if $x, y \in \mathbb{Z}$ satisfy $F(x,y) = 0$ and $|x| > 1/\varepsilon$, then also $P_\alpha(x,y) = 0$ for some α. By the previous lemma and its proof, $F(x,y) = 0$ has at most $(1 + 2/\varepsilon)n + n^2 c$ solutions $x, y \in \mathbb{Z}$, where $c = \max_\alpha \deg W_\alpha$, and we are done.

In order to construct the polynomials P_α, we solve $F(x,y) = 0$ for $x, y \in \mathbb{R}$ and x near ∞. For this we make the change of variables $x = 1/t, y = s/t$ and consider the integral polynomial

$$G(t,s) = t^n F(1/t, s/t) = g_n(s) + t g_{n-1}(s) + \ldots + t^n g_0(s) \ ,$$

where $g_j(s) = t^j f_j(1/t, s/t) \in \mathbb{Z}[s]$ has degree at most j (or is zero). We set $g(s) = g_n(s)$. Since $g(s) = f(1,s)$, the polynomial $g(s) \in \mathbb{Z}[s]$ has degree $n \geq 2$, is reducible and has no multiple root. Recall that α denotes the real roots of $g(s) = f(1,s)$. It follows that any pair $(t,s) = (0,\alpha)$ is a solution of

$$G(t,s) = 0 \ .$$

Since $\partial_s G(0,\alpha) = g'(\alpha) \neq 0$ (g has no multiple root), the implicit functions theorem applies in a neighborhood of the pair $(0,\alpha)$ and tells us that

- there is an $\varepsilon > 0$ such that for every $t \in (-\varepsilon, \varepsilon)$ there exists exactly one $s \in (\alpha - \varepsilon, \alpha + \varepsilon)$ with $G(t,s) = 0$, and the corresponding function

$s = s_\alpha(t)$ is analytic on $(-\varepsilon, \varepsilon)$:

$$s_\alpha(t) = \alpha + \alpha_0 t + \alpha_1 t^2 + \dots$$

for some coefficients $\alpha_j \in \mathbb{R}$.

The power series $s_\alpha(t)$ have other useful properties. It is not hard to prove that they capture every solution close to 0 in t:

- for small enough $\varepsilon > 0$, if $t \in (-\varepsilon, \varepsilon)$ and $s \in \mathbb{R}$ satisfy $G(t, s) = 0$, then $s = s_\alpha(t)$ for some α.

Considering the equation $G(t, s) = 0$ with $s \in \mathbb{C}[[t]]$ formally, ones sees that all coefficients α_j in $s_\alpha(t)$ express rationally in terms of α:

- for every $j = 0, 1, \dots$, the coefficient α_j lies in the number field $\mathbb{Q}(\alpha)$.

Exercise. Prove in detail the previous two claims on the power series $s_\alpha(t)$.

We return to the variables x, y. All expansions $\varphi_\alpha(x)$, given by

$$s/t = y = \varphi_\alpha(x) = s_\alpha(t)/t = x s_\alpha(1/x) = \alpha x + \alpha_0 + \alpha_1 x^{-1} + \dots \ ,$$

converge for $x \in \mathbb{R}$, $|x| > 1/\varepsilon$, for small enough $\varepsilon > 0$. By the second claim on $s_\alpha(t)$, if $x, y \in \mathbb{Z}$ satisfy $F(x, y) = 0$ and $|x| > 1/\varepsilon$, then there is an α (a real root of $f(1, s)$) such that $y = \varphi_\alpha(x)$.

We fix an α and prove that for $h \in \mathbb{N}$ large enough in terms of n, there exist polynomials $A_0, A_1, \dots, A_{n-1} \in \mathbb{Z}[x]$, not all of them zero, such that each $\deg A_i \le h$ and in (the expansion of)

$$\Phi_\alpha(x) = \sum_{i=0}^{n-1} A_i(x) \varphi_\alpha(x)^i$$

every power x^k with $k \ge 0$ has zero coefficient. By the third claim on $s_\alpha(t)$, each α_j is a $\mathbb{Q}$-linear combination of the d powers $1, \alpha, \alpha^2, \dots, \alpha^{d-1}$, where

$$d = \deg(\alpha) = [\mathbb{Q}(\alpha) : \ \mathbb{Q}] \ .$$

There are $h+n$ powers x^k in $\Phi_\alpha(x)$ with $k \ge 0$. The requirement on existence of the A_i is equivalent to a nontrivial solvability in $\mathbb{Z}$ of a homogeneous linear system with rational coefficients and with $d(h + n)$ equations (each of the d

coordinates — the coefficients of $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ — of each coefficient of x^k with $k \geq 0$ is set to 0) and $n(h+1)$ unknowns (the unknown coefficients in the polynomials A_i). By a well-known lemma, if the number of unknowns exceeds the number of equations, in our case if

$$n(h+1) > d(h+n) \ ,$$

then the system has a nontrivial solution (not everything is zero).

Exercise. Prove this lemma.

Crucially, by the assumed reducibility of $f(1,y)$, $d \leq n-1$ and the above inequality is satisfied for large h, for example for $h = n^2$. With this choice of h, the existence of the polynomials A_i is proven.

Now, with such A_is, we set

$$P_\alpha(x,y) = \sum_{i=0}^{n-1} A_i(x) y^i \in \mathbb{Z}[x,y] \ .$$

We check that the polynomials P_α have the property stated at the beginning. Clearly, each P_α is nonzero and in y has degree less than n. If $x, y \in \mathbb{Z}$ satisfy $F(x,y) = 0$ and $|x|$ is large enough, then (by the second claim on $s_\alpha(t)$) we have $y = \varphi_\alpha(x)$ and $P_\alpha(x,y) = \Phi_\alpha(x)$ for some α. But if $|x|$ is large enough,

$$|P_\alpha(x,y)| = |\Phi_\alpha(x)| < 1 \ ,$$

because the expansion of $\Phi_\alpha(x)$ contains only powers of x with negative exponents and $\Phi_\alpha(x) \to 0$ if $|x| \to +\infty$. But, for $x, y \in \mathbb{Z}$, $P_\alpha(x,y) \in \mathbb{Z}$ and so $|P_\alpha(x,y)| < 1$ implies $P_\alpha(x,y) = 0$. This proves the remaining part of the property of the polynomials P_α. The theorem is proven. □

The previous proof is taken from Sprindžuk [3, pp. 11–13].

And what does original Runge's theorem say? We write

$$F(x,y) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_{i,j} x^i y^j, \ a_{i,j} \in \mathbb{Z} \ ,$$

and assume that $\deg_x F = m$, $\deg_y F = n$ with $m, n \geq 1$. We denote by ℓ the line $x/m + y/n = 1$, which goes through the points $(m,0)$ and $(0,n)$, and consider the two sets of lattice points

$$S = \{(i,j) \in \mathbb{Z}^2 \mid a_{i,j} \neq 0\} \ \text{ and } \ T = \{(i,j) \in S \mid (i,j) \in \ell\} \ .$$

We state Runge's theorem in the natural contrapositive form. (In the literature one can find many different formulations of Runge's theorem; sometimes under "Runge's theorem" goes only its particular case.)

Theorem (Runge, 1887). *Suppose that $F \in \mathbb{Z}[x,y]$ is as above, is irreducible in $\mathbb{Q}[x,y]$, and the equation*

$$F(x,y) = 0$$

has infinitely many solutions $x, y \in \mathbb{Z}$. Then

1. *no point of S lies above the line ℓ (hence $(m,0),(0,n) \in T$);*
2. *the ℓ-leading part of F satisfies*

$$\sum_{(i,j)\in T} a_{i,j} x^i y^j = a p^k \ ,$$

   where $0 \neq a \in \mathbb{Z}$, $k \in \mathbb{N}$ and $p = p(x,y) \in \mathbb{Z}[x,y]$ is an irreducible polynomial;
3. *$F(x,y) = 0$ with $x, y \in \mathbb{C}$ and x near ∞ determines an algebraic (multivalued) function whose all Puiseux expansions are pairwise conjugate.*

Equivalently, if an irreducible F violates one of the conditions 1–3, then $F(x,y) = 0$ has only finitely many integral solutions.

Exercise. Check that the initial theorem is indeed a particular case of Runge's theorem.

The disadvantage of Runge's theorem is that it does not apply to many important and natural equations, such as $x^3 - 2y^3 = a$, $a \in \mathbb{Z}$ (which has only finitely many solutions $x, y \in \mathbb{Z}$ too, as proven by A. Thue in 1909). The big advantage is effectivity, since Runge's method gives explicit upper bounds on the size of solutions.

Exercise. Convince yourself that the above proof provides an explicit upper bound on $\max(|x|,|y|)$ if $x, y \in \mathbb{Z}$ and $F(x,y) = 0$.

As for concrete explicit bounds, A. Grytczuk and A. Schinzel [1] proved, among other results, that, denoting $h = \max |a_{i,j}|$, if F is irreducible and

$a_{m,j} \neq 0$ for some $j > 0$ (i.e., $S \cap (x = m)$ has a point above ℓ), then any solution $x, y \in \mathbb{Z}$ of $F(x, y) = 0$ satisfies

$$|x| \leq \Big((m+1)(n+1)(mn+1)^{2/n}h\Big)^{2n(mn+1)^3}$$

and

$$|y| \leq \Big((m+1)(n+1)(mn+1)^{2/n}h\Big)^{2(mn+1)^3} .$$

Let $d = \max(m, n)$ (and again $h = \max|a_{i,j}|$). The results of P. G. Walsh in [4] and the correction [5] give the following general bound: if F is irreducible and violates one of the conditions 1–3 of Runge's theorem, then for $x, y \in \mathbb{Z}$ with $F(x, y) = 0$ one has

$$\max(|x|, |y|) < (2d)^{2d+18d^7} h^{12d^6} .$$

For fixed d these bounds are polynomial in the height h of F, which are very strong bounds indeed.

References

[1] A. Grytczuk and A. Schinzel, On Runge's theorem about Diophantine equations, in: G. Halász, L. Lovász, D. Miklós and T. Szönyi (editors), *Sets, Graphs and Numbers. A birthday salute to Vera T. Sós and András Hajnal,* Colloq. Math. Soc. J. Bolyai, 60, North-Holland, 1992, pp. 329–356.

[2] C. Runge, Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, J. reine und angew. Math. 100 (1887), 425–435.

[3] V. G. Sprindžuk, Klassičeskije diofantovy uravnenija ot dvux neizvestnyx, Nauka, Moskva, 1982.

[4] P. G. Walsh, A quantitative version of Runge's theorem on Diophantine equations, Acta Arithm. 62 (1992), 157–172.

[5] P. G. Walsh, Corrections to: "A quantitative version of Runge's theorem on Diophantine equations", Acta Arithm. 73 (1995), 397–398.