PONTIFICIA
ACADEMIA
SCIENTIARVM

COMMENTARII

Vol. II N. 20

A. SCHINZEL

AN IMPROVEMENT OF RUNGE'S THEOREM ON DIOPHANTINE EQUATIONS

EX ADIEBVS ACADEMICIS IN CIVITATE VATICANA

PONTIFICIA
ACADEMIA
SCIENTIARVM

COMMENTARII
Vol. II - N. 20
pag. 1-12

AN IMPROVEMENT OF RUNGE'S THEOREM ON DIOPHANTINE EQUATIONS

A. SCHINZEL

SVMMARIVM — Auctor investigat quando aequatio cum duabus variabilibus infinitum solutionum integralium numerum habere possit.

I

The first general result concerning the number of integer solutions of a diophantine equation is due to RUNGE [3] and in its simplest form is as follows.

(i) If $f(x, y)$ is a polynomial with integer coefficients irreducible in the rational field and the equation $f(x, y) = 0$ has infinitely many integer solutions, then the highest homogeneous part of $f(x, y)$ is up to a constant factor a power of an irreducible form.

The more general formulation refers to the highest isobaric part of $f(x, y)$.

Paper presented on October 17th, 1968 by Pontifical Academician H.E. WACLAW SIERPINSKI.

The final result permitting to decide whether any given equation $f(x, y)=0$ has infinitely many integer solutions is due to SIEGEL [4] and is as follows.

(ii) If $f(x, y)=0$ has infinitely many integer solutions, then there exist rational functions $R(t)$, $S(t)$ not both constant such that

$$f(R(t), S(t))=0 \tag{1}$$

identically in t and either

$$R(t)=\frac{A(t)}{L(t)^m}, \quad S(t)=\frac{B(t)}{L(t)^m} \tag{2}$$

or

$$R(t)=\frac{C(t)}{Q(t)^m}, \quad S(t)=\frac{D(t)}{Q(t)^m}, \tag{3}$$

where A, B, C, D, L, Q are polynomials with integer coefficients, L is linear, Q irreducible indefinite quadratic.

The aim of this note is to deduce from the two above results the following improvement of the first one.

Theorem. If $f(x, y)$ is a polynomial with integer coefficients irreducible in the rational field and the equation $f(x, y)=0$ has infinitely many integer solutions then the highest homogeneous part of $f(x, y)$ is up to a constant factor a power of a linear or irreducible indefinite quadratic form.

Prof. Lef $f(x, y)$ have degree n and denote by $f_n(x, y)$ its highest homogeneous part. By (i) either $f_n(x, y)=a\,x^n$ or $f_n(x, y)=b\,y^n$ or

$$f_n(x, y)=a\,x^n+\ldots+b\,y^n \qquad (ab\neq 0). \tag{4}$$

It remains to consider the last case. By (ii) we have (1) where either

1. R, S are polynomials not both constant or
2. (2) holds with $m>0$, $(A,B,L)=1$ or
3. (3) holds with $m>0$, $(C,D,Q)=1$.

In the case 1. it follows from (1) and (4) that R and S are of the same degree. Denoting this degree by d and the leading coefficients of R and S by r and s, respectively, we get

$$f_n(r, s) = \lim_{t=\infty} t^{-nd} f\left(R(t), S(t)\right) = 0 .$$

Hence $f_n(x, y)$ is divisible by $s x - r y$ and by (i)

$$f_n(x, y) = c\,(s x - r y)^n .$$

In the case 2. let t_o be the zero of $L(t)$. Clearly $A(t_o)\neq 0$ or $B(t_o)\neq 0$. Multiplying (1) by $L(t)^{mn}$ and substituting afterwards $t=t_o$ we obtain

$$f_n\left(A(t_o),\ B(t_o)\right) = 0 .$$

Hence $f_n(x, y)$ is divisible by $B(t_o)\,x - A(t_o)\,y$ and by (i)

$$f_n(x, y) = c\,\left(B(t_o)\,x - A(t_o)\,y\right)^n .$$

In the case 3. let t_1, t_2 be the zeros of $Q(t)$. Clearly

$$C(t_i)\neq 0 \text{ or } D(t_i)\neq 0 \qquad (i=1,2) .$$

Multiplying (1) by $Q(t)^{mn}$ and substituting afterwards $t=t_i$ we obtain

$$f_n\left(C(t_i),\ D(t_i)\right) = 0 \qquad (i=1,2) .$$

Hence $f_n(x, y)$ is divisible by $D(t_i)\,x - C(t_i)\,y$ and by (4) $D(t_i) \neq 0$ $(i=1,2)$. If $C(t_1)\,D(t_1)^{-1}$ is rational then by (i)

$$f_n(x, y) = c\,\bigl(D(t_1)\;x - C(t_1)\;y\bigr)^n\,.$$

If $C(t_1)\,D(t_1)^{-1}$ is irrational, the $C(t_i)\,D(t_i)^{-1}$ are conjugate in a real quadratic field and by (1)

$$f_n(x, y) = c\,\bigl[\bigl(D(t_1)\,x - C(t_1)\,y\bigr)\,\bigl(D(t_2)\,\mathrm{x} - C(t_2)\,y\bigr)\bigr]^{n/2}\,.$$

Corollary. If $f_n(x, y)$ is an irreducible form of degree $n>2$ and $g(x, y)$ is a polynomial with integer coefficients of degree $m<n$ then the equation

$$f_n(x, y) = g(x, y)$$

has only finitely many integer solutions.

The corollary represents an improvement on the analogous results which ROTH [2] deduced from his famous theorem; this had stronger hypothesis $m<n-2$.

I conclude by expressing my thanks to Professors H. DAVENPORT and D.J. LEWIS for their helpful suggestion and in particular for pointing out the corollary.

II

In this second part I wish to extend the result of the first part so as to improve on Runge's theorem in its full generality.

Let $f(x, y)$ be a polynomial with integer coefficients irreducible in the rational field and suppose that the equation $f(x, y) = 0$ has infinitely many integer solutions. Then according to RUNGE [3] (see [6], p. 89):

(1) the highest terms in x and y occur in f separately as ax^m, by^n;

(2) each branch of the algebraic function y of x defined by $f = 0$ tends to infinity with x and is of order $x^{m/n}$, every term $cx^\rho\, y^\sigma$ in f has $n\rho + m\sigma \leq mn$;

(3) the sum $g(x, y)$ of the terms with $n\rho + m\sigma = mn$ is expressible as

$$b \prod_{\beta} (y^\nu - d^{(\beta)}\, x^\mu) \qquad \left(\beta = 1, \ldots, \frac{n}{\nu}\right),$$

where $\prod\limits_{\beta} (u\text{-}d^{(\beta)})$ is a power of an irreducible polynomial.

RUNGE does not say explicitly that

$$\frac{n}{\nu} = \frac{m}{\mu} = (m, n),$$

but what he really proves is that $g(x, y)$ is a power of an irreducible polynomial (for another proof see SKOLEM [5]).

Therefore, factorizing if necessary $y^{\nu} - d^{(\beta)} x^{\mu}$ we can conclude that

$$(4) \qquad g\,(x,\,y) = b\;\;h\,(x^{m/d},\;y^{n/d})^{\lambda}, \qquad d = (m,\,n),$$

where $h\,(u,\,v)$ is an irreducible form. We shall prove:

Theorem. If $f\,(x,\,y)$ is a polynomial with integer coefficients irreducible in the rational field, of degree m in x and n in y, and the equation $f\,(x,\,y) = 0$ has infinitely many integer solutions then (1) and (2) hold and the sum $g\,(x,\,y)$ of all terms $cx^{\rho}\,y^{\sigma}$ of f with $n\rho + m\sigma = mn$ is of the form $bh(x^{m/d}, y^{n/d})^{\lambda}$, where $d = (m,\,n)$ and h is a linear or irreducible indefinite quadratic form.

The proof is based on the theorem of SIEGEL [4] quoted in part I, it will be however a little simpler if we reformulate the said theorem, examining Siegel's argument. SIEGEL proves that if $f\,(x,\,y) = 0$ has infinitely many integer solutions then the genus of $f\,(x,\,y) = 0$ is zero (*). In this case (cf. SKOLEM [6] p. 102) there is a parametrization

$$(5) \qquad x = \frac{\varphi\;(u,\,v)}{\chi\;(u,\,v)}, \qquad y = \frac{\Psi\;(u,\,v)}{\chi\;(u,\,v)},$$

where φ, Ψ, χ are relatively prime forms of the same positive degree with rational coefficients and where the equation

$$\chi\;(u,\,v) = h$$

has infinitely many integer solutions for some $h \neq 0$. Now, as proved by MAILLET [1] (cf. [6] p. 100) the last condition implies that

(*) The assumptions imply the absolute irreducibility of f, hence the genus is defined.

$$(6) \quad \chi\,(u,v)=c_1(a_1+b_1v)^l \text{ or } \chi\,(u,v)=d_1\,(a_2u^2+b_2uv+c_2v^2)^l,$$

where $b_2^2-4a_2c_2$ is positive and is not a perfect square. The latter case by the substitution $u=t$, $v=1$ leads to a parametrization

$$(7) \qquad x(t)=\frac{C\,(t)}{Q\,(t)^\alpha}, \quad y\,(t)=\frac{D\,(t)}{Q\,(t)^\beta}, \qquad f\,(x\,(t),\,y\,(t))=0,$$

where C, D, Q are polynomials with rational coefficients, Q is irreducible indefinite quadratic, $\alpha \geqslant 0$, $\beta \geqslant 0$ and $x\,(t)$, $y\,(t)$ are not both constant.

Moreover, and this remark of MAILLET seems to have been so far overlooked, the former case leads to the same parametrization (7) with $\alpha=\beta=0$. Indeed on substituting $u=t$, $v=b_1^{-1}\,(1-a_1\,t)$ we get from (5) and (6)

$$x\,(t)=\frac{\varphi\,(t,\,b_1^{-1}\,(1-a_1\,t))}{c_1}, \quad y\,(t)=\frac{\Psi\,(t,\,b_1^{-1}\,(1-a_1\,t))}{c_1}$$

and the polynomials on the right hand side which are not both constant can be taken as C (t), B (t) in (7). Therefore, if $f\,(x,\,y)=0$ has infinitely many integer solutions then (7) holds and either

$$(8) \qquad \alpha=\beta=0, \quad C,\,D \quad \text{are not both constant}$$

or

$$(9) \qquad \alpha+\beta>0, \qquad (C, Q^{\alpha})=(D, Q^{\beta})=1 .$$

Proof of the theorem. By Runge's theorem we have (1), (2) and (4) and it remains to show that h is linear or indefinite quadratic. Set $m/d=\mu$, $n/d=\nu$.

In the case (8) let γ, δ be the degrees of C, D respectively and c_o, d_o their leading coefficients. If t tends to infinity then x is of order t^{γ}, y of order t^{δ} and by (2) $\delta=\gamma\, m/n$. Thus we get from (7)

$$g\,(c_o, d_o)=\lim_{t=\infty} t^{-\gamma m}\, f\bigl(x\,(t),\ y\,(t)\bigr)=0\ ,$$

from (4)

$$h\,(c^{\mu}{}_o, d^{\nu}{}_o) = 0$$

and $h\,(u, v)$ is divisible by $d^{\nu}{}_o u - c^{\mu}{}_o v$. Since h is irreducible it must be linear.

In the case (9) let t_1, t_2 be the zeros of $Q\,(t)$. If t tends to t_i then x is of order $(t_i-t_i)^{-\alpha}$ (possibly tend, to 0 if $\alpha=C\,(t_i)=0$), y of order $(t-t_i)^{-\beta}$ (possibly tends to 0 if $\beta=D\,(t_i)=0$) and by (2) $\beta=\alpha\, m/n$, $C\,(t_i)\neq 0\neq D\,(t_i)$ $(i=1, 2)$. Thus we get from (7)

$$g\bigl(C\,(t_i),\ D\,(t_i)\bigr) = \lim_{t=t_i} Q\,(t)^{\alpha m}\, f\bigl(x\,(t),\ y\,(t)\bigr)=0\ ,$$

from (4)

$$h\bigl(C\,(t_i)^{\mu},\ D\,(t_i)^{\nu}\bigr)=0$$

and $h\,(u, v)$ is divisible by $D\,(t_i)^{\nu}\, u - C\,(t_i)^{\mu}\, v$ $(i=1,2)$.

If C $(t_1)^{-\mu}$ D $(t_1)^{\nu}$ is rational h must be linear as before.

If C $(t_1)^{-\mu}$ D $(t_1)^{\nu}$ is irrational then C $(t_i)^{-\mu}$ D $(t_i)^{\nu}$ are conjugate in a real quadratic field, h is divisible by

$$\left(\mathrm{D}\ (t_1)^{\nu}\ u - \mathrm{C}\ (t_1)^{\mu}\ v\right)\left(\mathrm{D}\ (t_2)^{\nu}\ u - \mathrm{C}\ (t_2)^{\mu}\ v\right)$$

and h is indefinite quadratic. This completes the proof.

It should be noted that the above proof does not share an essential advantage of Runge's proof, namely it does not permit to estimate the size of solutions of $f\ (x,\ y) = 0$ if the theorem implies the finiteness of their number. The reason for this defect is the noneffective character of Siegel's theorem.

REFERENCES

[1] E. Maillet, *Détermination des points entiers des courbes algébriques unicursales à coefficients entiers*, « C.R. Acad. Sci. », Paris, *168*, 217-220 (1919).

[2] K.F. Roth, *Rational approximations to algebraic numbers*, « Mathematika », *2*, 1-20 (1955).

[3] C. Runge, *Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen*, « J. Reine Angew. Math. », *100*, 425-435 (1887).

[4] C.L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, « Abh. preuss. Akad. Wiss., Phys.-math. Kl. », Nr. 1 (1929).

[5] Th. Skolem, *Über ganzzahlige Lösungen einer Klasse unbestimmter Gleichungen*, « Norsk Mat. Foren. Skrifter » (I), Nr. 10 (1922).

[6] — *Diophantische Gleichungen*, Berlin (1938).