Reports of the Academy of Sciences of the USSR

1961

SovietRxiv

Abstract

Full Text

Reports of the Academy of Sciences of the USSR

1961. Volume 139, No. 4

MATHEMATICS

Yu. I. Manin

ON DIOPHANTINE EQUATIONS OVER FUNCTION FIELDS

(Presented by Academician I. M. Vinogradov on 16 III 1961)

1. The well-known Siegel–Mahler theorem ([1–3]) asserts that on any curve of genus $\geqslant 1$, defined over a finite extension k of the field of rational numbers, there lie only finitely many points whose coordinates belong to the field k and have in their denominators only prime divisors of the field k from a given finite set. This theorem, as well as the stronger, but still unproved Mordell conjecture ([4]) on the finiteness of the number of points rational over the field k on a curve of genus $\geqslant 2$, admits transfer to the case of a function field of constants. Lang ([3]) made several general remarks on this subject and showed that the method of proof belonging to Siegel and Mahler also extends to the function-field case; in doing so, of course, one must essentially rely on the functional analogue of the Thue–Siegel–Roth approximation theorem.

In the present note the author sets himself the goal of showing that in the function-field case the Siegel–Mahler theorem, as well as the Mordell conjecture for a certain class of curves of genus $\geqslant 2$, can be obtained by means of entirely different principles, whose numerical analogue is unknown. A first, fairly general, though incomplete exposition of them was given in the author' s paper ([5]), but without any applications. We shall illustrate here the application of the constructions of ([5]) to Diophantine problems by the example of elliptic curves. The general case the author intends to treat later. Below a sketch will be given of the proof of the following two theorems.

Let k be an algebraically closed field of characteristic zero; K the field of functions of one variable over the field of constants k; L a function field of genus one over the field of constants K; $\mathfrak{S}$ the set of prime divisors (points), and $\mathfrak{S}_K$ the set of prime divisors of degree one of the field L/K; $\mathfrak{h}$ the set of prime divisors of the field K/k. We denote elements of the set $\mathfrak{S}$ by the letters $\mathfrak{P}, \mathfrak{Q}, \mathfrak{R}$ with indices; elements of the set $\mathfrak{h}$ by the letters $\mathfrak{p}, \mathfrak{q}$. For any element $v \in L$, the symbol $v_{\mathfrak{P}}$ denotes the value of the function v at the point $\mathfrak{P}$; the symbol $v_{\mathfrak{P}}(v)$

denotes the order of the function v at the point $\mathfrak{P}$; the symbols (v), $(v)_0$, $(v)_\infty$ denote, respectively, the divisor, the divisor of zeros, and the divisor of poles of the function v. Completely analogous notation will be applied to elements of the field K/k and their divisors; confusion can arise only if an element $a \in K$ is regarded by us as a constant of the field L/K, but the precise meaning will each time be clear from the context. Finally, we shall assume that there does not exist a field L_1 of genus one over the field of constants k such that $L\widetilde{K} = L_1\widetilde{K}$ for some extension $\widetilde{K}$ of the field of constants K.

Theorem 1. *Let $v \in L$ be any nonconstant function of the field L, and let $S \subset \mathfrak{h}$ be any finite set of points of the field K/k. There exists only a finite set of points $\mathfrak{Q} \in \mathfrak{S}_K$ for which the divisor $(v_\mathfrak{Q})_0$ consists only of points of the set S.*

Theorem 2. *Let $v \in L$ be any nonconstant function of the field L, having no multiple zeros; let $m \geqslant 3$ be any integer. Then the field $L(v^{1/m})$ has only a finite number of prime divisors of degree one over the field of constants K.*

For simplicity we have formulated Theorem 2 not in its strongest form, even for the elliptic case. Its meaning is that a sufficiently strongly ramified covering of an elliptic curve over a function field satisfies Mordell' s hypothesis.

2. Let us first recall known facts from the theory of distributions of A. Weil. One considers the set of functions defined at all, except perhaps finitely many, prime divisors in $\mathfrak{S}$, and taking values in the group of divisors of the field K/k. Two such functions f, g are called equivalent on some infinite subset of their domains of definition if both ratios $f^{-1}g$ and fg^{-1} (where they are defined) divide some fixed divisor of the field K/k; we then write $f \sim g$. A. Weil effectively defines a class of such functions corresponding one-to-one to divisors $\mathfrak{A}$ of the field L. Namely, the function $\mathfrak{A}(\mathfrak{D})$ is equal to

$$\prod_i \mathfrak{p}_i(\mathfrak{D})^{a_i}, \quad \text{if} \quad \mathfrak{A} = \prod_i \mathfrak{P}_i^{a_i},$$

and the system of functions $\mathfrak{P}(\mathfrak{D})$, for all $\mathfrak{P} \in \mathfrak{S}$, has the following properties: a) the function $\mathfrak{P}(\mathfrak{D})$ is equivalent to an integral-valued function and is defined everywhere except $\mathfrak{D} = \mathfrak{P}$; b) if $\mathfrak{P}_1 \neq \mathfrak{P}_2$, then $\gcd(\mathfrak{P}_1(\mathfrak{D}), \mathfrak{P}_2(\mathfrak{D})) \sim 1$; c) for any element $v \in L$ the functions $(v_\mathfrak{D})$ and $(v)(\mathfrak{D})$ are equivalent.

For any set S of prime divisors of the field K/k and any divisor

$$\mathfrak{a} = \prod \mathfrak{p}_i^{a_i} \quad \text{put} \quad \mathfrak{a}_S = \prod_{\mathfrak{p}_i \in S} \mathfrak{p}_i^{a_i}, \quad \mathfrak{a}_{\bar{S}} = \mathfrak{a}\,\mathfrak{a}_S^{-1}.$$

Then from properties a), b), c) it follows that, for any pair of points $\mathfrak{P}_1 \neq \mathfrak{P}_2$, there exists such a finite set S of points of the field K that $\gcd(\mathfrak{P}_1(\mathfrak{D}), \mathfrak{P}_2(\mathfrak{D}))_{\bar{S}} = 1$; moreover, obviously, the degrees of the prime divisors occurring in $\gcd(\mathfrak{P}_1(\mathfrak{D}), \mathfrak{P}_2(\mathfrak{D}))$ are bounded.

3. The proofs of Theorems 1 and 2 will be carried out according to a common scheme. The letter v will always denote the function appearing in the hypothesis of the theorem being proved.

Suppose this theorem is false; then there exists an infinite sequence $\{\mathfrak{D}_i\}$ of points of $\mathfrak{S}_K$ such that either $(v_{\mathfrak{D}_i})_0 = (v_{\mathfrak{D}_i})_{0S}$, or the divisor $(v_{\mathfrak{D}_i})_0$ is an m-th power, $m \geqslant 3$. From the supposition made regarding the field L it follows that the heights of the points $\mathfrak{D}_i$ increase without bound, i.e. the degrees of the divisors $(v_{\mathfrak{D}_i})_0$ increase (cf. (3)). But $(v_{\mathfrak{D}_i})_0 \sim (v)_0(\mathfrak{D}_i)$. Hence it follows that, if Theorem 1 is false, then there exists a prime divisor $\mathfrak{D} \in \mathfrak{S}$ and a point $\mathfrak{p} \in S$ such that $v_{\mathfrak{D}} = 0$ and $v_{\mathfrak{p}}(\mathfrak{D}(\mathfrak{D}_i)) \to \infty$; if, however, Theorem 2 is false, then for any finite set S of divisors of the field K/k the degrees of at least one of the sequences of divisors $\mathfrak{D}(\mathfrak{D}_i)_S$ and $\mathfrak{D}(\mathfrak{D}_i)_{\bar{S}}$ increase without bound, moreover $\mathfrak{D}(\mathfrak{D}_i)_{\bar{S}} = \mathfrak{A}_i^m$.

Extending, if necessary, the field K, we may assume that $\mathfrak{D} \in \mathfrak{S}_K$. We choose the point $\mathfrak{D}$ as the zero of the group law on the set $\mathfrak{S}_K$, which we define in the usual way, by putting $\mathfrak{P}_1 + \mathfrak{P}_2 = \mathfrak{P}_3$ if the divisor

$$\frac{\mathfrak{P}_1\mathfrak{P}_2}{\mathfrak{D}\mathfrak{P}_3}$$

is principal.

4. Main lemma. *Let $t \in K$ be any nonconstant element; let ∂ be the unique derivation of the field K/k for which $\partial t = 1$; let ∂_v be the unique extension of the derivation ∂ to the field L/k satisfying the equality $\partial_v v = 0$. Let also $\omega = u\,dv$ be a differential of the first kind of the field L/K.*

Then: a) there exist elements $a, b \in K$ and $w \in L$ such that $(\partial_v^2 u + a\partial_v u + bu)\,dv = dw$; b) the mapping $\mu : \mathfrak{S}_K \to K$, defined for all,

except for a finite number, of points $\Omega \in \mathfrak{S}_K$ by the formula

$$\mu(\Omega) = w_\Omega - w_{\mathfrak{D}} + au_\Omega \partial v_\Omega + (\partial vu)_\Omega dv_\Omega + \partial(u_\Omega dv_\Omega), \tag{1}$$

can be uniquely extended so that it becomes a homomorphism of the group $\mathfrak{S}_K$ into the additive group of the field K. The kernel of this homomorphism consists only of points of finite order.

Let us note that heuristically

$$\mu(\Omega) = (\partial^2 + a\partial + b) \int_{\mathfrak{D}}^{\Omega} u\,dv;$$

moreover, the image of the homomorphism μ, by the Mordell–Weil–Néron theorem, is a finitely generated lattice in K and therefore consists of elements of the field K/k of bounded degree.

The basic ideas of the proof of this assertion (for a curve of arbitrary genus) are contained in the paper ([5]).

5. We shall show that if Theorem 1 or Theorem 2 is false, then the totality $\{\mu(\Omega_i)\}$ will contain functions with zeros of arbitrarily high order or with an arbitrarily large number of zeros. Obviously, this contradicts the remark just made.

First of all, let us observe that in formula (1) one may put $w_{\mathfrak{D}} = 0$. Indeed, it follows from it that $w_{\mathfrak{D}} \neq \infty$, and then instead of the function w one may take $w - w_{\mathfrak{D}}$.

Suppose Theorem 1 is false; then, as in § 2, $v_{\mathfrak{p}}(\mathfrak{D}(\Omega_i)) \to \infty$ for some point $\mathfrak{p} \in S$ and some sequence of points $\{\Omega_i\}$. From the results of the theory of distributions cited in § 2 it follows that for any element $x \in L$ there exists a constant $c \geq 0$ such that

$$\left| v_{\mathfrak{p}}(x_{\Omega_i}) - v_{\mathfrak{D}}(x) v_{\mathfrak{p}}(\mathfrak{D}(\Omega_i)) \right| \leq c. \tag{2}$$

We shall apply this inequality to the functions $u, v, w, \partial v u$, noting that

$$v_{\mathfrak{D}}(\partial v u) \geq v_{\mathfrak{D}}(u) = v_{\mathfrak{D}}\left(\frac{\omega}{dv}\right) \geq -v_{\mathfrak{D}}(dv) = 1 - v_{\mathfrak{D}}(v). \tag{3}$$

Finally, putting $e = v_{\mathfrak{p}}(dt) + 1$, let us note that for any element $g \in K$ the inequality

$$v_{\mathfrak{p}}(\partial g) \geq v_{\mathfrak{p}}(g) - e \tag{4}$$

is valid.

Combining the inequalities (2), (3), (4), we obtain

$$v_{\mathfrak{p}}(a u_{\Omega_i} \partial v_{\Omega_i}) \geq v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(\mathfrak{D}(\Omega_i)) - c - e \to \infty,$$

$$v_{\mathfrak{p}}((\partial v u)_{\Omega_i} dv_{\Omega_i}) \geq v_{\mathfrak{p}}(\mathfrak{D}(\Omega_i)) - c - e \to \infty,$$

$$v_{\mathfrak{p}}(\partial(u_{\Omega_i} dv_{\Omega_i})) \geq v_{\mathfrak{p}}(\mathfrak{D}(\Omega_i)) - c - 2e \to \infty.$$

Finally, since $w_{\mathfrak{D}} = 0$, also $v_{\mathfrak{p}}(w_{\Omega_i}) \to \infty$. As was said, this gives $v_{\mathfrak{p}}(\mu(\Omega_i)) \to \infty$ and leads to a contradiction.

Suppose now that Theorem 2 is false. From what has just been proved it follows that, in the notation of § 2, the degrees of the divisors $\mathfrak{D}(\Omega_i)_S$ are bounded, and hence the degrees of the divisors $\mathfrak{D}(\Omega_i)_{\overline{S}}$ increase, whatever the finite set S of

points of the field K/k may be. In this set we shall include all divisors of the denominator of the coefficient a and all divisors $\mathfrak{p}$ for which there exists a point Ω_i with $v_\mathfrak{p}(\mathfrak{D}(\Omega_i)) \neq 0$, and in the inequality (2) with $x = u, v, w, \partial_{vu}$ the constant c cannot be put equal to zero. The finiteness of such a set S follows from the results of § 2. Finally, include in S all $\mathfrak{p}$ for which $v_\mathfrak{p}(dt) \neq 0$, i.e. $e \neq 1$.

Suppose $v_\mathfrak{p}(\mathfrak{D}(\Omega_i)) \neq 0$; then $v_\mathfrak{p}(\mathfrak{D}(\Omega_i)) \geq m \geq 3$, and for $\mathfrak{p} \notin S$ the following estimates hold:

$$v_\mathfrak{p}(w_{\Omega_i}) = v_\mathfrak{D}(w)\, v_\mathfrak{p}(\mathfrak{D}(\Omega_i)) \geq m,$$

$$v_\mathfrak{p}(a u_{\Omega_i}\, \partial v_{\Omega_i}) \geq v_\mathfrak{p}(\mathfrak{D}(\Omega_i)) - 1 \geq m - 1,$$

$$v_\mathfrak{p}((\partial u)_{\Omega_i} \partial v_{\Omega_i}) \geq v_\mathfrak{p}(\mathfrak{D}(\Omega_i)) - 1 \geq m - 1,$$

$$v_\mathfrak{p}(\partial(u_{\Omega_i} \partial v_{\Omega_i})) \geq v_\mathfrak{p}(\mathfrak{D}(\Omega_i)) - 2 \geq m - 2.$$

It follows from these, obviously, that the degrees of the divisors $(\mu(\Omega_i))_{0\bar{S}}$ increase without bound, and this again gives the required contradiction.

6. In order to show in the proper light the meaning of the main construction of the lemma, we shall indicate a general result of this type. Let K be a regular extension of an algebraically closed field k of characteristic zero. Then one can construct an algebraic-differential homomorphism of the group A_K of points rational over K of an abelian variety A, defined over the field K, into a direct sum of a finite number of additive groups of this field. Denote by the symbol (B, τ) the K/k-trace of the variety A. The kernel of the homomorphism just mentioned necessarily contains the subgroup generated by all points of finite order and by the points of the subgroup τB_k. The author conjectures that this kernel is thereby exhausted, although he has an (analytic) proof of this fact only in the case when the degenerate specializations over the field k of the variety A have the simplest form. (Cf. ([5]), where essentially the case of the Jacobian of a variety over a one-dimensional field of constants is analyzed in sufficient detail.) This result, together with the fact of uniform continuity of the homomorphism under consideration with respect to the topologies of the groups A_K and K generated by the discrete valuations of the field K, plays the main role in applications to Diophantine analysis, as the author hoped to show in the example discussed.

V. A. Steklov Mathematical InstituteAcademy of Sciences of the USSR

Received9 III 1961

REFERENCES

1. C. L. Siegel, Abh. Preuss. Akad. Wiss., Phys.-Mat. Kl., **1**, 41 (1929).

2. K. Mahler, J. f. reine u. angew. Math., **170**, 168 (1934).

3. W. D. Lang, Inst. des Hautes Études Sci., Publ. Math., **6**, 27 (1960).

4. L. J. Mordell, Proc. Cambr. Phil. Soc., **21**, 179 (1922).

5. Yu. I. Manin, Izv. AN SSSR, ser. matem., **22**, 737 (1958).

Note: Figure translations are in progress. See original paper for figures.