RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

U. ZANNIER

An effective solution of a certain diophantine problem

Rendiconti del Seminario Matematico della Università di Padova, tome 93 (1995), p. 177-183

<http://www.numdam.org/item?id=RSMUP_1995__93__177_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 93 (1995)

An Effective Solution of a Certain Diophantine Problem.

U. ZANNIER (*)

Introduction.

Consider the following diophantine question:

Let $f(X, Y) \in K[X, Y]$, where K is a number field with ring of integers D. Determine the set $S = S_f = S_{f,K} = \{m \in D: f(m, Y)$ splits into linear factors over $K\}$.

A celebrated theorem of Siegel immediately implies that, if the splitting field Σ of f over $K(X)$ has positive genus, then S is finite. Actually, even if no effective version of the general Siegel's theorem is known at present, it follows from work of Belotserkovski [3] that one can effectively determine S (which is essentially equivalent to an effective Siegel's theorem on the integral points of a Galois covering of the projective line. See also the Appendix in [5] for a proof). The purpose of this brief note is to complete such analysis with an effective description of S in the easier case when Σ has genus zero. We remark that Siegel himself gave a good description of the integral points for the general equation of genus zero, which moreover can now be made effective. Nevertheless some additional information, compared to the general case, is gained by looking at the above question.

We may clearly assume f to be irreducible over K. Let $d^* = \deg_Y f$. Define $\tilde{K}$ as the algebraic closure of K in Σ, G as the Galois group of Σ over $\tilde{K}(X)$ and let d be the order of G. We shall prove the following

(*) Indirizzo dell'A.: D.S.T.R., S. Croce 191, 30135 Venezia (Italy).
E-mail: zannier@udmi5400.cineca.it.

THEOREM. *Assume that Σ has genus zero. Then one may determine whether S is finite (in which case its elements may be found), or not. If not, then $\tilde{K} = K$, and G is cyclic or dihedral according as X has one or two poles in Σ. In the first case K contains a primitive d-th root of unity. Otherwise a primitive $(d/2)$-th root of 1 is either in K or quadratic over K. Moreover there are computable explicit parametric formulae for the elements of S (given by (5), (8), (11) below).*

In the proof we shall use the fact that, given a curve C defined over K, of genus 0, it is effectively possible to establish whether there exists a K-rational point [1] on it (by Hasse principle for instance) and, in the affirmative case, to produce one such point. Even if this is well known, for the sake of completeness we recall very briefly one possible method. For α a divisor, let $V(\alpha)$ be the vector space of rational functions f such that $\operatorname{div}(f) \geq \alpha$. The divisor δ of a nonzero K-rational differential on the curve is of degree -2, so, by Riemann-Roch, $V(\delta)$ has dimension 3. Let $\langle f, g, h\rangle$ be a basis for $V(\delta)$ (Coates algorithm—see [4]—guarantees the effectivity of such procedure). Then the functions $f^2, fg, fh, g^2, gh, h^2$ lie in $V(2\delta)$ which, by Riemann-Roch again, has dimension 5. A nontrivial linear relation among such six functions gives a model for C as a conic in $\boldsymbol{P}^2$ which, after a change of variables, may be assumed to be of the form $Y^2 - aX^2 = cZ^2$ where $a, c \in K^*$ [2]. Rational points thus give nontrivial solutions in D of such equation and exist iff c is a relative norm from $K(\sqrt{a})$ to K. (We may exclude the trivial case $a \in K^{*2}$.)

Take any nontrivial solution $(X, Y, Z) \in D^3$. It is easy to see (using the finiteness of the class number) that the greatest common ideal divisor of X, Y may be assumed to divide a fixed ideal.

Consider then the ideal factorization of $Y + X\sqrt{a}$ in the ring of integers of $K(\sqrt{a})$. By the above remark $(Y + X\sqrt{a}) = IJ^2$ where I is an ideal in a finite set depending on c. Choose an ideal J^* in the class of J and having bounded absolute norm. Then, set $(Y^* + X^*\sqrt{a}) = IJ^{*2}$, $(t) = J^{-1}J^*$. We have that IJ^{*2} has bounded absolute norm, whence Y^*, X^* may be chosen to have bounded height, while $t \in K(\sqrt{a})$. Also, $(Y + X\sqrt{a})(t^2) = (Y^* + X^*\sqrt{a})$ as fractional ideals, whence $Y^* + X^*\sqrt{a} = \mu t^{*2}(Y + X\sqrt{a})$ where μ is a unit from a finite set (in fact, the group of units is finitely generated, and the squares of units may be absorbed in t^{*2}). Taking norms N from $K(\sqrt{a})$ to K we get $N((Y^* + X^*\sqrt{a})/\mu) = cU^2$, where $U = ZN(t^*) \in K$. Since Y^*, X^*, μ have

[1] Here and in the sequel by *point* on a curve we mean a point on the nonsingular model of it.

[2] This result goes back to Hurwitz.

bounded height, both $(Y^* + X^*\sqrt{a})/\mu$ and U have bounded height too, whence our original equation has solutions whose height may be explicitly bounded, proving the above contention.

Having possibly found such a K-rational point P we may take (after Coates algorithm) a nonconstant function t in $V(-P)$. Then the function field $K(C)$ equals $K(t)$ and we may effectively write any given function $f \in K(C)$ in the form $a(t)$, $a \in K(t)$.

PROOF OF THEOREM. We first show, by means of a familiar trick that, if $\tilde{K} \neq K$, then S is finite and computable.

Let z be a primitive element for Σ over $K(X)$ of the form $z = c_1 y_1 + \ldots + c_{d^*} y_{d^*}$ (where $c_i \in K^*$ and the y_i are the roots of $f(X, Y) = 0$) and let $H(X, Z) = 0$ be a minimal equation over $K(X)$, irreducible over $K[X]$. Since the conjugates of z over $K(X)$ are linear forms in $y_1, \ldots, y_{d^*}$ with coefficients in K, we see that, if $m \in S_f$ then $H(m, Z)$ splits into linear factors over K. Now it is well known that $\tilde{K} \neq K$ if and only if $H(X, Z)$ is not absolutely irreducible. Assume this is the case, let $L(X, Z)$ be an absolutely irreducible factor with algebraic coefficients, and write

$$L(X, Z) = t_1 L_1(X, Z) + \ldots + t_s L_s(X, Z) \tag{1}$$

where the t_i are algebraic numbers linearly independent over K while $L_i \in K[X, Z]$ for all i.

If the L_i have a common factor Q, this divides L, whence $L = \mu Q$ for some algebraic number μ. Also, we may clearly assume $Q \in K[X, Z]$, so, since Q divides H, which is irreducible over K, we would have $H = \nu L$ for some algebraic number ν and H would be absolutely irreducible.

So the polynomials L_i are coprime, whence an equation

$$B_1(X, Z)L_1(X, Z) + \ldots B_s(X, Z)L_s(X, Z) = C(X) \tag{2}$$

where $B_i \in K[X, Z]$ for all i while C is a nonzero polynomial with coefficients in K.

Now, if $m \in K$ and the equation $L(m, Z) = 0$ has a solution $\zeta \in K$, then, in view of (1) and the independence of the t_i over K we have $L_i(m, \zeta) = 0$ for all i, so, from (2), $C(m) = 0$. Since C is computable the proof of the above contention is completed, i.e. we may assume that K is algebraically closed in Σ.

According to the remarks before the proof, either Σ has no rational nonsingular points, whence S is finite and computable (as a subset of the singular set of the plane curve determined by the minimal polyno-

mial for a primitive element z as above), or we may compute a parametrization

$$X = a(t), \qquad a \in K(t) \tag{3}$$

where $\Sigma = K(t)$.

Also, there are parametrizations $y_i = b_i(t)$, where $b_i \in K(t)$, $i = 1, \ldots, d^*$. Since $K(X, y_1, \ldots, y_{d^*}) = \Sigma = K(t)$, we have a relation

$$t = R(a(t), b_1(t), \ldots, b_{d^*}(t)) \tag{4}$$

where R is a rational function in its arguments with coefficients in K. In particular this shows that if the values of X and the y_i are defined at t_0, then they all lie in K if and only if $t_0 \in K$.

If the rational function a has at least three distinct poles then, as explained in [6], Ch. 8, § 5, values of t in K such that $X \in D$ lead to a finite number of (computable) Thue equations to be solved in D, so, by Baker's results (see [1], Ch. 4, Thm. 4.1), there are finitely many solutions which can be found.

So, assume that a has at most two distinct poles.

The Galois group G has clearly a realization as a finite group of linear fractional transformations on t. (The structure of such groups is well known: G may be either cyclic, dihedral or one of three sporadic groups. See [2] for details.) Moreover the action of G leaves the rational function a fixed and permutes the b_i so we see from (4) that the coefficients of such tranformations may be assumed to lie in K.

Now, if $\sigma \in G$ and $\pi \in \boldsymbol{C} \cup \infty$ is a pole of a, we have that $\sigma(\pi)$ is a pole of a, whence the orbit of π under the action of G contains one or two elements.

Suppose first X has only one pole, corresponding to $t = \pi$. Then π is certainly in $K \cup \infty$, so, replacing eventually t with $\pi + 1/t$, we may assume that $\pi = \infty$. In particular $a(t)$ in (12) is a polynomial. Also, G stabilizes ∞ and thus consists of tranformations of type $\rho t + \phi$. This implies that G is cyclic (the map $\rho t + \phi \to \rho$ is an isomorphism of G onto a finite subgroup of K^*). Finally it is easily seen that, after a suitable K-translation on t, we may assume that G is generated by a transformation $t \to \zeta t$, where $\zeta \in K$. Necessarily ζ is a primitive d-th root of 1.

The degree of the polynomial $a(t)$ is, by (3), the degree of t over $K(X)$, which equals d by definition. On the other hand a is invariant under the action of G so, by the above, $a \in K[t^d]$ whence

$$a(t) = at^d + b$$

where $a, b \in K$.

Now we see that $m \in S$ if and only if $m = a\tau^d + b$ for a suitable

$\tau \in K$. It remains so to classify the $\tau \in K$ such that $a\tau^d + b \in D$. It is clear that the denominator of τ must be bounded, so we reduce to let τ vary over finitely many sets of the form $\{\delta_i \mu\}$ where δ_i are fixed computable elements of K and μ runs over D. Further $a\delta_i^d \mu^d + b \in D$ if and only if μ lies in certain congruence classes modulo a certain ideal J of D depending on a, b, δ_i. In conclusion S is the union of a finite set with finitely many sets of the form

$$\{a\delta_i^d \mu^d + b : \mu \in \gamma_i + J_i\} \tag{5}$$

for computable $\delta_i \in K$, $\gamma_i \in D$ and ideals $J_i \subset D$.

Suppose now that X has precisely two distinct poles corresponding to $t = \pi_1$ and $t = \pi_2$. Observe that π_1, π_2 either lie both in $K \cup \infty$ or are conjugate numbers in a quadratic extension. Put $K' = K(\pi_1)$. Consider the transformation

$$\tau(t) = \frac{t - \pi_1}{t - \pi_2} \in K'(t)$$

We may use $\tau(t) = u$, say, as a variable in place of t. In terms of this variable we have

$$X = a^*(u) \qquad a^* = a \circ \tau^{-1} \in K'(u) \tag{6}$$

and now the poles of X correspond to $u = 0, \infty$ while G is replaced by $G^* = \tau G \tau^{-1}$ as a group of linear fractional transformations on u.

Since the action of the Galois group is transitive on the places above a given one, some element of G^* (necessarily of the form $u \to b/u$) permutes the places $u = 0$ and $u = \infty$, so the stabilizer of ∞ in G^* has index 2. It follows also that G is dihedral of order $d = 2d'$ and that

$$G^* = \{\zeta u : \zeta^{d'} = 1\} \cup \{b\zeta u^{-1} : \zeta^{d'} = 1\} \tag{7}$$

for some $b \in K'$. In particular K' contains a primitive d'-th root of 1, say η. (From the above formula for τ it follows also that, if $K' \neq K$, then the nontrivial automorphism of K' over K acts as complex conjugation on η.)

We have

$$a^*(u) = \frac{f(u)}{u^m}$$

for some polynomial $f \in K'[u]$ satisfying $f(0) = 0$ and $d = \deg f > m$. Also, since a^* is invariant under the action of G^* we obtain that

$f \in K'[u^{d'}]$, $m = d'$, whence

$$a^*(u) = f_1 u^{d'} + f_0 + f_{-1} u^{-d'} \tag{8}$$

where the f_i lie in K'. Actually, since $a \in K(t)$ and π_1 and π_2 either lie in K or are conjugate quadratic, one obtains from (6) and (8) that in fact $f_0 \in K$, while f_1 and f_{-1}, if not in K, are conjugate in K'.

From (8) it follows that, if $u \in K'$ is such that $X = a^*(u)$ is an algebraic integer, then the fractional ideal generated by u in D', the ring of integers of K', has finitely many computable possibilities, so

$$u = \alpha v \tag{9}$$

where α runs through a finite computable set and v is a unit in D'.

Starting from (9), the necessary and sufficient condition for (8) to be an algebraic integer amounts to a congruence condition on v which, in view of Dirichlet's Theorem, is satisfied for all v in suitable cosets of the full unit group modulo a subgroup V of finite index whose generators may be computed. So $X \in D'$ iff

$$u = \beta w \tag{10}$$

where β runs through a finite computable set while $w \in V$.

We have still to exploit the condition $X \in K$, in case $K' \neq K$. This is equivalent to $t \in K$ which, by the above formulas amounts to $u\tilde{u} = 1$ where the tilde denotes conjugation in K' over K. From (10) we thus get

$$(\beta\tilde{\beta})w\tilde{w} = 1 .$$

This is satisfied precisely when w lies in a certain set (possibly empty) of cosets of V modulo its subgroup W consisting of elements whose relative norm to K is 1. (We remark that one may find generators for W.)

Finally we have that $X \in D$ if and only if

$$u = \gamma z \tag{11}$$

where γ lies in a finite computable set while $z \in W$.

REMARK. It follows from the proof that the set $S_{f,K'}$ differs by a finite set from a set of the form $S_{g,K'}$ where either $g(X, Y) = \alpha Y^d + \beta + X$ and $K' = K$ or $g(X, Y) = \alpha Y^{2d'} + (\beta X + \gamma)Y^{d'} + \delta$ and $[K' : K] \leqslant 2$.

REFERENCES

[1] A. BAKER, *Transcendental Number Theory*, Cambridge Univ. Press, Cambridge (1976).

[2] F. BALDASSARRI - B. DWORK, *On second order linear differential equations with algebraic solutions*, Amer. J. Math., **101** (1979), pp. 42-75.

[3] YU. BELOTSERKOVSKI (BILU), *Effective analysis of a new class of Diophantine equations* (Russian), Vestsi Akad. Navuk BSSR, Ser. Fiz.-Math. Navuk, (1988), no. 3, pp. 111-115 (Math. Rew. 89i:11038).

[4] J. COATES, *Construction of rational functions on a curve*, Proc. Camb. Phil. Soc., 68 (1970), pp. 105-123.

[5] R. DVORNICICH - U. ZANNIER, *Fields containing values of algebraic functions* ([3]), Annali Sc. Norm. Sup. Cl. Sci. Serie IV, Vol. XXI, Fasc. 3 (1994).

[6] S. LANG, *Fundamentals of Diophantine Geometry*, Springer-Verlag (1983).

([3]) A previous version of this paper appeared, without the Appendix, already in 1982 under the same title as a preprint of the University of Pisa.

Manoscritto pervenuto in redazione il 30 giugno 1993
e, in forma revisionata, il 12 ottobre 1993.