**C. R. Acad. Sci. Paris, Ser. I 334 (2002) 267–271**

**Théorie des nombres/*Number Theory***

# A subspace theorem approach to integral points on curves

**Pietro Corvaja [a], Umberto Zannier [b]**

[a] **Dip. di Matematica e Informatica, Via delle Scienze, 33100 Udine, Italy**

[b] **Ist. Univ. Arch.-D.C.A., S. Croce, 191, 30135 Venezia, Italy**

**Received 27 November 2001; accepted 10 December 2001**

**Note presented by Enrico Bombieri.**

**Abstract** We present a proof of Siegel's theorem on integral points on affine curves, through the Schmidt subspace theorem, rather than Roth's theorem. This approach allows one to work only on curves, avoiding the embedding into Jacobians and the subsequent use of tools from the arithmetic of Abelian varieties. ***To cite this article: P. Corvaja, U. Zannier, C. R. Acad. Sci. Paris, Ser. I 334 (2002) 267–271.*** © 2002 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

**Points entiers sur les courbes et théorème des sous-espaces**

**Résumé** Nous donnons une nouvelle démonstration du théorème de Siegel sur les points entiers des courbes, qui repose sur le théorème des sous-espaces de Schmidt. Notre méthode n'utilise pas le plongement d'une courbe dans sa jacobienne, évitant ainsi l'utilisation de résultats sur l'arithmétique des variétés abéliennes. ***Pour citer cet article : P. Corvaja, U. Zannier, C. R. Acad. Sci. Paris, Ser. I 334 (2002) 267–271.*** © 2002 Académie des sciences/Éditions scientifiques et médicales Elsevier SAS

## *Version française abrégée*

Soit $\widetilde{C}$ une courbe algébrique projective, absolument irréductible, définie sur un corps de nombres $k$. Soit $C$ un ouvert affine non vide de $\widetilde{C}$, plongé dans un espace affine $\mathbf{A}^m$. Soit $\mathcal{O}$ l'anneau des entiers de $k$. Le célèbre théorème de Siegel s'énonce alors :

THÉORÈME DE SIEGEL. – *Supposons que $C$ contient une infinité de points entiers de $\mathbf{A}^m(\mathcal{O})$. Alors $\widetilde{C}$ est de genre* 0 *et* $\#(\widetilde{C} \setminus C) \leqslant 2$.

La démonstration de Siegel [10] commence par plonger la courbe $\widetilde{C}$ dans sa jacobienne (dans le cas de genre non nul) ; après quoi les principaux ingrédients de la preuve sont : l'approximation diophantienne, le théorème de Mordell–Weil faible et le comportement quadratique de la hauteur sur les variétés abéliennes. Dans les démonstrations modernes, l'outil d'approximation diophantienne employé est le théorème de Roth, qui permet de simplifier la preuve originelle de Siegel. Après les travaux fondamentaux de W. Schmidt [7, 8], on dispose d'une généralisation en dimension supérieure du théorème de Roth, à savoir le théorème des

*E-mail addresses:* corvaja@dimi.uniud.it (P. Corvaja); zannier@iuav.it (U. Zannier).


S1631-073X(02)02240-9/FLA

sous-espaces [11, Theorem 2.2.1] concernant les approximations rationnelles d'une famille d'hyperplans définis sur $\overline{\mathbf{Q}}$. Nous montrons que ce résultat amène à une simplification de la preuve du théorème de Siegel.

Soit $S$ un ensemble fini de places de $k$, contenant les places archimédiennes; notons $\mathcal{O}_S$ l'anneau des $S$-entiers de $k$. Commencons par démontrer le

THÉORÈME 1. – *Supposons que* $\#(\widetilde{C}\backslash C) \geqslant 3$. *Alors* $C$ *ne contient qu'un nombre fini de points entiers de* $\mathbf{A}^m(\mathcal{O}_S)$.

*Démonstration.* – Il n'y a pas de perte de généralité à supposer que $\widetilde{C}$ soit lisse. Soient $Q_1, \ldots, Q_r$ les points de $\widetilde{C}\backslash C$, avec $r \geqslant 3$, que l'on peut supposer définis sur $k$. Pour tout entier positif $N$ considérons l'espace vectoriel $V = V_N$ sur le corps $k$ défini par

$$V = V_N = \left\{\varphi \in k(C) : \operatorname{div}(\varphi) \geqslant -N(Q_1 + \cdots + Q_r)\right\};$$

notons $d = d_N$ sa dimension et $\{\varphi_1, \ldots, \varphi_d\}$ une base. Le théorème de Riemann–Roch fournit l'inégalité $d \geqslant Nr + 1 - g$ où $g$ est le genre de la courbe $\widetilde{C}$. Soit $\{P_n\}_{n\in\mathbf{N}}$ une suite infinie de points $S$-entiers dans l'ouvert $C$. En remplaçant la suite $\{P_n\}_{n\in\mathbf{N}}$ par une sous-suite infinie, on se ramène au cas où, pour toute place $v \in S$, la suite converge vers un point $P^v \in \widetilde{C}(k_v)$; notons $S'$ le sous-ensemble de $S$ formé des places $v$ telles que $P^v \in \widetilde{C}\backslash C$ et posons $S'' = S\backslash S'$. Pour tout $v \in S'$ on peut construire une base $\{L_{1,v}, \ldots, L_{d,v}\}$ de $V$ de telle sorte que, pour tout $j = 1, \ldots, d$, la fonction $L_{j,v}$ s'annule au point $P^v$ avec une multiplicité $\geqslant N - j + 1$. Pour tout $v \in S''$ soit $\{L_{1,v}, \ldots, L_{d,v}\}$ une base quelconque de $V$. On fait choix d'un paramètre local $t_v \in k(\widetilde{C})$ au point $P^v$, pour toute place $v \in S'$. On a

$$\left|L_{j,v}(P_n)\right| \ll \left|t_v(P_n)\right|_v^{j-1-N}, \quad j = 1, \ldots, d,$$

ainsi que $|L_{j,v}(P_n)|_v \ll 1$ pour les places $v \in S''$. Alors

$$\prod_{v\in S}\prod_{j=1}^{d}\left|L_{jv}(P_n)\right|_v \ll \left(\prod_{v\in S'}\left|t_v(P_n)\right|_v\right)^{(d/2)(d-2N-1)} \leqslant \left(\prod_{v\in S'}\left|t_v(P_n)\right|_v\right)^{d((r-2)N-g)/2}.$$

Grâce à l'hypothèse d'intégralité des points $P_n$, on peut majorer la hauteur projective du point $(\varphi_1(P_N) : \ldots : \varphi_d(P_N))$ par $(\prod_{v\in S'}|t_v(P_n)|_v)^{-N}$. L'inégalité ci-dessus permet alors d'obtenir l'estimation

$$\prod_{v\in S}\prod_{j=1}^{d}\left|L_{j,v}(P_n)\right|_v \ll H\left(\varphi_1(P_n) : \ldots : \varphi_d(P_n)\right)^{-d((r-2)N-g)/(2N)}.$$

Pour $N \geqslant g + 1$, on a $d \geqslant 2$ et une application du théorème des sous-espaces permet de conclure que les points $(\varphi_1(P_n), \ldots, \varphi_d(P_n))$ sont contenus dans une réunion finie de sous-espaces propres de $k^d$, ce qui contredit l'indépendance des fonctions $\varphi_1, \ldots, \varphi_d$, démontrant ainsi le théorème 1.

Le cas général du théorème de Siegel se déduit du théorème 1 par une construction classique : si $\widetilde{C}$ est une courbe de genre $> 0$, elle admet des revêtements connexes non ramifiés $\pi : \widetilde{C}' \to \widetilde{C}$ de degré $> 1$. Les points entiers de $C$ se relèvent en des points entiers de $C' := \pi^{-1}(C)$ dans une extension de degré fini de $k$. Une application du théorème 1 à la courbe $C'$ permet alors de conclure.

## 1. Introduction

Let $\widetilde{C}$ be a projective, absolutely irreducible curve defined over a number field $k$, and let $C$ be an affine nonempty open subset of $\widetilde{C}$, embedded in affine space $\mathbf{A}^m$. Let $\mathcal{O}$ be the ring of integers of $k$. The celebrated Siegel's theorem on integral points on curves may be stated as follows:

**To cite this article: P. Corvaja, U. Zannier, C. R. Acad. Sci. Paris, Ser. I 334 (2002) 267–271**

SIEGEL'S THEOREM. – *Suppose that $C$ has infinitely many points in $\mathbf{A}^m(\mathcal{O})$. Then $\widetilde{C}$ has genus zero and moreover $\#(\widetilde{C} \setminus C) \leqslant 2$.*

Of course, at least for genus $g \geqslant 2$, this is a very special case of Faltings's celebrated solution of Mordell's Conjecture [2,4]. However, Siegel's original approach remains of independent interest.

Siegel's proof [10], starts by embedding $\widetilde{C}$ in its Jacobian (when the genus is positive); then essentially three ingredients come into the picture: the Diophantine approximation, the weak Mordell–Weil theorem and the quadratic behaviour of the height in Abelian varieties. (*See* also [4,5,9].)

The Diophantine approximation part nowadays appears through Roth's theorem. This substantially simplifies certain features of the original argument, which had to make recourse to simultaneous approximations.

Now, after the fundamental work of W.M. Schmidt [7,8], we dispose of a far-reaching generalization of Roth's theorem, namely the Subspace theorem and its subsequent versions by H.P. Schlickewei.

In the present Note we show that a substantial simplification in the proof of Siegel's theorem can be obtained by an appeal to Schmidt's theorem rather than Roth's. In particular, one avoids completely the final argument in the proof based on the behaviour of the height under pull-back of isogenies of the Jacobian of the curve.

The classical strategy is as follows. Let $\{P_n\}_{n\in\mathbf{N}}$ be a sequence of integral points on $\widetilde{C}$, converging to a point $Q \in \widetilde{C} \setminus C$ with respect to some valuation $v$ of $k$. Then, for a nonconstant function $\varphi \in k(C)$, one may assume that:

$$\big|\varphi(P_n) - \varphi(Q)\big|_v \ll H\big(\varphi(P_n)\big)^{-\delta} \qquad (*)$$

for some $\delta > 0$ depending only on the geometry of the curve $\widetilde{C}$. Since $\varphi(Q)$ must be an algebraic number and $\varphi(P_n) \in k$, this would be in direct contradiction of Roth's theorem if we had $\delta > 2$. This needs not be *a priori* the case, but replacing $\widetilde{C}$ by its pull-back by the isogeny multiplication-by-$m$ on the Jacobian $J(\widetilde{C})$, writing $P_n$ as $P_n = mP'_n + R$ where $R$ belongs to a finite set (by the weak Mordell–Weil theorem), and then replacing $Q$ by $Q' = (Q - R)/m$, one obtains $(*)$ with $P'_n$, $Q'$ in place of $P_n$, $Q$, and $\delta m^2$ in place of $\delta$. By choosing $m$ large we can achieve $\delta m^2 > 2$, concluding the argument.

Our main point is that using linear forms in sufficiently many variables $\varphi_1(P_n), \ldots, \varphi_r(P_n)$, with $\varphi_1, \ldots, \varphi_r$ suitable linearly independent rational functions on $\widetilde{C}$, one obtains an analogue of $(*)$ which directly contradicts Schmidt's subspace theorem, thus avoiding the rest of the argument and opening the possibility of new extensions to higher dimensions.

Let $S$ be a finite set of places of $k$ containing the Archimedean ones, and define as usual $\mathcal{O}_S = \{x \in k : |x|_v \leqslant 1 \text{ for all } v \notin S\}$. We shall first prove:

THEOREM 1. – *Assume that $\#(\widetilde{C} \setminus C) \geqslant 3$. Then $C$ has only finitely many points in $\mathbf{A}^m(\mathcal{O}_S)$.*

The full form of Siegel's theorem (actually in the sharpened formulation by Mahler with $\mathcal{O}_S$ in place of $\mathcal{O}$) covering the case in which $\#(\widetilde{C} \setminus C) \leqslant 2$ but with positive genus, is a well-known argument, applying Theorem 1 to an unramified cover of $\widetilde{C}$, with the only purpose of increasing the cardinality of $\widetilde{C} \setminus C$.

Before starting with the proofs, we recall for the reader's convenience a relevant version of the Subspace theorem, for instance as stated in [11], Theorem 2.2.1. We assume that each valuation $|\cdot|_v$ is normalized so that if $v|p$, then $|p|_v = p^{-[k_v:\mathbf{Q}_p]/[k:\mathbf{Q}]}$, where $k_v$ is the completion of $k$ at $v$, and similarly for Archimedean $v$. As usual, for a point $(x_1 : \ldots : x_d) \in \mathbf{P}^{d-1}(k)$, $(d \geqslant 2)$, we define the projective height as $H(x_1 : \ldots : x_d) = \prod_v \max(|x_1|_v, \ldots, |x_d|_v)$. We have:

SUBSPACE THEOREM. – *For an integer $d \geqslant 2$ and $v \in S$, let $L_{1v}, \ldots, L_{dv}$ be independent linear forms in $X_1, \ldots, X_d$ with coefficients in $k$, and let $\varepsilon > 0$. Then the solutions $(x_1, \ldots, x_d) \in \mathcal{O}_S^d$ of the inequality*

$$\prod_{v\in S}\prod_{j=1}^{d} \big|L_{jv}(x_1, \ldots, x_d)\big|_v \leqslant H^{-\varepsilon}(x_1 : \ldots : x_d)$$

*lie in the union of finitely many proper linear subspaces of $k^d$.*

## 2. Proof of Theorem 1

First of all, there is no loss of generality in assuming that $\widetilde{C}$ is nonsingular, as one readily verifies by going to a normal model. This may have the effect of enlarging the field $k$ and the set $S$, but the qualitative statement remains, because the cardinality $\#(\widetilde{C} \setminus C)$ will not decrease. We may also assume that the points $Q_1, \dots, Q_r$, $r \geqslant 3$, in $\widetilde{C} \setminus C$ are defined over $k$.

For a large positive integer $N$, to be chosen later, we consider the vector space $V = V_N$ over $k$ defined by

$$V = V_N = \big\{\varphi \in k\big(\widetilde{C}\big) : \operatorname{div}(\varphi) \geqslant -N(Q_1 + \ldots + Q_r)\big\}.$$

By the Riemann–Roch theorem we have

$$d = d_N := \dim_k V_N \geqslant Nr + 1 - g. \tag{1}$$

Let $\{\varphi_1, \dots, \varphi_d\}$ be a basis for $V$. The $\varphi_i$ are regular functions on $C$, expressed as the restrictions to $C$ of suitable polynomials in $k[X_1, \dots, X_m]$. On multiplying by a denominator, we may even assume that all the involved coefficients lie in $\mathcal{O}$.

Let now $\{P_n\}_{n\in\mathbf{N}}$ be an infinite sequence of distinct points in $C \cap \mathbf{A}^m(\mathcal{O}_S)$. By the previous remark, $\varphi_i(P_n) \in \mathcal{O}_S$ for $i = 1, \dots, d$ and all $n \in \mathbf{N}$.

Now, since $\widetilde{C}$ is complete, $\widetilde{C}(k_v)$ is compact. Therefore, replacing $\{P_n\}$ with an infinite subsequence, we may suppose that for each $v \in S$ the sequence $\{P_n\}$ converges $v$-adically to a point $P^v \in \widetilde{C}(k_v)$. We let $S = S' \cup S''$, where $S'$ is the set of places $v \in S$ such that $P^v \in \widetilde{C} \setminus C$ and $S'' = S \setminus S'$. Note that for $v \in S''$ the values $|\varphi_i(P_n)|_v$ are uniformly bounded, since then $P^v \in C(k_v)$ and since the $\varphi_i$ are regular on $C$.

Fix now $v \in S'$ and for $j \geqslant 1$ consider the vector subspace of $V$ defined by

$$W_j = W_{j,v} = \{\varphi \in V : \operatorname{ord}_{P^v}\varphi \geqslant j - 1 - N\}.$$

We plainly have $V = W_1 \supset W_2 \supset \cdots$ and $\dim(W_j/W_{j+1}) \leqslant 1$, since the additional vanishing imposes at most one linear condition; in particular, $\dim W_j \geqslant \dim V - j + 1 = d - j + 1$. We may now choose a basis of $W_d \neq \{0\}$ and successively complete it to bases of $W_{d-1}, W_{d-2}, \dots, W_1$, obtaining vectors $w_d, \dots, w_1$. Because $\dim W_j \geqslant d - j + 1$, we have $w_j \in W_j$ for $1 \leqslant j \leqslant d$. By expressing these vectors as linear combinations of the $\varphi_i$, we thus obtain linearly independent linear forms $L_{dv}, \dots, L_{1v}$ in $\varphi_1, \dots, \varphi_d$, defined over $k$ (because now $P^v \in \widetilde{C}(k)$) such that

$$\operatorname{ord}_{P^v} L_{jv} \geqslant j - 1 - N, \quad j = 1, \dots, d.$$

We define such linear forms also for $v \in S''$, simply by putting $L_{jv} = \varphi_j$ for $j = 1, \dots, d$.

For $v \in S'$, choose once and for all a local parameter $t_v \in k(\widetilde{C})$ at $P^v$ (which is possible since again $P^v \in \{Q_1, \dots, Q_r\}$ is defined over $k$). Then, for a function $\psi \in k(\widetilde{C})$ having order $q$ at $P^v$, we have that $t_v^{-q}\psi$ is regular at $P^v$, whence $|t_v^{-q}(P_n)\psi(P_n)|_v$ is bounded, since $P_n \to_v P^v$. In other words, $|\psi(P_n)|_v \ll |t_v(P_n)|_v^q$, where the implied constant is independent of $n$. Taking into account that $|t_v(P_n)|_v \leqslant 1$ for large $n$, we find

$$\big|L_{jv}(P_n)\big|_v \ll \big|t_v(P_n)\big|_v^{j-1-N}, \quad j = 1, \dots, d,$$

whence

$$\prod_{j=1}^{d}\big|L_{jv}(P_n)\big|_v \ll \big|t_v(P_n)\big|_v^{d(d-1)/2-dN} = \big|t_v(P_n)\big|_v^{(d/2)(d-2N-1)}. \tag{2}$$

Also, $|L_{jv}(P_n)|_v \ll 1$ for $v \in S''$ (because the $|\varphi_j(P_n)|_v$ are then bounded), whence

$$\prod_{v\in S}\prod_{j=1}^{d}\big|L_{jv}(P_n)\big|_v \ll \left(\prod_{v\in S'}\big|t_v(P_n)\big|_v\right)^{(d/2)(d-2N-1)} \leqslant \left(\prod_{v\in S'}\big|t_v(P_n)\big|_v\right)^{d((r-2)N-g)/2}. \tag{3}$$

On the other hand, we have $\max_j |\varphi_j(P_n)|_v \leqslant 1$ for $v \notin S$, $\max_j |\varphi_j(P_n)|_v \ll 1$ for $v \in S \setminus S'$ and $\max_j |\varphi_j(P_n)|_v \ll |t_v(P_n)|_v^{-N}$ for $v \in S'$. (Again, the implied constants do not depend on $n$.)

Therefore the projective height $H(\varphi_1(P_n) : \ldots : \varphi_d(P_n))$ is $\ll (\prod_{v\in S'} |t_v(P_n)|_v)^{-N}$. Comparing with (3) we obtain

$$\prod_{v\in S}\prod_{j=1}^{d} \big|L_{jv}(P_n)\big|_v \ll H\big(\varphi_1(P_n) : \ldots : \varphi_d(P_n)\big)^{-d((r-2)N-g)/(2N)}.$$

For $N \geqslant g+1$, we have $d \geqslant 2$, so the $\varphi_j$ are not all proportional. Hence $H(\varphi_1(P_n) : \ldots : \varphi_d(P_n)) \to \infty$ as $n \to \infty$, otherwise all the ratios $\varphi_j(P_n)/\varphi_1(P_n)$ would belong to a finite set independent of $n$, and the same would be true for $P_n$. We may thus apply the Subspace theorem and conclude that all the points $(\varphi_1(P_n), \ldots, \varphi_d(P_n))$, $n \in \mathbf{N}$, lie in the union of finitely many proper linear subspaces of $k^d$. Since $\varphi_1, \ldots, \varphi_d$ are linearly independent functions on $\widetilde{C}$, this again implies that $P_n$ belongs to a finite set independent of $n$, a contradiction which proves Theorem 1.

*Remark.* – Using the quantitative versions of the Subspace Theorem due to Schlickewei [6] and Evertse [1], it is possible to get uniform versions of Theorem 1. For instance, an argument similar to the above one shows that for a given curve $C$ with $\#(\widetilde{C} \setminus C) \geqslant 3$, the number of points of $C$ over the ring of integers of $k$ may be bounded only in terms of the degree $[k : \mathbf{Q}]$. This result does not follow from the classical method of proof.

## 3. Proof of Siegel's theorem

We may plainly suppose that $\widetilde{C}$ has positive genus, so there exists a topological (unramified) covering space $\pi : \widetilde{C}' \to \widetilde{C}$ of finite degree $\geqslant 3$. It is a well-known fact (but a highly nontrivial one) that $\widetilde{C}' \to \widetilde{C}$ can be given the structure of a cover of algebraic curves (see, e.g., [3]), and by specialization we may also assume that the cover is defined over $\overline{\mathbf{Q}}$. Alternatively, one constructs $\widetilde{C}'$ by immersion of $\widetilde{C}$ in its Jacobian and pull-back by a suitable isogeny.

Let now $C' = \pi^{-1}(C)$. Then $C'$ is affine and $\#(\widetilde{C}' \setminus C') \geqslant 3$. Now, by a rather simple version of the Chevalley–Weil theorem, we verify as in (3), p. 109 of [9], that the $S$-integral points on $C$ lift simultaneously to $S'$-integral points on $C'$, relative to a suitable number field $k' \supset k$ and finite set of places $S'$ of $k'$.

To conclude, it suffices now to apply Theorem 1 to $C'$, $k'$ and $S'$.

**Acknowledgements.** The authors acknowledge the kind hospitality and the support provided by the Université de Lille 1, July 2001, when the present paper was prepared. They also thank Professor Enrico Bombieri for helpful advice on the final arrangement of the manuscript.

## References

[1] J.H. Evertse, An improvement of the quantitative subspace theorem, Compositio Math. 101 (1996) 225–311.
[2] G. Faltings, Endlichkeitssätzes für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983) 349–366.
[3] O. Forster, Riemann Surfaces, Springer-Verlag, 1981.
[4] M. Hindry, Silverman J.H., Diophantine Geometry, Springer-Verlag, 2000.
[5] S. Lang, Fundamentals of Diophantine Geometry, Springer-Verlag, 1982.
[6] H.P. Schlickewei, The quantitative subspace theorem for number fields, Compositio Math. 82 (1992) 245–273.
[7] W.M. Schmidt, Diophantine Approximation, Lecture Notes in Math., Vol. 785, Springer-Verlag, 1987.
[8] W.M. Schmidt, Diophantine Approximations and Diophantine Equations, Lecture Notes in Math., Vol. 1467, Springer-Verlag, 1991.
[9] J.-P. Serre, Lectures on the Mordell–Weil Theorem, Vieweg, 1989.
[10] C.L. Siegel, Über einige Anwendungen diophantischer Approximationen, Abh. Pr. Akad. Wiss. 1 (1929) (Ges. Abh., I, 209–266).
[11] P. Vojta, Diophantine Approximations and Value Distribution theory, Lecture Notes in Math. 1239, Springer-Verlag.