

ANDREA SURROCA (*)

Siegel's theorem and the *abc* conjecture ()**

1 - Introduction

One of the fundamental theorems in diophantine geometry, proved by C.L. Siegel, says that an algebraic affine curve of genus ≥ 1 or of genus zero with 3 points at infinity and defined over a number field K has only finitely many integral points. Thanks to the contribution of K. Mahler, Siegel's theorem was extended to the S -integral points, that is, those having the prime factors of the denominators in the finite set of valuations S of K .

For curves of genus ≥ 2 , Siegel's theorem is superseded by Falting's one (Mordell's conjecture), which asserts that there are finitely many rational points on an algebraic projective curve of genus ≥ 2 . However, there are no effective versions of these theorems, in the sense that the proofs do not provide an algorithm to find such points. Some effective results concerning integral points are known, thanks to Baker's method based on linear forms in logarithms. In fact, this method gives upper bounds for the height (i.e. the size) of the (S -)integral points.

N. Elkies proposed in [El] an effective method to study rational points on algebraic curves, but it remains conjectural, because it is based on the *abc* conjecture of Masser-Oesterlé. This approach was the motivation for the work that we explain here.

(*) Institut de mathématiques de Jussieu, Université Pierre et Marie Curie (Paris 6), Equipe de Théorie de nombres, Case 247, 175 rue du Chevaleret, 75013 Paris, France; e-mail: surroca@math.jussieu.fr

(**) Received 2nd March 2004 and in revised form 1st September 2004. AMS classification 11 G 30, 11 J 25, 11 G 50.

Conjecture 1 (abc). *Let K be a number field. For every $\varepsilon > 0$, there exists a real number $c_{\varepsilon, K} > 0$ such that, for every $a, b, c \in K \setminus \{0\}$ and verifying $a + b = c$, we have*

$$h_K(a : b : c) < (1 + \varepsilon) \operatorname{rad}(a : b : c) + c_{\varepsilon, K}.$$

In this note we will explain some links between upper bounds on the height of S -integral points on algebraic curves and the *abc* conjecture.

Acknowledgements. The results quoted in this note come from the PhD thesis of the author, who wants to thank her advisors, Marc Hindry and Michel Waldschmidt. She wants also to thank Machiel van Frankenhuysen for sending her some of his off prints, and the anonymous referee for pointing out to her the references [S-T1], [S-T2] and [Tu].

2 - Notations

Let us denote by U an algebraic affine curve of genus g defined over a number field K , \tilde{U} will denote its normalization and C a projective curve containing \tilde{U} . Let $U_{\infty} = C \setminus \tilde{U} = \{P_1, \dots, P_t\}$ be the «points at infinity». The Euler-Poincaré characteristic of U is the number $\chi(U) = 2 - 2g - t$. The curve U verifies the hypothesis of Siegel's theorem if and only if $\chi(U) < 0$.

Let S be a finite set of valuations of the number field K and denote O_K and $O_{K,S}$ respectively, the ring of integers and the ring of S -integers of K .

Denote also by $U(O_{K,S})$ the K -rational points on U which have S -integral coordinates with respect to the embedding $\phi_D: U \hookrightarrow \mathbf{A}^n$ given by a very ample divisor $D \in \operatorname{Div}(C)$, such that $\operatorname{supp}(D) = U_{\infty}$.

All along this paper, h will denote the absolute logarithmic Weil's height on \mathbf{P}^n , $h_K = [K : \mathbf{Q}] h$, and h_U a height on U relative to a degree 1 divisor (e.g. $h_U = \frac{1}{\deg(f)} h \circ f$, where f is a non constant regular function on U).

If $x = (x_0 : x_1 : x_2) \in \mathbf{P}^2(K)$, we define the radical (or the support) of x (with logarithmic notation) by

$$\operatorname{rad}(x) = \sum \log N_{K/\mathbf{Q}}(\mathfrak{p}),$$

where the sum is taken over the prime ideals \mathfrak{p} of K for which the cardinality of $\{v_{\mathfrak{p}}(x_0), v_{\mathfrak{p}}(x_1), v_{\mathfrak{p}}(x_2)\}$ is greater than or equal to 2.

For example, if x_0, x_1, x_2 are nonzero rational coprime numbers, $h(x_0 : x_1 : x_2)$

$= \log \max \{ |x_0|, |x_1|, |x_2| \}$ and $\text{rad}(x_0 : x_1 : x_2) = \log \prod p$, where the product is taken over the prime numbers p dividing x_0, x_1 or x_2 .

3 - Statement of the results

Following the ideas proposed by Elkies in [El] (see also [MvF]) we show that (an effective version of) the *abc* conjecture implies an effective version of Siegel's theorem i.e. an upper bound for the height of the S -integral points where the dependence on S is explicit. (Cf. the last section for the proof.)

Theorem 1. *Let K be a number field, U an affine algebraic curve defined over K such that $\chi(U) < 0$, S a finite set of absolute values of K and $h_{U,K}$ a height function on $U(K)$ associated to a degree 1 divisor.*

*Suppose the *abc* conjecture is true.*

For every $\varepsilon \in]0, -\chi(U)[$ and every S -integral point x on U , there exists a number γ depending on the number field K , on the curve U , on the choice of the height $h_{U,K}$ and on ε , but neither on the point x nor on the set S , such that

$$(1) \quad h_{U,K}(x) \leq -\frac{1}{\varepsilon + \chi(U)} \sum_{p \in S} \log N_{K/\mathbf{Q}}(p) + \gamma.$$

Moreover, if the constant $c_{\varepsilon,K}$ of the Conjecture 1 were effective, the same would be true for γ .

If we consider a version of the *abc* conjecture where the dependence of $c_{\varepsilon,K}$ on the number field is explicit, e. g. $c_{\varepsilon,K} = 2 \log d_K + \kappa$ (cf. [Ma]), we would obtain the same upper bound, but with

$$(2) \quad \gamma = -\frac{2}{\varepsilon + \chi(U)} \log d_K + \kappa,$$

where d_K is the absolute value of the discriminant of K and κ only depends on the degree $[K : \mathbf{Q}]$ of the number field K .

Inequality (1) modified with (2) suggests the following hypothesis.

Fix an algebraic affine curve U defined over K and verifying $\chi(U) < 0$, as well as a height function h_U on U , associated to a divisor of degree 1.

Hypothesis 1 Siegel (U, K). *For every $\delta \geq [K : \mathbf{Q}]$, there exists constants $k_1(U, h_U, \delta) > 1$, $k_2(U, h_U, \delta) > 1$ and $k_3(U, h_U, \delta) > 0$ such that, for every fini-*

te extension L/K of degree $[L : \mathbf{Q}] \leq \delta$, for every finite set S of valuations of L and for every S -integral point x on U , we have

$$(3) \quad h_{U,L}(x) \leq k_1 \sum_{\mathfrak{q} \in S} \log N_{L/\mathbf{Q}}(\mathfrak{q}) + k_2 \log d_L + k_3,$$

where d_L is the absolute value of the discriminant of the field L and $h_{U,L} = [L : \mathbf{Q}] h_U$.

A similar hypothetical upper bound for rational points was considered by L. Moret-Bailly [M-B] to show that an effective version of Mordell's conjecture would imply the *abc* conjecture. Moreover, the analogue of the hypothesis 1 in the function field case has already been proved (see the appendix of [Sur] and the references therein).

We prove the following theorem.

Theorem 2. *Let K be a number field, U an algebraic affine curve defined over K and such that $\chi(U) < 0$. Let h_U be a height function on U associated to a degree 1 divisor.*

Assume the hypothesis 1.

Then, there exists real positive numbers η_1 and η_3 depending on U and on the degree $[K : \mathbf{Q}]$, and η_2 depending only on U such that, for every $a, b, c \in K \setminus \{0\}$ and verifying $a + b = c$, we have

$$h_K(a : b : c) < \eta_1 \text{rad}(a : b : c) + \eta_2 \log d_K + \eta_3.$$

The proofs of Theorem 1 and Theorem 2 make use of a Belyĭ function.

Theorem 3 (Belyĭ). *An algebraic projective curve C is defined over $\overline{\mathbf{Q}}$ if and only if there exists a finite and surjective morphism $f : C \rightarrow \mathbf{P}^1$, unramified outside $\{0, 1, \infty\}$.*

Moreover, if $\Sigma \subset C(\overline{\mathbf{Q}})$, we can choose f such that $f(\Sigma) \subset \{0, 1, \infty\}$.

The construction of such a function is completely explicit and if the curve C is defined over a number field K the same will be true for the function f .

For the proof of Theorem 2 the main idea is to put $y = (a : c) \in \mathbf{P}^1(K)$ and prove that a point x in U such that $f(x) = y$, where f is a Belyĭ function, is in fact S' -integral for some finite extension L/K and some finite set S' of valuations of L . To conclude we apply the hypothesis 1 to x . (Cf. [Sur] for a detailed proof.)

Yu. Bilu obtained in [Bi] an upper bound weaker than (3), but unconditional, for Galois coverings. His result allows us to prove the following theorem.

Theorem 4. *For every number field K , there exists real and effectively computable numbers $\gamma_1, \gamma_2 > 1$, depending on K such that, for every (a, b, c) in $K \setminus \{0\}$ and verifying $a + b = c$,*

$$h_K(a : b : c) \leq \exp \{ \gamma_1 \text{rad}(a : b : c) + \gamma_2 \}.$$

Theorem 4 generalizes to any number field a result of Stewart-Yu [S-Y] (valid over \mathbf{Q}) which is the best known result in the direction of the *abc* conjecture.

4 - Proof of Theorem 1

Let U be an algebraic affine curve of genus g defined over a number field K , \tilde{U} its normalization and C a projective curve containing \tilde{U} . Suppose that $\chi(U) < 0$.

Lemma 1. *There exists a rational function $f \in K(C)$ such that*

$$\text{card}(\{x \in U(\overline{\mathbf{Q}}) / f(x) \in \{0, 1, \infty\}\}) = \chi(U) + d,$$

where d is the degree of f .

Proof of the Lemma 1. Apply Theorem 3 to the projective curve C , and to the set $\Sigma = \{P_1, \dots, P_t\}$. Fix such a Belyĭ function f and set $d = \deg(f)$.

Set also $m = \text{card}(\{x \in C(\overline{\mathbf{Q}}) / f(x) \in \{0, 1, \infty\}\})$.

The function f is ramified only above $0, 1$ and ∞ , so the Riemann-Hurwitz formula gives

$$\sum_{P \in C, f(P) \in \{0, 1, \infty\}} (e_P(f) - 1) = 2d + 2g - 2,$$

and then

$$m = 3d - \sum_{P \in C, f(P) \in \{0, 1, \infty\}} (e_P(f) - 1) = d - 2g + 2.$$

Moreover, $f(\{P_1, \dots, P_t\}) \subset \{0, 1, \infty\}$, then

$$\text{card}(\{x \in U(\overline{\mathbf{Q}}) / f(x) \in \{0, 1, \infty\}\}) = m - \text{card}(U_\infty(\overline{\mathbf{Q}})) = m - t = d + \chi(U). \quad \blacksquare$$

Let S be a finite set of absolute values of K . Let x be in $U(O_{K,S})$ such that $f(x) = (r : 1) \in \mathbf{P}^1 \setminus \{0, 1, \infty\}$. (If $f(x) \in \{0, 1, \infty\}$, then $h_K(f(x)) = 0$ and the inequality (1) is verified.) We can then apply Conjecture 1 to $P_x = (r : 1 - r : 1)$. For

every $\varepsilon > 0$, there exists a constant $c_{\varepsilon, K}$, such that

$$h_K(P_x) \leq (1 + \varepsilon)\text{rad}(P_x) + c_{\varepsilon, K}.$$

Choose $h_{U, K} = \frac{1}{d}(h_K \circ f)$. We then have

$$dh_{U, K}(x) = h_K(f(x)) = h_K(r : 1) \leq h_K(r : 1 - r : 1) = h_K(P_x).$$

We conclude with the following proposition which gives an upper bound of the radical in terms of the height.

Proposition 1. *There exists constants c_1 and c_2 depending only on the degree $[K : \mathbf{Q}]$ of the number field K and of the curve U , such that*

$$\text{rad}(P_x) \leq \left(\frac{\chi(U)}{d} + 1 \right) h_K(f(x)) + c_1 \sqrt{h_K(f(x))} + c_2 + \sum_{\mathfrak{p} \in S} \log N(\mathfrak{p}).$$

To prove Proposition 1, let us introduce, like in [MvF], the divisors of zero, of 1 and of the point at infinity, with respect to the Belyi's function f . Let $D_0 = f^*(0) = \sum_{x \in C(\overline{\mathbf{Q}}), f(x)=0} e_x(f)(x) \in \text{Div}(C)$, where $e_x(f)$ is the ramification index of f at the point x , be the divisor of zero. Denote by $D_0|_U = \sum_{x \in U(\overline{\mathbf{Q}}), f(x)=0} e_x(f)(x)$ the restriction of the divisor to the affine curve U . In the same way, define the divisor D_1 of 1, and D_∞ of the infinity. The curve U is defined over K , so Belyi's theorem allows us to take f defined over K . The divisors $D_0|_U, D_1|_U$ and $D_\infty|_U$ are defined over K and have a decomposition into irreducible divisors:

$$D_0|_U = e_1 M_1 + \dots + e_i M_i,$$

$$D_1|_U = e_{i+1} M_{i+1} + \dots + e_j M_j,$$

$$D_\infty|_U = e_{j+1} M_{j+1} + \dots + e_k M_k.$$

By the Riemann-Roch theorem we can prove that for every $\nu \in \{1, \dots, k\}$, there is a function $m_\nu: C \rightarrow \mathbf{P}^1$ such that

$$(2g + 1) M_\nu = m_\nu^*(0).$$

We can show that there exists a finite set T of valuations of K (depending only on the curve U) such that, there exists a model \mathcal{C} of the curve C over \mathcal{B} , where $\mathcal{B} = \text{Spec}(O_{K, \tau}) = \text{Spec}(O_K) \setminus T$, such that:

- i) all the special fibers of this model are smooth projective curves,

ii) the functions f and m_v extend to morphisms \tilde{f} and \tilde{m}_v from \mathcal{C} to $\mathbf{P}_{O_{K,T}}^1 = \mathbf{P}_{\mathcal{B}}^1$ over \mathcal{B} .

In other words, we can say that the curve C has good reduction at primes outside T , and that the functions f and m_v are not reduced to the identically zero function.

Lemma 2. *Let \mathfrak{p} be a prime ideal in \mathcal{B} , which contributes to the radical of P_x . If $\mathfrak{p} \notin S$, then*

$$\log N(\mathfrak{p}) \leq \frac{d_{\mathfrak{p}}}{2g+1} \sum_{v=1}^k \max\{0, v_{\mathfrak{p}}(m_v(x))\}.$$

Proof of the Lemma 2. Fix $\mathfrak{p} \in \mathcal{B}$ and put $\mathcal{U} = \mathcal{C} \setminus \overline{\text{supp}(D)}^{Zar}$. Then \mathcal{U} is an affine model of U over \mathcal{B} for which all the fibers are smooth affine curves.

Every rational point $x \in C(K) \setminus f^{-1}(\{0, 1, \infty\})$ corresponds to a morphism $\text{Spec}(K) \rightarrow C$ and extends to a section $\sigma_x: \mathcal{B} \rightarrow \mathcal{C}$. The point $f(x) \in \mathbf{P}_K^1$ extends to a section $\sigma_{f(x)}: \mathcal{B} \rightarrow \mathbf{P}_{O_{K,T}}^1$. Moreover $\tilde{f}(\sigma_x(\mathfrak{p})) = \sigma_{f(x)}(\mathfrak{p})$.

If $D = \sum n_x(x)$ is a divisor of C defined over K (i.e. the sum is taken over some points $x \in C(K)$), let us denote $\tilde{D} = \sum n_x \sigma_x(\mathfrak{p})$ the reduced divisor. (A priori, the point $\sigma_x(\mathfrak{p}) \in \mathcal{C}_{\mathfrak{p}}$ and, $\sigma_x(\mathfrak{p}) \in \mathcal{U}_{\mathfrak{p}}$ if and only if, x is in U and is \mathfrak{p} -integral). Moreover, $\text{supp}(\tilde{D}) \cap \mathcal{U}_{\mathfrak{p}} = \text{supp}(\tilde{D}|_{\mathcal{U}})$.

Set $H_x = \{q/v_q(f(x)) > 0 \text{ or } v_q(f(x)) < 0 \text{ or } v_q(1-f(x)) > 0\}$. Note that $\{q/\text{card}(\{v_q(r), v_q(1-r), v_q(1)\}) \geq 2\} = H_x$. Then

$$\text{rad}(P_x) = \sum_{q \in H_x} \log N(q).$$

We then have

$$\begin{aligned} \mathfrak{p} \in H_x &\Leftrightarrow \sigma_{f(x)}(\mathfrak{p}) = \tilde{0} \text{ or } \sigma_{f(x)}(\mathfrak{p}) = \tilde{\infty} \text{ or } \sigma_{f(x)}(\mathfrak{p}) = \tilde{1}, \\ &\Leftrightarrow \tilde{f}(\sigma_x(\mathfrak{p})) = \tilde{0} \text{ or } \tilde{f}(\sigma_x(\mathfrak{p})) = \tilde{\infty} \text{ or } \tilde{f}(\sigma_x(\mathfrak{p})) = \tilde{1} \\ &\Leftrightarrow \sigma_x(\mathfrak{p}) \in \text{supp}(\tilde{D}_0) \cup \text{supp}(\tilde{D}_{\infty}) \cup \text{supp}(\tilde{D}_1), \end{aligned}$$

where \tilde{D}_0, \tilde{D}_1 et \tilde{D}_{∞} are divisors of the special fiber $\mathcal{C}_{\mathfrak{p}}$.

If we suppose that x is an S -integral point of U and that $\mathfrak{p} \notin S$, then the reduced point is in the reduced affine curve, i.e. $\sigma_x(\mathfrak{p}) \in \mathcal{U}_{\mathfrak{p}}$. In this case, we then have

$$\begin{aligned} \mathfrak{p} \in H_x &\Rightarrow \sigma_x(\mathfrak{p}) \in \text{supp}(\widetilde{D}_0|_U) \cup \text{supp}(\widetilde{D}_\infty|_U) \cup \text{supp}(\widetilde{D}_1|_U) \\ &\Leftrightarrow \exists \mu \in \{1, \dots, k\}, \sigma_x(\mathfrak{p}) \in \text{supp}(\widetilde{M}_\mu) \\ &\Leftrightarrow \exists \mu \in \{1, \dots, k\}, \text{ord}_{\sigma_x(\mathfrak{p})}(\widetilde{M}_\mu) \geq 1. \end{aligned}$$

By definition, $v_{\mathfrak{p}}(m_\mu(x)) = \frac{\text{ord}_{\mathfrak{p}}(m_\mu(x))}{d_{\mathfrak{p}}} \log N(\mathfrak{p})$, where $d_{\mathfrak{p}}$ is the local degree. Since $\text{ord}_{\mathfrak{p}}(m_\mu(x)) \geq \text{mult}_{\sigma_x(\mathfrak{p})}(\widetilde{m}_\mu) = (2g + 1) \text{ord}_{\sigma_x(\mathfrak{p})}(\widetilde{M}_\mu) \geq 2g + 1$, then

$$v_{\mathfrak{p}}(m_\mu(x)) \geq \frac{2g + 1}{d_{\mathfrak{p}}} \log N(\mathfrak{p}) \text{ i.e. } \log N(\mathfrak{p}) \leq \frac{d_{\mathfrak{p}}}{2g + 1} v_{\mathfrak{p}}(m_\mu(x)).$$

Therefore, if $x \in U(O_{K,S})$ et $\mathfrak{p} \in (\mathcal{B} \cap H_x) \setminus S$, then

$$\log N(\mathfrak{p}) \leq \frac{d_{\mathfrak{p}}}{2g + 1} \sum_{\nu=1}^k \max\{0, v_{\mathfrak{p}}(m_\nu(x))\}. \quad \blacksquare$$

Proof of the Proposition 1. Lemma 2 gives us an upper bound for $\log N(\mathfrak{p})$ for the prime ideals \mathfrak{p} contributing to the radical of P_x (i.e. for $\mathfrak{p} \in H_x$) for which $f(x)$ is \mathfrak{p} -integral and the curve C and the functions f and m_ν have good reduction. Denote by Σ_S (respectively by Σ_T) the sum of $\log N(\mathfrak{p})$ taken over $\mathfrak{p} \in S$ (respectively over $\mathfrak{p} \in T$). Applying Lemma 2 we then obtain

$$\text{rad}(P_x) \leq \sum_{\mathfrak{p} \in (H \cap \mathcal{B}) \setminus S} \frac{d_{\mathfrak{p}}}{2g + 1} \sum_{\nu=1}^k \max\{0, v_{\mathfrak{p}}(m_\nu(x))\} + \Sigma_S + \Sigma_T.$$

Since $(H \cap \mathcal{B}) \setminus S$ is included in the set of all the valuations of K and $\frac{d_{\mathfrak{p}}}{2g + 1} \sum_{\nu=1}^k \max\{0, v_{\mathfrak{p}}(m_\nu(x))\}$ is always positive, we obtain

$$\text{rad}(P_x) \leq \sum_{\nu=1}^k \frac{1}{2g + 1} \sum_{v \in M_K} d_v \max\{0, v(m_\nu(x))\} + \Sigma_S + \Sigma_T.$$

But $\sum_{v \in M_K} d_v \max\{0, v(m_\nu(x))\} = h_K(m_\nu(x))$. Since for every $\nu \in \{1, \dots, k\}$, h_{K, m_ν} and $h_{K, f}$ are two height functions on the curve C , by the height theory we have

$$h_K(m_\nu(x)) = \frac{\deg(m_\nu)}{\deg(f)} h_K(f(x)) + O(\sqrt{h_K(f(x))}),$$

where the implicit constant in the O depends only on the degree of the number field K and on the curve C . Since $\deg(m_\nu) = (2g + 1) \deg(M_\nu) = (2g + 1) d_\nu$ and $\deg(f) = d$, we have

$$\text{rad}(P_x) \leq \frac{1}{d} \left(\sum_{\nu=1}^k d_\nu \right) h_K(f(x)) + c_1 \sqrt{h_K(f(x))} + \Sigma_S + \Sigma_T,$$

where the constant c_1 depends only on the degree of K and on the curve C .

Since for all $\nu \in \{1, \dots, k\}$, $d_\nu = \deg(M_\nu) = \text{card}(\text{supp}(M_\nu))$, we conclude applying the lemma 1:

$$\sum_{\nu=1}^k d_\nu = \text{card}(\{x \in U(\overline{\mathbf{Q}}) / f(x) \in \{0, 1, \infty\}\}) = \chi(U) + d. \quad \blacksquare$$

References

- [Be] G. V. BELYĬ, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izvestija **14** (2) (1980).
- [Bi] YU. F. BILU, *Quantitative Siegel's theorem for Galois coverings*, Compositio Math. **106** (1997), 125-158.
- [El] N. D. ELKIES, *ABC implies Mordell*, Internat. Math. Res. Notices **7** (1991), 99-109.
- [MvF] M. VAN FRANKENHUYSEN, *The ABC conjecture implies Roth's theorem and Mordell's conjecture*, Mat. Contemp. **16** (1999), 45-72.
- [Ma] D. W. MASSER, *On abc and discriminants*, Proc. Amer. Math. Soc. **130** (2002), 3141-3150.
- [M-B] L. MORET-BAILLY, *Hauteurs et classes de Chern sur les surfaces arithmétiques*, Astérisque **183** (1990), 37-58.
- [S-T1] X. SONG and T. J. TUCKER, *Dirichlet's theorem, Vojta's inequality, and Vojta's conjecture*, Compositio Math. **116** (1999), 219-238.
- [S-T2] X. SONG and T. J. TUCKER, *Arithmetic discriminants and morphisms of curves*, Trans. Amer. Math. Soc. **353** (2001), 1921-1936.

- [S-Y] C. L. STEWART and K. YU, *On the abc conjecture, II*, Duke Math. J. **108** (2001), 169-181.
- [Sur] A. SURROCA, *Méthodes de transcendance et géométrie diophantienne*, Thèse de doctorat de l'Université Paris VI, 2003. <http://www.math.jussieu.fr/~surroca>
- [Tu] T. J. TUCKER, *Irreducibility, Brill-Noether loci and Vojta's inequality*, with an appendix of O. Debarre, Trans. Amer. Math. Soc. **354** (2002), 3011-3029.

Abstract

Following N. Elkies [E1] we show that the abc conjecture of Masser-Oesterlé implies an effective version of Siegel's theorem about integral points on algebraic curves, i.e. an upper bound for the height of the S -integral points where the dependence on S is explicit. The converse statement is also announced in this note. For both results, the main geometric tool is a theorem of G.V. Belyĭ.
