数理解析研究所講究録 1319 巻 2003 年 202-210

Vojta's method in diophantine geometry, applications and related topics

Gaël RÉMOND

1 Introduction

The method of Vojta's referred to in the title is the one he introduced to prove Mordell's conjecture. We therefore start from this conjecture. As is well known, Faltings ([F1]) was the first to prove the following statement in 1983, some sixty years after Mordell's question:

Theorem 1. *A curve of genus at least two over a number field has finitely many rational points.*

Then, in 1990, Vojta gave a different proof of this fact which was based on diophantine approximation (see [V1]). His approach led to various and powerful generalisations of Faltings' theorem. This paper is intended as a short survey of this topic: I shall briefly sketch the original method and then present the different results that can be obtained through extensions of it.

In this introduction, we give a slight generalisation of Theorem 1 in a formulation that will make the further generalisations appear more natural. In the situation of Theorem 1, let C be the curve and K the number field. We introduce the Jacobian J of C. We recall that it is an abelian variety of dimension equal to the genus of C. Furthermore, C can be imbedded in J (assume for example that C has at least one rational point). Finally, let $\Gamma = J(K)$ be the group of rational points of J. The well-known Mordell-Weil theorem states that Γ is a finitely generated group. With this notation, the rational points of C can be written

$$C(K) = C(\bar{K}) \cap \Gamma.$$

In this way, the following statement indeed contains Theorem 1.

Theorem 2. *Let C be a* $\boxed{\textit{curve of genus } \geq 2}$ *in an* $\boxed{\textit{abelian variety}}$ *A over $\bar{\mathbb{Q}}$ and Γ a* $\boxed{\textit{finitely generated subgroup}}$ *of $A(\bar{\mathbb{Q}})$. Then the set $C(\bar{\mathbb{Q}}) \cap \Gamma$ is* $\boxed{\textit{finite}}$.

Note that considering any finitely generated subgroup, instead of simply rational points over a given number field, is in fact no strengthening of the statement, since any such Γ is contained in $A(K')$ for a certain number field K' (simply consider a field of definition for a finite set of generators of Γ). On the other hand, replacing the Jacobian by any abelian variety gives a slightly stronger statement but Vojta's proof yields at once this form.

The boxed words in the theorem indicate in what directions we are going to generalise it. Roughly speaking, we will describe three directions: allowing more choice for respectively C, A and Γ. Let us say here that another natural variation would be to consider other fields than $\bar{\mathbb{Q}}$. Interesting results exist in this direction (see for example [Hr] and work by Moriwaki [Mo]) but in the following we restrict ourselves to $\bar{\mathbb{Q}}$.

Extensions of Theorem 2 will be described in the third section. First, we sketch a proof of this theorem.

2 Vojta's method

Here we rely on Bombieri's rewriting of the proof with more elementary tools (see [Bo]). Let $\hat{h}$ be a Néron-Tate height on $A(\bar{\mathbb{Q}})$. We recall that $\hat{h}$ induces a positive definite quadratic form on $A(\bar{\mathbb{Q}}) \otimes \mathbb{R}$.

We divide the proof of Theorem 2 into three steps.

a) Inequality of heights

Here is the main ingredient in the proof.

Theorem 3 (Vojta). *There exist positive real numbers c_1, c_2 and c_3 such that*

$$\hat{h}(ax - y) \geq c_1^{-1}(a^2\hat{h}(x) + \hat{h}(y))$$

for any integer $a \geq c_2$ and points $(x, y) \in C(\bar{\mathbb{Q}})^2$ with $\hat{h}(x) \geq c_3$ and $\hat{h}(y) \geq a^2 c_3$.

This statement is really the technical heart of the proof. The details are quite involved but the general strategy is rather classical in diophantine approximation. It makes use of:

(i) Siegel's lemma to construct a small section of an invertible sheaf on $C \times C$ related to the height $\hat{h}(ax - y) - \varepsilon(a^2\hat{h}(x) + \hat{h}(y))$;

(ii) some local estimates for the derivatives of this section yielding the required inequality if the section vanishes with a sufficiently low order in (x, y);

(iii) Roth's lemma to show that, under the hypotheses on a and (x, y), the above order of vanishing cannot be too high.

b) Euclidean geometry

By assumption, the real vector space $\Gamma \otimes \mathbb{R}$ equipped with the norm $\sqrt{\hat{h}}$ is a (finite-dimensional) euclidean space. Simple geometrical considerations in this space together with the above inequality will show that, under the assumptions of Theorem 2, the height is bounded on the set $C(\bar{\mathbb{Q}}) \cap \Gamma$.

Indeed, if x and y in this set are such that $\hat{h}(x) \geq c_3$ and $\hat{h}(y) \geq (c_2+1)^2\hat{h}(x)$ and if a is the nearest integer to $\sqrt{\hat{h}(y)/\hat{h}(y)}$, the inequality of Theorem 3 can be translated into a lower bound of the angle between x and y (in terms of c_1). If we denote this bound by θ, we simply have to cover $\Gamma \otimes \mathbb{R}$ by cones in which any two points make an angle smaller than θ. In one of these cones, as soon as we can find one point x of our set with $\hat{h}(x) \geq c_3$ then any other has to satisfy $\hat{h}(y) \leq (c_2+1)^2\hat{h}(x)$. Since there are a finite number of cones, this proves the claim.

Notice that, though we can be more precise about the number of points of $C(\bar{\mathbb{Q}})\cap\Gamma$ of height at least c_3, this method offers no mean of bounding their height. Doing so is an open difficult problem usually known as "effective Mordell". The reasons for ineffectivity here are the same as in Roth's theorem.

c) Northcott's theorem

Once we know that the set $C(\bar{\mathbb{Q}}) \cap \Gamma$ is of bounded height, we very simply conclude the proof by Northcott's theorem since (see above) this set is defined over a certain number field.

These three steps are of course of inequal difficulties but we have given them in this way because we will encounter later the same pattern: an inequality of heights (technical part) gives the boundedness of the height on the given set through geometrical considerations and then another independent argument is needed to yield finiteness.

3 Generalisations of Theorem 2

We are now going to extend Theorem 2 that is, when replacing the boxed parts of the theorem as indicated, we obtain, unless otherwise specified, another theorem. In Theorem 4 below we will give a statement containing all the previous ones.

a) Variations on C

It is natural to look for higher dimensional versions of Theorem 2. We have to impose a condition extending the one on the genus. So we replace C by *any subvariety X which is not a translate of a subgroup of A* and we also replace the finiteness in the conclusion by the fact that the set is *not Zariski-dense.* In this form, the result was conjectured by Lang and proven by Faltings (see [F3]). It is also possible to retain finiteness with a stronger condition on X (as in [F2]) but an easy argument shows that this is contained in the statement we consider here.

b) Variations on A

We replace A by more general algebraic groups. Historically, the first case to be proven, by Laurent in 1984 (see [La]), was with a torus $A = \mathbb{G}^n_{m,\bar{\mathbb{Q}}}$. The proof (Vojta's method not being available yet!) relied on Schmidt's subspace theorem. Note that following the same lines a quantitative version was given by Evertse and Schlickewei (see [Ev]). Sharper bounds can now be obtained through Vojta's method (see [R3]).

It turns out that the statement can be further extended to a family of algebraic groups containing both abelian varieties and tori. We allow A to be a *semi-abelian variety*, that is, an extension of an abelian variety A_0 by a torus $\mathbb{G}^n_{m,\bar{\mathbb{Q}}}$:

$$0 \longrightarrow \mathbb{G}^n_{m,\bar{\mathbb{Q}}} \longrightarrow A \longrightarrow A_0 \longrightarrow 0.$$

The proof of the theorem in this semi-abelian case is due to Vojta (see [V3]). Here, A is no longer proper and one has to work with sheaves on a certain blow-up.

c) Variations on Γ

Modifying Γ really changes the nature of the problem.

• We start from the case of the set of all torsion points, that is: $\Gamma = A_{\mathrm{tors}}$. This is usually known (at least in the abelian case) as the Manin-Mumford conjecture and was proven by Raynaud (see [Ra]). We generalise this case in three directions.

• First, consider for Γ a finite rank subgroup (this means that $\Gamma \otimes \mathbb{Q}$ is a finite-dimensional vector space). Hindry (see [H1]) has shown how Faltings' result implies this in the abelian case and McQuillan (see [McQ]) has extended the argument to the semi-abelian case. Here we have indeed a generalisation of the Manin-Mumford conjecture (which deals with zero rank) and also of the initially considered case of a finitely generated subgroup. It had been also conjectured by Lang.

• Next, we look at points of small normalised height namely $\{x \in A(\bar{\mathbb{Q}}) \mid \hat{h}(x) \leq \varepsilon\}$ (in the abelian case $\hat{h}$ is a Néron-Tate height and this can be extended to the semi-abelian case — see for example [Po]). This type of question was first raised by Bogomolov and we call this a "Bogomolov property". The statement is that there exists a positive ε (small enough) such that the modified Theorem 2 holds. This fact is due to Zhang (see [Z1]) for abelian varieties and to David and Philippon (see [DP]) for semi-abelian varieties. We recover the Manin-Mumford conjecture with $\varepsilon = 0$.

• We mention a third, mainly open, possible generalisation of $\Gamma = A_{\mathrm{tors}}$. For some integer r, we let

$$\Gamma = \bigcup_{\dim B \leq r} B(\bar{\mathbb{Q}})$$

where the union runs through all algebraic subgroups B satisfying the dimension condition. It is clear that $r = 0$ is again Manin-Mumford. It is not at all so clear what other values of r are possible for a given subvariety X. This kind of problems was raised in 1999 in a paper by Bombieri, Masser and Zannier (see [BMZ]) where the case of a curve C in a torus $A = \mathbb{G}^n_{m,\bar{\mathbb{Q}}}$ is solved: we can take $r = n - 2$ (which is then easily seen to be optimal) if C is not contained in a translate of a proper algebraic subgroup of A (this is probably not optimal: one would like to say only "not contained in a proper algebraic subgroup of A"). The only other case known is due to Viada (see [Vi]) and deals with curves in E^n where E is an elliptic curve.

• Given the three preceding directions, one can try to blend then into unified results. Initially, the idea is due to Poonen (see [Po]) who conjectured that one can take

$$\Gamma = \Gamma'_\varepsilon := \{x + y \in A(\bar{\mathbb{Q}}) \mid x \in \Gamma' \text{ et } \hat{h}(y) \leq \varepsilon\}$$

where Γ' is a finite rank subgroup of $A(\bar{\mathbb{Q}})$ and ε small enough. He called his conjecture "Mordell-Lang plus Bogomolov" and was able to prove it for split semi-abelian varieties (so in particular for tori and abelian varieties); Zhang (see [Z3]) obtained independently the same result. Recently, we obtained the general case (see [R4]).

• Following the same line one could ask for results with Γ of the form

$$\Gamma = \bigcup_{\dim B \leq r} \Gamma'_\varepsilon + B(\bar{\mathbb{Q}})$$

combining everything. This is, as far as I know, completely open and I will not venture to propose a conjecture. However, it should be noted that this has some links with a far-reaching conjecture of Zhang (see [Z2]): roughly speaking, the case of curves here in certain abelian varieties would yield the case of constant families in Zhang's conjecture.

We conclude this section by a statement containing all the previous results (except those of [BMZ] and [Vi]) that is, "Mordell-Lang plus Bogomolov" in the semi-abelian case (proven in [R4]).

Theorem 4. *Let X be a subvariety of a semi-abelian variety A over $\bar{\mathbb{Q}}$ such that X is not the translate of a subgroup of A. Let Γ' be a finitely generated subgroup of $A(\bar{\mathbb{Q}})$. Then there exists $\varepsilon > 0$ such that the set $X(\bar{\mathbb{Q}}) \cap \Gamma'_\varepsilon$ is not Zariski-dense in X.*

4 Extensions of Vojta's method

We want to sketch how the method of Section 2 is used in the proof of (some of) the results quoted in Section 3. For the sake of simplicity, we deal only with abelian varieties from now on (but the general framework is the same in the semi-abelian case).

Let X be an integral subvariety of an abelian variety A. To mimic Section 2, we need finiteness instead of non-density. We therefore introduce the exceptional subset

$$Z_X = \bigcup_{x+B\subset X} x+B$$

defined as the union of translates contained in X of nonzero abelian subvarieties B of A. It can be shown that

- Z_X is a closed subset of X;
- $X = Z_X$ if and only if X is itself a translate of an abelian subvariety of A.

Thus, to prove the non-density of $X(\bar{\mathbb{Q}}) \cap \Gamma$, it is enough to prove the finiteness of $(X \setminus Z_X)(\bar{\mathbb{Q}}) \cap \Gamma$.

a) Inequality on $(X \setminus Z_X)(\bar{\mathbb{Q}})$

When points of Z_X are excluded, Theorem 3 can be generalised. We let $m = \dim X + 1$.

Theorem 5 (Faltings). *There exist positive real numbers c_1, c_2 and c_3 such that*

$$\sum_{i=1}^{m-1} \hat{h}(a_i x_i - a_{i+1}x_{i+1}) \geq c_1^{-1} \sum_{i=1}^{m} a_i^2 \hat{h}(x_i)$$

for any $a \in (\mathbb{N}\setminus\{0\})^m$ and m-tuple of points $x \in (X\setminus Z_X)(\bar{\mathbb{Q}})^m$ with $a_i/a_{i+1} \geq c_2$ and $a_i^2\hat{h}(x_i) \geq a_1^2 c_3$.

Without giving any precisions, let us say that this is again the technical part and that the strategy closely resembles the one used in Section 2 with an additional induction based on the product theorem of Faltings (instead of Roth's lemma). For a quantitative statement (values of c_1, c_2 and c_3) see [R1] and the introduction of [R5] for a slightly sharper inequality; the original result is due to Faltings and is described briefly in [F3]; details can be found for example in [EE], [H2], [R1] or [V2].

b) $\hat{h}$ is bounded on $(X \setminus Z_X)(\bar{\mathbb{Q}}) \cap \Gamma$

As in Section 2, this is a consequence of the inequality as soon as Γ can be covered by a finite number of small cones. This is the case:

1. obviously, if Γ is finitely generated (see Section 2);
2. by the same argument if Γ is of finite rank since $\Gamma \otimes \mathbb{R}$ is still finite-dimensional;

3. also when $\Gamma = \Gamma'_\varepsilon$; here, although the span of Γ is infinite-dimensional, we obtain a covering in the following way: first cover Γ' as above with cones defined with an angle θ; then choose ε small enough such that the cones defined with 2θ cover $\{x \in \Gamma \mid \hat{h}(x) \geq c_3\}$ (see [R4]).

c) Finiteness

We consider the same three cases:

1. again this is clear by Northcott's theorem;

2. originally Raynaud's method and its extensions (see [Ra], [H1] and [McQ]) used Galois arguments to reduce to the previous case. A different proof is obtained if one uses the next case.

3. here the points of Γ'_ε of height less than, say, c can be divided in finitely many small balls of radius 2ε. When ε is small enough, we can the apply the Bogomolov property to each of these balls to get finiteness. We need some uniformity to apply this argument, see [R4].

Let us say just one word about the proofs in [BMZ] and [Vi]. Here a direct argument is used to bound the height in the case of curves. Once the height is bounded, finiteness is obtained through good estimates in the direction of the generalised Lehmer problem proven in [AD] for tori and in [DH] for abelian varieties with complex multiplication. This second part seems to generalise in higher dimension but the first one looks specific to curves. Hence one can try to use Vojta's method to supply the boundedness of the height... The general formulation of the height inequality of the method given in [R5] may give some hope to do this...

References

[AD] F. Amoroso and S. David. Le problème de Lehmer en dimension supérieure. *J. Reine Angew. Math.* 513. 1999. p. 145–179.

[Bo] E. Bombieri. The Mordell conjecture revisited. *Ann. Scuola Norm. Sup. Pisa* Série IV. 17. 1990. p. 615–640. — Erratum. *Ann. Scuola Norm. Sup. Pisa* Série IV. 18. 1991. p. 473.

[BMZ] E. Bombieri, D. Masser and U. Zannier. Intersecting a curve with algebraic subgroups of multiplicative groups. *Internat. Math. Res. Not.* 20. 1999. p. 1119–1140.

[DH] S. David and M. Hindry. Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C. M. *J. Reine Angew. Math.* 529. 2000. p. 1–74.

[DP] S. David and P. Philippon. Sous-variétés de torsion des variétés semi-abéliennes. *C. R. Acad. Sci. Paris.* 331. 2000. p. 587–592.

[EE] B. Edixhoven and J.-H. Evertse. *Diophantine approximation and abelian varieties.* L.N.M. 1566. Springer-Verlag. 1994.

[Ev] J.-H. Evertse. Points on subvarieties of tori. *A Panorama in Number Theory or the View from Baker's Garden, Proc. Conf. Number Theory in honour of the 60th birthday of Prof. Alan Baker, Zurich 1999* (G. Wüstholz, ed.). Cambridge Univ. Press, 2002. p. 214–230.

[F1] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Inv. Math.* 73. 1983. p. 349–366. — Erratum. *Inv. Math.* 75. 1984. p. 381.

[F2] G. Faltings. Diophantine approximation on abelian varieties. *Ann. of Math.* 133. 1991. p. 549–576.

[F3] G. Faltings. The general case of S. Lang's conjecture. *Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991).* Perspect. Math. 15. Academic Press. San Diego. 1994. p. 175–182.

[H1] M. Hindry. Autour d'une conjecture de Serge Lang. *Inv. Math.* 94. 1988. p. 575–603.

[H2] M. Hindry. Sur les conjectures de Mordell et de Lang [d'après Vojta, Faltings et Bombieri]. *Astérisque.* 209. 1992. p. 39–56.

[Hr] E. Hrushovski. The Mordell-Lang conjecture for function fields. *J. Amer. Math. Soc.* 9. 1996. p. 667–690.

[La] M. Laurent. Équations diophantiennes exponentielles. *Invent. math.* 78. 1984. p. 299–327.

[McQ] M. McQuillan. Division points on semi-abelian varieties. *Invent. math.* 120. 1995. p. 143–159.

[Mo] A. Moriwaki. A generalization of conjectures of Bogomolov and Lang over finitely generated fields. *Duke Math. J.* 107. 2001. p. 85–102.

[Po] B. Poonen. Mordell-Lang plus Bogomolov. *Invent. math.* 137. 1999. p. 413–425.

[Ra] M. Raynaud. Sous-variétés d'une variété abélienne et points de torsion. *Arithmetic and geometry,* Vol. I. Progr. Math. 35. Birkhäuser. Boston. 1983. p. 327–352.

[R1] G. Rémond. Inégalité de Vojta en dimension supérieure. *Ann. Scuola Norm. Sup. Pisa* Série IV. 29. 2000. p. 101–151.

[R2] G. Rémond. Décompte dans une conjecture de Lang. *Invent. math.* 142. 2000. p. 513–545.

[R3] G. Rémond. Sur les sous-variétés des tores. *Compositio math.* 134. 2002. p. 337–366.

[R4] G. Rémond. Approximation diophantienne sur les variétés semi-abéliennes. *Ann. Sci. École Norm. Sup.* 2003 (to appear).

[R5] G. Rémond. Inégalité de Vojta généralisée. Preprint 2002.

[Vi] E. Viada. The intersection of a curve with abelian subvarieties in a product of elliptic curves. *Ann. Scuola Norm. Sup. Pisa* (to appear).

[V1] P. Vojta. Siegel's theorem in the compact case. *Ann. of Math.* 133. 1991. p. 509–548.

[V2] P. Vojta. Applications of arithmetic algebraic geometry to diophantine approximations. *Lecture Notes in Math.* 1553. Springer-Verlag. 1993. p. 164–208.

[V3] P. Vojta. Integral points on subvarieties of semiabelian varieties, I. *Invent. math.* 126. 1996. p. 133–181.

[Z1] S. Zhang. Equidistribution of small points on abelian varieties. *Ann. of Math.* 147. 1998. p. 159–165.

[Z2] S. Zhang. Small points and Arakelov theory. Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998). Doc. Math. 1998, Extra Vol. II; 217–225 (electronic).

[Z3] S. Zhang. Distribution of almost division points. *Duke Math. J.* 103. 2000. p. 39–46.

Gaël Rémond
Institut Fourier, UMR 5582
BP 74
38402 Saint-Martin-d'Hères Cedex
France
`Gael.Remond@ujf-grenoble.fr`