

AFFINE CURVES WITH INFINITELY MANY INTEGRAL POINTS

DIMITRIOS POULAKIS

(Communicated by Michael Stillman)

ABSTRACT. Let $C \subset \mathbf{A}^n$ be an irreducible affine curve of (geometric) genus 0 defined by a finite family of polynomials having integer coefficients. In this note we give a necessary and sufficient condition for C to possess infinitely many integer points, correcting a statement of J. H. Silverman (Theoret. Comput. Sci., 2000).

Let C be an irreducible affine curve of (geometric) genus 0 in the affine space \mathbf{A}^n defined by a finite family of polynomials having integer coefficients. We denote by $C(\mathbf{Z})$ the set of integral points on C . Let $\overline{\mathbf{Q}}$ be an algebraic closure of \mathbf{Q} and $\overline{\mathbf{Q}}(C)$ the function field of C . Let \overline{C} be the Zariski closure of C in the projective space \mathbf{P}^n and $C_\infty = (\overline{C} \setminus C)(\overline{\mathbf{Q}})$. We say that a discrete valuation ring U of $\overline{\mathbf{Q}}(C)$ lies at infinity if U dominates the local ring $O_P(C)$ at a point $P \in C_\infty$ (i.e. U contains $O_P(C)$ and the maximal ideal of U contains the maximal ideal of $O_P(C)$). We denote by Σ_∞ the set of discrete valuation rings at infinity. Note that Σ_∞ is essentially the set of points in the desingularization of C_∞ .

The main result of [5] is as follows:

Theorem A. *The set $C(\mathbf{Z})$ is infinite if and only if one of the following two conditions is satisfied:*

- (a) C_∞ consists of one point and $C(\mathbf{Z})$ contains at least one non-singular point.
- (b) C_∞ consists of two points which are conjugate over a real quadratic field and $C(\mathbf{Z})$ contains at least one non-singular point.

The “only if” part of Theorem A, in case $n = 2$, is a direct consequence of [4, Part I]. Unfortunately, the “if” part is not correct. One can easily see it by the following two counterexamples:

1. The equation $Y^2 = (X + 1)^2(X^2 + 15)$ defines a rational curve C with $C_\infty = \{(0 : 1 : 0)\}$. Furthermore the pair $(1, 8)$ is a non-singular point on C . Then Theorem A implies that $C(\mathbf{Z})$ is infinite. If (x, y) is an integer solution of the above equation, then $(x + 1) | y$ and so $y = (x + 1)z$, where z is an integer. It follows that $z^2 - x^2 = 15$ which clearly has finitely many solutions. We deduce that $(X, Y) = (1, \pm 8), (-1, 0), (7, \pm 64), (-7, \pm 48)$. Hence part (a) of Theorem A is not correct.

2. Let C be the rational curve defined by $f(X, Y) = (X^2 - 2Y^2)^2 + XY = 0$. Then $C_\infty = \{(\sqrt{2} : 1 : 0), (-\sqrt{2} : 1 : 0)\}$ and the couple $(1, -1)$ is a non-singular

Received by the editors March 19, 2001 and, in revised form, January 8, 2002.
2000 *Mathematics Subject Classification.* Primary 11G30, 14G25, 11D41.

point on C . By Theorem A it follows that $C(\mathbf{Z})$ is infinite. Let $x, y \in \mathbf{Z} - \{0\}$ with $f(x, y) = 0$. Set $d = \gcd(x, y)$. Then $x = dx', y = dy'$, where $x', y' \in \mathbf{Z}$ and $\gcd(x', y') = 1$. Thus $(d(x'^2 - 2y'^2))^2 = |x'y'|$, whence $|x'| = u^2, |y'| = v^2$ with $u, v \in \mathbf{Z}$ and $u > 0, v > 0$. It follows that $d(u^4 - 2v^4) = uv$ and since $\gcd(u^4 - 2v^4, uv) | 2$, we get $(u^4 - 2v^4) | 2$. By [1, Theorem 7, p. 207], the only integer solutions of $u^4 - 2v^4 = 1$ are $(u, v) = (\pm 1, 0)$. We easily see that the $u^4 - 2v^4 = 2$ has no integer solution. Using [1, Theorem 15, p. 274] we deduce that the only integer solutions of $u^4 - 2v^4 = -1$ are $(u, v) = (\pm 1, \pm 1)$. If $u, v \in \mathbf{Z}$ with $u^4 - 2v^4 = -2$, then $v^4 - 8(u')^4 = 1$, where $u = 2u'$ and $u' \in \mathbf{Z}$, and by [1, p. 208] we have $(v, u') = (\pm 1, 0)$. Thus we obtain that the only integer solutions of $f(X, Y) = 0$ are $(X, Y) = (0, 0), (1, -1), (-1, 1)$. Therefore part (b) of Theorem A is also not correct.

Note that it is possible for a curve C to verify (a) or (b) but at the same time to have more than two discrete valuations rings at infinity (as in the case of the second example) and so Siegel's finiteness theorem implies that $C(\mathbf{Z})$ is finite.

In [5] the author obtains a birational morphism defined over \mathbf{Q} ,

$$\phi : \mathbf{P}^1 \rightarrow \overline{C}, (s : t) \rightarrow (\phi_0(s, t) : \dots : \phi_n(s, t)),$$

where $\phi_i(S, T)$ are homogeneous polynomials of the same degree with integer coefficients. The error arose from the fact that the author considers that the sets C_∞ and $\{(s : t) \in \mathbf{P}^1(\overline{\mathbf{Q}}) : \phi_0(s, t) = 0\}$ have the same number of elements. This is correct in the case where all the points of C_∞ are non-singular, but if they are not, then it may not be true. Consider for example the rational curve $C : X^2 = Y^4 - 3Y^2$. It has only the point $(1 : 0 : 0)$ at infinity which is a cusp. It is easily seen that the projective closure of C defined by $X^2Z^2 = Y^4 - 3Y^2Z^2$ admits the following parametrization:

$$\begin{aligned} X(S, T) &= 2(S^2 - ST + T^2)(-S^2 + 4ST - T^2), \\ Y(S, T) &= 2(S^2 - ST + T^2)(S^2 - T^2), \\ Z(S, T) &= (S^2 - T^2)^2. \end{aligned}$$

The zeros of $Z(S, T)$ in \mathbf{P}^1 are $(\pm 1 : 1)$. Thus we see that C_∞ and $Z(S, T)$ do not have the same number of elements. Furthermore if (x, y) is an integer solution to the above equation, then $yz = x$, where z is an integer, and hence $y^2 - z^2 = 3$ which clearly has finitely many solutions. On the other hand, since $(2, 2)$ is a simple integer point on C and $|C_\infty| = 1$, part (a) of Theorem A yields that C has infinitely many integer points. Thus the above curve provides one other counterexample to Theorem A.

We call an element V of Σ_∞ defined over a subfield k of $\overline{\mathbf{Q}}$, if $\tau(V) = V$ for every $\tau \in \text{Gal}(\overline{\mathbf{Q}}/k)$. Furthermore two elements V and W of Σ_∞ are conjugate over a quadratic field k if V and W are defined over k and there is $\sigma \in \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which is not the identity on k such that $\sigma(V) = W$.

The statement of Theorem A can be corrected if we replace the set C_∞ by Σ_∞ . Thus we have the following result:

Theorem 1. *The set $C(\mathbf{Z})$ is infinite if and only if one of the following two conditions is satisfied:*

- (a) Σ_∞ consists of one element and $C(\mathbf{Z})$ contains at least one non-singular point.
- (b) Σ_∞ consists of two elements which are conjugate over a real quadratic field and $C(\mathbf{Z})$ contains at least one non-singular point.

For the proof of Theorem 1 we only need the following result:

Lemma 1. *The sets Σ_∞ and $\{(s, t) \in \mathbf{P}^1(\overline{\mathbf{Q}}) : \phi_0(s, t) = 0\}$ have the same number of elements.*

Proof. The proof is an easy generalisation of the proof of [2, Lemma 2.2].

Following Silverman's proof, replacing C_∞ by Σ_∞ and using Lemma 1, we deduce Theorem 1.

Remarks. 1) In [3, Theorem 5.1], there is a quick proof of Theorem 1 for $n = 2$.

2) In the proof in [5] of the "only if" part of Theorem A, the author, supposing that $C(\mathbf{Z})$ is infinite, claims that " C_∞ consists of at most two points, necessarily non-singular" (page 169, line 5). This claim is not correct. For a counterexample consider the curve $Y^3 = X$. It has infinitely many integer points and $(1 : 0 : 0)$ is its only point at infinity which is singular.

REFERENCES

- [1] L. J. Mordell, *Diophantine Equations*, Academic Press 1969. MR **40**:2600
- [2] D. Poulakis and E. Voskos, On the Practical Solution of Genus Zero Diophantine Equations, *J. Symbolic Computation* 30 (2000), 573-582. MR **2001j**:11126
- [3] D. Poulakis and E. Voskos, Solving genus zero diophantine equations with at most two infinite valuations, *J. Symbolic Computation* 33 (2002), 479-491.
- [4] A. Schinzel, An improvement of Runge's Theorem on diophantine equations, *Pontificia Acad. Sci.* 2 (1969), 1-9. MR **43**:1922
- [5] J. H. Silverman, On the distribution of integer points on curves of genus zero, *Theoret. Comput. Sci.* 235 (2000), no. 1, 163-170. MR **2001h**:11080

DEPARTMENT OF MATHEMATICS, ARISTOTLE UNIVERSITY OF THESSALONIKI, 54124 THESSALONIKI, GREECE

E-mail address: `poulakis@auth.gr`