ANNALES
POLONICI MATHEMATICI
88.1 (2006)

Integer points on a curve and the plane Jacobian problem

by NGUYEN VAN CHAU (Hanoi)

Abstract. A polynomial map $F = (P, Q) \in \mathbb{Z}[x, y]^2$ with Jacobian $JF := P_x Q_y - P_y Q_x \equiv 1$ has a polynomial inverse with integer coefficients if the complex plane curve $P = 0$ has infinitely many integer points.

1. Introduction. Let $F : \mathbb{C}^n \to \mathbb{C}^n$ be a polynomial map with integer coefficients, $F = (F_1, \dots, F_n) \in \mathbb{Z}[X_1, \dots, X_n]^n$. The mysterious Jacobian conjecture (JC) (see [BCW] and [E]), posed first by Keller in 1939 and still open even for the two-dimensional case, asserts that such a map F is invertible and has a polynomial inverse with integer coefficients if the Jacobian $JF := \det(\partial F_i/\partial X_j) \equiv 1$. K. McKenna and L. van den Dries in [DK] discovered the nice fact that every polynomial surjection of $\mathbb{Z}^n$ is an automorphism of $\mathbb{Z}^n$, which reduces Keller's problem to proving the surjectivity of such maps F. In this note we present the following.

THEOREM 1. *Let $F = (P, Q) : \mathbb{C}^2 \to \mathbb{C}^2$ be a polynomial map with integer coefficients, $F = (P, Q) \in \mathbb{Z}[x, y]^2$, and $JF \equiv 1$. If the complex plane curve $P = 0$ has infinitely many points in $\mathbb{Z}[i]^2$, then F has a polynomial inverse with integer coefficients.*

Here, as usual, $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$ and the elements of $\mathbb{Z}[i]^n$ are called *integer points.*

In the proof of Theorem 1 presented in §4 we will show that if $F = (P, Q)$ is not invertible, then the numbers of integer points lying on the curves $P = c$, $c \in \mathbb{Z}[i]$, must be uniformly bounded. This fact will be deduced from Proposition 1 of §3, which gives a plane version of van den Dries's result (see [CD] and [E]) on the behavior of integer counterexamples to (JC). In view of Siegel's theorem [Sie], which states that there are only finitely many integer points on a curve of genus $g \geq 1$, if the complex plane curve $P = 0$ has

2000 *Mathematics Subject Classification*: Primary 14R15.
Key words and phrases: exceptional value set, Jacobian conjecture, Keller's question.
Supported in part by the National Basic Program on Natural Science, Vietnam, and ICTP, Trieste, Italy.

infinitely many points in $\mathbb{Z}[i]^2$, at least one of its irreducible components is a rational curve. Part of the plane Jacobian conjecture is the question *whether a polynomial map* $f = (p, q) \in \mathbb{C}[x, y]^2$ *with* $Jf \equiv c \in \mathbb{C}^*$ *is invertible if the curve* $p = 0$ *has an irreducible component which is a rational curve.* It has only been known that such a map f is invertible if the curve $p = 0$ has an irreducible component homeomorphic to $\mathbb{C}$ or if all fibers of p are irreducible and the generic fiber of p is a rational curve (see [R], [LW] and [NN]).

2. Lemma on partial inverse. We consider a given $F : \mathbb{C}^n \to \mathbb{C}^n$, $(F_1, \dots, F_n) \in \mathbb{C}[X_1, \dots, X_n]^n$, with $F(0) = 0$ and $JF \equiv c \in \mathbb{C}^*$. In view of the implicit function theorem the map F has a unique local analytic inverse $G(Y) = (G_1, \dots, G_n)(Y)$ defined on an open neighborhood W of 0 for which $G(0) = 0$ and

$$F \circ G(Y) = Y, \qquad G \circ F(X) = X, \qquad Y \in W,\ X \in G(W). \tag{1}$$

Furthermore, the components G_i of G are power series in variables $Y = (Y_1, \dots, Y_n)$ with complex coefficients and the identities in (1) hold in the sense of formal series.

The following lemma, which will be used in the next section, may be of independent interest.

LEMMA 1. *Let* $1 \le k \le n$ *be fixed and* $L := \{y \in \mathbb{C}^n : y_j = 0, j = k+1, \dots, n\}$. *If* $G_i(Y_1, \dots, Y_k, 0, \dots, 0)$, $i = 1, \dots, n$, *are polynomials*, *then*

(i) *the map* $g : L \to g(L) \subset \mathbb{C}^n$ *defined by*

$$g(y_1, \dots, y_k, 0, \dots, 0) := G(y_1, \dots, y_k, 0, \dots, 0)$$

is an isomorphism,

(ii) *the inverse of* g *is the restriction* f *of* F *to the image* $g(L)$,

(iii) *if* $n = 2$ *and* $k = 1$, *then the map* F *is invertible and* $F^{-1} = G$.

Proof. First, we will prove (i) and (ii). Let V be the connected component of $F^{-1}(L)$ containing the origin 0. Since $JF \equiv c \in \mathbb{C}^*$, $F^{-1}(L)$ is a nonsingular algebraic set of dimension k, and hence V is a nonsingular irreducible algebraic set of dimension k. Let F_V be the restriction of F to V. As the components $G_i(Y_1, \dots, Y_k, 0, \dots, 0)$, $i = 1, \dots, n$, are polynomials, the maps $F_V \circ g$ and $g \circ F_V$ are well defined and are regular morphisms. Furthermore, by (1) we have $F_V \circ g = \mathrm{id}_L$ on $L \cap W$ and $g \circ F_V = \mathrm{id}_V$ on $V \cap G(W)$. As L and V are nonsingular irreducible algebraic sets of dimension k, it follows that

$$F_V \circ g = \mathrm{id}_L, \qquad g \circ F_V = \mathrm{id}_V$$

and

$$g(L) = V, \qquad f = F_V.$$

Hence, we get the conclusions (i) and (ii).

Now, we consider the case $n = 2$ and $k = 1$. By (i) and (ii) the maps $g : L \to \mathbb{C}^2$ and $f : g(L) \to \mathbb{C}^2$ are embeddings. Applying the Abhyankar–Moh–Suzuki Theorem on embeddings of the line into the plane (see [AM], [S]), we can find new affine coordinates of $\mathbb{C}^2$ in which $g(L)$ is a line. Thus, F maps the line $g(L)$ one-to-one to the line L, as f is the restriction of F to $g(L)$. Then F is invertible and $F^{-1} = G$ by the well known fact (see [G], [E]) that a non-zero constant Jacobian polynomial map of $\mathbb{C}^2$ is invertible if it sends a line one-to-one into the plane (this results from an application of the Abhyankar–Moh–Suzuki Theorem and the similarity of Newton polygons of components of Jacobian pairs). ∎

3. A plane version of van den Dries's result. Van den Dries (see [CD] and [E]) observed that if $F \in \mathbb{Z}^n[X]$ is a counterexample to (JC) and $JF \equiv 1$, then F will map the lattice $\mathbb{Z}[i]^n$ into a narrow neighborhood of its exceptional value set A_F, namely

$$\mathrm{Dist}(F(p), A_F) \le 1 \quad \text{for all } p \in \mathbb{Z}[i]^n, \tag{2}$$

where

$$\mathrm{Dist}(p, V) := \inf_{q\in V} \max_{i=1,\dots,n} |p_i - q_i|$$

and the *exceptional value set* of F is the smallest subset $A_F \subset \mathbb{C}^n$ such that the restriction $F : \mathbb{C}^n \setminus F^{-1}(A_F) \to \mathbb{C}^n \setminus A_F$ gives an unbranched covering.

The following gives a version of the above-mentioned result for the plane case. For points $q = (a, b) \in \mathbb{C}^2$ and a subset $V \subset \mathbb{C}^2$ we define

$$\widehat{d}(q, V) := \max(\min\{|a - u| : (u, b) \in V\}, \min\{|b - v| : (a, v) \in V\}).$$

Here, by convention, $\max\{\emptyset\} := +\infty$. Clearly, $\mathrm{Dist}(q, V) \le \widehat{d}(q, V)$.

PROPOSITION 1. *Let $F = (P, Q) \in \mathbb{Z}[x, y]^2$ with $JF \equiv 1$. If F is not invertible, then*

$$\widehat{d}(F(p), A_F) \le 1 \quad \textit{for all } p \in \mathbb{Z}[i]^2. \tag{3}$$

Proof. Assume the contrary that there is a point $(a, b) \in \mathbb{Z}[i]^2$ such that $\widehat{d}(F(a, b), A_F) > 1$, for instance,

$$\min\{|P(a, b) - u| : (u, Q(a, b)) \in A_F\} > 1. \tag{4}$$

Instead of F, we consider the map $\overline{F} = (\overline{P}, \overline{Q})$ given by $\overline{F}(x, y) := F(x + a, y+b) - F(a, b)$. As $(a, b) \in \mathbb{Z}[i]^2$ and $F \in \mathbb{Z}[x, y]^2$ with $JF \equiv 1$, one can verify that $\overline{F} \in \mathbb{Z}[i][x, y]^2$, $J\overline{F} \equiv 1$, $\overline{F}(0, 0) = (0, 0)$ and, like F, $\overline{F}$ is not invertible. Furthermore, $A_{\overline{F}} = A_F - F(a, b)$ and $\min\{|P(a, b) - u| : (u, Q(a, b)) \in A_F\} = \min\{|u| : (u, 0) \in A_{\overline{F}}\}$. Hence, by (4),

$$\min\{|u| : (u, 0) \in A_{\overline{F}}\} > 1.$$

It follows that there are numbers $r > 1$ and $s > 0$ small enough such that the set $A_{\overline{F}}$ does not intersect the box $B := \{(u, v) \in \mathbb{C}^2 : |u| < r,\ |v| < s\}$.

Now, let $G(u, v) = (R(u, v), S(u, v))$ be the local inverse of $\overline{F}$ at $(0, 0)$, $G(0, 0) = (0, 0)$, $\overline{F} \circ G(u, v) = (u, v)$ on a neighborhood W of $(0, 0)$ and $R(u, v)$ and $S(u, v)$ are convergent power series in W. Since $\overline{F} : \mathbb{C}^2 \setminus \overline{F}^{-1}(A_{\overline{F}}) \to \mathbb{C}^2 \setminus A_{\overline{F}}$ is an unbranched covering and B is an open simply connected set with $B \cap A_{\overline{F}} = \emptyset$, the local inverse G of $\overline{F}$ can be extended analytically over the box B. It follows that the power series $R(u, 0)$ and $S(u, 0)$ are convergent for $|u| < r$. As $R(u, 0)$ and $S(u, 0)$ are power series with coefficients in $\mathbb{Z}[i]$ and $r > 1$, $R(u, 0)$ and $S(u, 0)$ must be polynomials in u. Hence, by applying Lemma 1 we find that $\overline{F}$ is invertible, which contradicts the assumption. ∎

Remark 1. As shown in [E, p. 262], there exist dominant mappings F of $\mathbb{C}^n$ which satisfy van den Dries's estimate. One of such maps is the map $F = (P, Q)$, where

$$P(x, y) = x^6y^4 + x^2y, \qquad Q(x, y) = x^9y^6 + 3x^5y^3 + 3x,$$

given by Makar–Limanov. For this map $A_F = \{u = 0\} \cup \{u^3 - v^2 = 0\}$, $P(x, y) = s^2 - (xy)^{-2}$ and $Q(x, y) = s^3 - (xy)^{-3}$, where $s := x^3y^2 + (xy)^{-1}$. Then $\mathrm{Dist}(F(x, y), A_F) = 0$ for $x = 0$ or $y = 0$ and $\mathrm{Dist}(F(x, y), A_F) \le \mathrm{Dist}(F(x, y), (s^2, s^3)) \le 1$ for $(xy)^{-1} < 1$. Hence,

$$\mathrm{Dist}(F(x, y), A_F) \le 1 \quad \text{ for all } (x, y) \in \mathbb{Z}[i]^2.$$

However, this map does not satisfy the estimate (3). Indeed, for $(x, y) = (1, 1)$, $F(1, 1) = (3, 7)$ and the line $u = 3$ intersects A_F at $(3, 3\sqrt{3})$ and $(3, -3\sqrt{3})$. So, $\widehat{d}(F(1, 1), A_F) > 1$, since

$$\min\{|7 - v| : (3, v) \in A_F\} = 7 - 3\sqrt{3} > 1.$$

4. Proof of Theorem 1. Let $k \in \mathbb{Z}[i]$ and denote by $I(P, k)$ the set of all integer points lying on the curve $P = k$, $I(P, k) := \{P = k\} \cap \mathbb{Z}[i]^2$. Theorem 1 follows directly from the following lemma.

Lemma 2. *Let $F = (P, Q) \in \mathbb{Z}[x, y]^2$ with $JF \equiv 1$. If F is not invertible, then the numbers $\#I(P, k)$, $k \in \mathbb{Z}[i]$, must be uniformly bounded*:

$$\max_{k \in \mathbb{Z}[i]} \#I(P, k) < \infty.$$

Proof. Since F is not invertible, $A_F \neq \emptyset$ and is an algebraic curve in $\mathbb{C}^2$ (see for example [J]). Let $\mathrm{Deg}\, A_F$ be the degree of the curve A_F and $\deg_{\mathrm{geo}} F$ be the topological degree of F, that is, $\deg_{\mathrm{geo}} F = \#F^{-1}(p)$ for generic points $p \in \mathbb{C}^2$. As $JF \equiv 1$, we have $\deg_{\mathrm{geo}} F \ge \#F^{-1}(p)$ for all $p \in \mathbb{C}^2$.

Now, fix a number $k \in \mathbb{Z}[i]$. Denote by L the line $\{(u, v) \in \mathbb{C}^2 : u = k\}$ and by D the disk $\{(0, c) \in \mathbb{C}^2 : |c| \le 1\}$. Then in view of Proposition 1 we have

$$I(P,k) \subset F^{-1}\Big(\bigcup_{p \in L \cap A_F} ((p+D) \cap \mathbb{Z}^2[i]) \Big).$$

It is easy to see that none of the sets $(p+D) \cap \mathbb{Z}^2[i]$ has more than five points. So, we get

$$\#I(P,k) \le 5 \deg_{\mathrm{geo}} F \cdot \#(L \cap A_F).$$

The number $\#(L \cap A_F)$ cannot be larger than the intersection number of the line L and the curve A_F, except for the situation $L \subset A_F$. However, such a situation is impossible, since the irreducible components of A_F cannot be isomorphic to a line (see [C1]). Hence, we obtain

$$\#I(P,k) \le 5 \deg_{\mathrm{geo}} F \operatorname{Deg} A_F. \ \blacksquare \tag{5}$$

REMARK 2. Examining the intersection $L \cap A_F$ more carefully and using the results of [C1], one can improve the bound in (4). In fact, we can get

$$\#I(P,k) < 5 \deg_{\mathrm{geo}} F \deg P \, \frac{\gcd(\deg P, \deg Q) - 1}{\gcd(\deg P, \deg Q)}. \tag{6}$$

REMARK 3. One may ask for which curves $h = 0$ the set $I(h \circ F, 0)$ is finite. If $h = 0$ is not such a curve, the curve $h \circ F = 0$ must have a branch at infinity γ which contains infinitely many integer points. Then the branch $F(\gamma)$, which is a branch at infinity of $h = 0$, must be very close to branches at infinity of the curve A_F. Using the description of A_F in [C2], we can see that if $(P,Q) \in \mathbb{Z}[x,y]^2$ is a counterexample to (JC), then $\#I(h \circ F, 0) < \infty$ for almost all curves $h = 0$ homeomorphic to $\mathbb{C}$.

To conclude the paper we remark that both Theorem 1 and Proposition 1 remain true if one replaces the ring $\mathbb{Z}[i]$ by subrings R of the ring of integers of a quadratic number field of the form $\mathbb{Q}(i\sqrt{m})$. In fact, in our arguments to prove Theorem 1 and Proposition 1 the only fact on $\mathbb{Z}[i]$ used is that every power series with coefficients in $\mathbb{Z}[i]$ and convergence radius larger than 1 must be a polynomial. This fact is also true for power series with coefficients in such a ring R (see [E]).

Acknowledgments. The author wishes to thank Prof. A. van den Essen for many valuable suggestions and useful discussions.

References

[A] S. S. Abhyankar, *Expansion Techniques in Algebraic Geometry*, Tata Inst. Fund. Res., 1977.

[AM] S. S. Abhyankar and T. T. Moh, *Embeddings of the line in the plane*, J. Reine Angew. Math. 276 (1975), 148–166.

[BCW] H. Bass, E. Connell and D. Wright, *The Jacobian conjecture: reduction of degree and formal expansion of the inverse*, Bull. Amer. Math. Soc. 7 (1982), 287–330.

[CD] E. Connell and L. van den Dries, *Injective polynomial maps and the Jacobian conjecture*, J. Pure Appl. Algebra 28 (1983), 235–239.

[C1] Nguyen Van Chau, *Non-zero constant Jacobian polynomial maps of* $\mathbb{C}^2$, Ann. Polon. Math. 71 (1999), 287–310.

[C2] —, *Note on the Jacobian condition and non-proper value set*, ibid. 84 (2004), 203–210.

[DK] L. van den Dries and K. McKenna, *Surjective polynomial maps, and a remark on the Jacobian problem*, Manuscripta Math. 67 (1990), 1–15.

[E] A. van den Essen, *Polynomial Automorphisms and the Jacobian Conjecture*, Progr. Math. 190, Birkhäuser, Basel, 2000.

[G] J. Gwoździewicz, *Injectivity on one line*, Bull. Soc. Sci. Łódź Sér. Rech. Déform. 15 (1993), 59–60.

[J] Z. Jelonek, *The set of points at which a polynomial map is not proper*, Ann. Polon. Math. 58 (1993), 259–266.

[LW] Le Dung Trang et C. Weber, *Polynômes à fibres rationnelles et conjecture jacobienne à 2 variables*, C. R. Acad. Sci. Paris Sér. I Math. 320 (1995), 581–584.

[NN] W. D. Neumann and P. Norbury, *Nontrivial rational polynomials in two variables have reducible fibres*, Bull. Austral. Math. Soc. 58 (1998), 501–503.

[R] M. Razar, *Polynomial maps with constant Jacobian*, Israel J. Math. 32 (1979), 97–106.

[Sie] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Deutsch. Akad. Wiss. Berlin Phys.-Math. Kl. 1929, no. 1; Gesammelte Abhandlungen, Band I, Springer, 1966, 209–266.

[S] M. Suzuki, *Propriétés topologiques des polynômes de deux variables complexes et automorphismes algébriques de l'espace* $\mathbb{C}^2$, J. Math. Soc. Japan 26 (1974), 241–257.

Institute of Mathematics
18 Hoang Quoc Viet Road
10307 Hanoi, Vietnam
E-mail: nvchau@math.ac.vn

Received 23.6.2005
and in final form 27.10.2005 (1593)