ACTA ARITHMETICA
LXXVIII.2 (1996)

Remarks on a question of Skolem about the integer solutions of $x_1x_2 - x_3x_4 = 1$

by

Umberto Zannier (Venezia)

Introduction. We discuss here a problem raised by a remark due to Skolem, appearing in [Sko], p. 23, Bemerkung 1, concerning the integer solutions of the equation

$$x_1x_2 - x_3x_4 = 1. \tag{1}$$

He pointed out that it seemed unlikely that all the integral solutions could be obtained from a fixed polynomial parametrization of (1) by letting the variables run through all integers (actually Skolem considered the more general equation $\det(x_{ij}) = 1$, $1 \le i, j \le n$). Observe (cf. [Sz]) that we can find infinitely many polynomial solutions of (1) with coefficients in $\mathbb{Z}$ by considering the generic continued fractions $a_0 + \frac{1}{a_1 +} \ldots \frac{1}{a_n}$ where the a_i are variables. As is well known, we can write the value of such fraction as p_n/q_n, where p_n, q_n are polynomials in the a_i's satisfying $p_{n+1}q_n - q_{n+1}p_n = (-1)^n$. However, no such formula produces all integral solutions of $x_1x_2 - x_3x_4 = 1$ by letting the a_i run through all integers: in fact, it can be easily shown by induction on n that, if the $a_i \in \mathbb{Z}$, the rational number p_n/q_n has a continued fraction expansion with a number of terms bounded by a function of n only. (These references and remarks were pointed out to me by A. Schinzel.)

In the present note we shall prove Skolem's expectation under the assumption (apparently very strong, but see Remarks 3, 4 and Example 1 below) that the polynomials appearing in the parametrization depend on three variables only (i.e. like the dimension of the quadric defined by (1)); actually, we shall argue over any number field k, with ring of integers $\mathcal{O}_k$. We have the following

Theorem 1. *Given a finite number of polynomial solutions of* (1) $x_i = p_i^{(j)} \in k[t_1, t_2, t_3]$, $j = 1, \ldots, h$, *there exist numerical solutions of* (1), $(a_1, a_2, a_3, a_4) \in \mathcal{O}_k^4$ *which cannot be obtained from any of the polynomial ones by specializations of the* t_i*'s to integers in* $\mathcal{O}_k$.

We shall deduce Theorem 1 from Theorem 2 below, which leads to similar statements for more general varieties.

With no restriction on the number of variables in the parametrization, we have strong evidence that the result should not be true for general fields k; more precisely, relating the question with Artin's conjecture on primitive roots, we shall point out in Remark 3 how the truth of the Generalized Riemann Hypothesis implies the existence of counterexamples to the analogue for $\mathbb{Z}[\sqrt{2}]$ of Skolem's belief, already allowing five variables. (The method actually works for any k which is neither the rational field nor an imaginary quadratic field.)

This fact also says that no refinement of our method, which works for rings of integers of any number field k, can possibly provide a complete answer to Skolem's feeling, which, if correct, seems to depend on peculiar properties of $\mathbb{Z}$ compared to general $\mathcal{O}_k$ (like e.g. the structure of units). Actually, it is possible that the example of Remark 3, for the field $\mathbb{Q}(\sqrt{2})$ and five variables, gives as a byproduct an example over the rational field, in ten variables. We shall briefly explain this in Remark 4, pointing out the connection of the problem with a simply stated general question on polynomial ideals.

On the other hand, it would be interesting to sharpen the theorem by allowing the polynomials to depend on four variables. Of course this would be conjecturally best possible, in view of the above remarks. We conclude this section with two examples illustrating what can happen in this respect for other simple equations.

EXAMPLE 1. Take $\mathcal{V}$ to be the affine cone with equation $x^2 + y^2 = z^2$. It is easy to see (using e.g. the well known formulae recalled below), that $\mathcal{V}$ satisfies assumption VW of Theorem 2 below: namely, roughly speaking there are integral points satisfying any compatible congruence condition. Also, $\mathcal{V}$ is normal and not isomorphic to affine space. Nevertheless, the formulas $x = 2abc, y = (a^2-b^2)c, z = (a^2+b^2)c$ and the similar one obtained by interchanging x, y, produce all the integral solutions by letting a, b, c run through $\mathbb{Z}$. This shows that we cannot in general expect results like Theorem 1 (or Theorem 2) allowing more variables than the dimension. In this example $\mathcal{V}$ is not smooth, however. I do not know to what extent the existence of singularities can influence the conclusions in the general case.

EXAMPLE 2. In contrast with Example 1, we sketch a proof that, for the variety $\mathcal{V}$ defined by $z^2 = 1 + xy$, its points over $\mathbb{Z}$ cannot be obtained from any number of parametrizations *defined over* $\mathbb{Q}$ ([1]), even if we allow *three* variables. The argument (like Remark 3!) is related to the lack of units of $\mathbb{Z}$.

([1]) This restriction can be eliminated.

Assume the contrary and let $\phi := (\phi_1, \phi_2, \phi_3)$ be one of the relevant parametrizations, where the $\phi_i \in \mathbb{Q}[t_1, t_2, t_3]$. Considering the equation $(\phi_3 - 1)(\phi_3 + 1) = \phi_1\phi_2$ we easily see that, for some $\alpha, \beta, \delta, \eta \in \mathbb{Q}[t_1, t_2, t_3]$ such that $\alpha\eta - \beta\delta = 2$, we have $\phi_1 = \alpha\delta, \phi_2 = \beta\eta, \phi_3 = \beta\delta + 1$ ([2]). Choose now rational integers r, s, d, e with $re - sd = 2$. Then $(rd, se, sd + 1)$ lies on $\mathcal{V}(\mathbb{Z})$, so it is in $\phi(\mathbb{Z})$ for some ϕ as above, taken from a finite set. Comparing with the above equations it is now easy to see that, for some integer a, taken from a finite set ([3]), (r, s, d, e) lies in the image on $\mathbb{Z}^3$ of $(a\alpha, a\beta, a^{-1}\delta, a^{-1}\eta)$. So all the integer solutions of $xy - zw = 2$ could be obtained from a finite number of polynomial parametrizations in three variables, in contradiction with the obvious analogue of Theorem 1 (which follows in the same way from Theorem 2, and has not been stated for simplicity).

Proofs. Before stating Theorem 2 we introduce some notation and a couple of definitions. For k a number field, we let Σ_k be the set of its places. For $v \in \Sigma_k$, k_v will denote, as usual, the completion of k with respect to v. We will denote with $\mathcal{O}_v = \mathcal{O}_{k,v}$ the valuation ring of k_v. For an affine variety $\mathcal{V} \subset \mathbb{A}^n$ and a ring R, we shall denote by $\mathcal{V}(R)$ the set of points of $\mathcal{V}$ with coordinates in R.

Definition 1. Let $\mathcal{V}$ be an affine variety defined over a number field k. We say that $\mathcal{V}$ has the *weak approximation property* for a finite set S of places if $\mathcal{V}(\mathcal{O}_k)$ is dense in $\prod_{v\in S} \mathcal{V}(\mathcal{O}_v)$. We say that $\mathcal{V}$ has the *very weak approximation property* (denoted by VW) if there exists a finite set S_0 of places of k such that $\mathcal{V}$ has the weak approximation property for every finite set S disjoint from S_0.

This definition is essentially copied from Def. 3.5.6, p. 29 of [Se], which however refers to projective (instead of affine) varieties and rational (instead of integral) points. From [Se], p. 19, we recall another definition.

Definition 2. A subset $A \subset \mathcal{V}(k)$ is of *type* (C1) if it is not Zariski dense in $\mathcal{V}$, of *type* (C2) if there is a variety $\mathcal{V}'$ with $\dim \mathcal{V}' = \dim \mathcal{V}$ and a generically surjective morphism $\pi : \mathcal{V}' \to \mathcal{V}$ of degree ≥ 2 with $A \subset \pi(\mathcal{V}'(k))$. Finally, A is called *thin* if it is contained in a finite union of sets of type (C1) or (C2).

We have the following result (which could be stated in a more general form with $\mathbb{A}^d$ replaced by another d-dimensional affine variety).

Theorem 2. *Let $\mathcal{V} \subset \mathbb{A}^n$ be an affine normal variety of dimension d, defined over k and satisfying VW. Let $\Phi_1, \ldots, \Phi_h : \mathbb{A}^d \to \mathcal{V}$ be morphisms.*

([2]) E.g. put $\delta := \gcd(\phi_1, \phi_3 - 1)$ etc.

([3]) Here we use the fact that $\mathbb{Z}$ has finitely many units.

Suppose that $\mathcal{V}(\mathcal{O}_k)$ is contained in the union of $\Phi_j(\mathcal{O}_k^d)$, $1 \le j \le h$. Then some Φ_j is an isomorphism defined over k.

Note that normality is relevant: without that assumption, the data $k = \mathbb{Q}$, $\mathcal{V} = \{(x,y) : y^2 = x^3\}$, $\Phi_1 : \mathbb{A}^1 \to \mathcal{V}$, $\Phi_1(t) = (t^2, t^3)$, provide a counterexample, as is easy to verify.

We let $\mathcal{Q}$ be the affine quadric defined by (1). It is a nonsingular, whence normal, variety. Hence Theorem 1 follows at once from Theorem 2 and the next two lemmas. The content of Lemma 1 is certainly known, but, lacking a reference, we give the very short proof.

LEMMA 1. *$\mathcal{Q}$ satisfies VW.*

Proof. We take S_0 to be the set of archimedean places of k. Then, in view of the Chinese theorem, it plainly suffices to prove the following: *Let $a, b, c, d, M \in \mathcal{O}_k$ and let $ab - cd \equiv 1 \pmod{M}$. Then there exists $(a^*, b^*, c^*, d^*) \in \mathcal{Q}(\mathcal{O}_k)$ such that $(a^*, b^*, c^*, d^*) \equiv (a, b, c, d) \pmod{M}$.* To see this we first observe that $(a, c, M)\mathcal{O}_k = 1$, so, replacing if necessary a with $a + tM$ (for a suitable $t \in \mathcal{O}_k$), we may in fact assume $(a, c)\mathcal{O}_k = 1$. Put $ab - cd = 1 + qM$, $q \in \mathcal{O}_k$ and find $x, y \in \mathcal{O}_k$ with $ax - cy = q$. Then $a(b - xM) - c(d - yM) = 1$, proving what is needed. ∎

LEMMA 2. *The affine quadric $\mathcal{Q}$ defined by* (1) *is not isomorphic to affine* 3*-space, even over* $\mathbb{C}$.

This is probably well known (in any dimension, for affine quadrics equivalent to $\sum_{i=1}^n x_i^2 = 1$), but I have no reference for a direct proof. Here are two simple arguments.

Assume the contrary. Then there exists a morphism $\mathbf{f} : \mathbb{A}^3 \to \mathcal{Q}$ such that its inverse $\mathbf{g}$ is a regular function on $\mathcal{Q}$, namely given by polynomials in the coordinates $x_1, \dots, x_4$. Now, this amounts to the fact that certain equations in the coefficients of the relevant polynomials have a complex solution. By the Nullstellensatz, these equations have already a solution over some number field k. If p is a large prime number and π is a prime ideal in $\mathcal{O}_k$ lying above p, we can reduce the coefficients modulo π, producing an isomorphism of $\mathcal{Q}$ with affine space, defined over some finite field $\mathbb{F}_q$, say. Now we use a suggestion of D. Zagier: the existence of that isomorphism would imply in particular that the two relevant varieties have the same number of points over $\mathbb{F}_q$, so it suffices to prove this is not true (we are using the zeta function as an invariant). Formulas can be computed at once in our case. Affine 3-space has q^3 points over $\mathbb{F}_q$. As to $\mathcal{Q}$, we have plainly

$$\#\mathcal{Q}(\mathbb{F}_q) = \#\mathrm{SL}_2(\mathbb{F}_q) = \frac{1}{q-1}\#\mathrm{GL}_2(\mathbb{F}_q) = (q^2 - 1)q,$$

proving what is needed.

For the second argument (which will be useful in connection with Remark 2), observe first that by a linear transformation with complex coefficients the equation for $\mathcal{Q}$ may be brought in the form $x_1^2 + \ldots + x_4^2 = 1$. Consider the differential form on $\mathcal{Q}$

$$\omega := \frac{dx_1 \wedge dx_2 \wedge dx_3}{x_4}.$$

Observe that ω is regular throughout on $\mathcal{Q}$. In fact, differentiating the defining equation we have $x_1dx_1 + \ldots + x_4dx_4 = 0$ whence, for all j, $\omega = \pm(1/x_j)\bigwedge_{i\neq j} dx_i$. Since $\mathcal{Q}$ is plainly covered by its intersection with the sets where $x_j \neq 0$ we get the assertion.

Since ω has maximal dimension (as a holomorphic form), it is certainly closed. If on the other hand it were exact, its integral over the real part of $\mathcal{Q}$, namely over the sphere S^3, would be zero, in view of the Stokes theorem; we shall now show that this is not the case. In particular this will prove that $\mathcal{Q}$ is not homeomorphic to affine 3-space. Also, the argument automatically proves that S^3 has nontrivial homology class in $H_3(\mathcal{Q})$ ([4]).

We can transform ω by using the rational parametrization of $\mathcal{Q}$ obtained by intersecting it with the pencil of lines through the point $P := (0,0,0,1)$. The parametrization takes the form

$$x_i = -\frac{2w_i}{\sigma+1} \quad \text{for } i < 4, \quad x_4 = \frac{\sigma-1}{\sigma+1}$$

where $\sigma := w_1^2 + w_2^2 + w_3^2$. The inverse, defined on $\mathcal{Q} \setminus \{P\}$, is given by $w_i = x_i/(x_4 - 1)$. In particular, this provides a 1-1 C^∞ map from $\mathbb{R}^3$ to $S^3 \setminus \{P\}$, which can be used for the computation of the above mentioned integral. We find, after some computations,

$$dx_1 \wedge dx_2 \wedge dx_3 = x_4\left(\frac{2}{\sigma+1}\right)^3 dw_1 \wedge dw_2 \wedge dw_3.$$

Using the above parametrization we therefore find

$$\int_{S^3} \omega = \int_{\mathbb{R}^3} \left(\frac{2}{\sigma+1}\right)^3 dw_1 \wedge dw_2 \wedge dw_3 \neq 0$$

as wanted ([5]). ∎

Before proving Theorem 2 we need another lemma.

([4]) This fact in turn implies that e.g. there is no morphism $\phi : \mathbb{A}^4 \to \mathcal{Q}$ which is the identity on $\mathcal{Q}$: otherwise $\mathcal{Q}$ would be a retract of affine 4-space, whence would have trivial homology. Of course the existence of such a morphism would produce a parametrization of all integral points.

([5]) It seems not obvious how to prove algebraically that ω is not exact.

LEMMA 3. *Let A be a thin subset of $\mathcal{V}(k)$ and let S_0 be a finite set of places of k. Then there exists a finite set $S \subset \Sigma_k$, disjoint from S_0, such that the image of A in $\prod_{v\in S}\mathcal{V}(\mathcal{O}_v)$ is not dense.*

This is Theorem 3.5.3, p. 28 of [Se], except that k_v has been replaced by $\mathcal{O}_v$. Actually, the proof described in [Se], through Propositions 3.5.1 and 3.5.2, gives the present statement. ∎

Proof of Theorem 2. Renumbering indices if necessary, we may assume that $\Phi_1, \dots, \Phi_r$ are defined over k and generically surjective, while, for each $j > r$, either Φ_j is not defined over k or its image is contained in some proper closed subvariety of $\mathcal{Q}$. Let $\Phi := (\phi_1, \dots, \phi_n)$ be some Φ_j, not defined over k. Here the ϕ_i are polynomials in d variables, not all of whose coefficients lie in k. So we see that $\{\mathbf{x} \in k^d : \Phi(\mathbf{x}) \in k^n\}$ is contained in a proper algebraic subset of $\mathbb{A}^d$. In particular $\Phi(\mathcal{O}_k^d) \cap \mathcal{V}(\mathcal{O}_k)$ is contained in an algebraic subset of $\mathcal{V}$ of dimension $\le d-1$. Hence there exists an algebraic subset $\mathcal{W} \subset \mathcal{V}$, of dimension $< d$, such that

$$(\mathcal{V} \setminus \mathcal{W})(\mathcal{O}_k) \subset \bigcup_{j\le r} \Phi_j(\mathcal{O}_k^d). \tag{2}$$

Renumbering again the first r indices if necessary we may assume that $\Phi_1, \dots, \Phi_s$ are birational isomorphisms, while Φ_j has degree ≥ 2 for all j with $s < j \le r$. By adding to $\mathcal{W}$ a proper closed subset of $\mathcal{V}$ if necessary, we may assume that, for $j = 1, \dots, s$, the inverse of Φ_j (a rational function on $\mathcal{V}$) is defined on $\mathcal{V} \setminus \mathcal{W}$, so, in particular, each point on $(\mathcal{V} \setminus \mathcal{W})(\mathbb{C})$ is the image under Φ_j of a unique point on $\mathbb{A}^d(\mathbb{C})$.

In view of Definition 2 the set $A := \bigcup_{s<j\le r} \Phi_j(\mathcal{O}_k^d) \cup \mathcal{W}(\mathcal{O}_k)$ is thin, and we have, by (2)

$$\mathcal{V}(\mathcal{O}_k) \setminus A \subset \bigcup_{j\le s} \Phi_j(\mathcal{O}_k^d). \tag{3}$$

If some Φ_j, $j \le s$, is an isomorphism we are done, so assume the contrary to derive a contradiction. Let $t_1, \dots, t_d$ be the coordinate functions on $\mathbb{A}^d$. Under each of the Φ_j^{-1}, $j \le s$, we may view the t_i as rational functions on $\mathcal{V}$. Since no such Φ_j is an isomorphism, for each $j \le s$ we may find $i = i_j$ such that t_i lies in $k(\mathcal{V}) \setminus k[\mathcal{V}]$. We denote by g_j such a function. Since $\mathcal{V}$ is normal, the only rational functions on $\mathcal{Q}$ with trivial divisor of poles are the regular ones (by e.g. [Hart, Prop. 6.3A, p. 132]) and we can thus write, for a suitable prime divisor $\mathcal{D}_j$ on $\mathcal{V}$ (say defined over $\overline{k}$),

$$g_j = \xi_j/\eta_j, \qquad 1 \le j \le s,$$

where $\xi_j, \eta_j \in \overline{k}[\mathcal{V}]$, ξ_j is a unit at $\mathcal{D}_j$ while η_j has positive order at $\mathcal{D}_j$.

Denote by $\mathcal{P}_j$ the $(d-1)$-dimensional quasi-affine variety obtained by removing from $\mathcal{D}_j$ the set of zeros of ξ_j. Let x_j be a point on $\mathcal{P}_j$ having co-

ordinates which are algebraic over k and let L be the number field generated over k by all such coordinates, with ring of integers $\mathcal{O}_L$.

Also, let S_0 be a finite set of places of k such that $\mathcal{V}(\mathcal{O}_k)$ is dense in $\prod_{v\in S}\mathcal{V}(\mathcal{O}_v)$ for all finite $S \subset \Sigma_k$ disjoint from S_0. Select now distinct prime numbers $l_1, \dots, l_s$ splitting completely in L and not lying below places in S_0, and choose places $\mu_1, \dots, \mu_s \subset \Sigma_L$, lying resp. above $l_1, \dots, l_s$. By choosing the l_j large we may assume that the coefficients of the Φ_j and the coordinates of the x_j are μ_j-integers. We have $L_{\mu_j} = \mathbb{Q}_{l_j}$ for each $j \le s$. Finally, let $S_1 := \{v_1, \dots, v_s\}$ be the set of places of k lying resp. below $\mu_1, \dots, \mu_s$. Plainly $\mathcal{O}_{L,\mu_j} = \mathcal{O}_{k,v_j} = \mathbb{Z}_{l_j}$.

By Lemma 3 we may find a set $S_2 \subset \Sigma_k$, disjoint from $S_0 \cup S_1$, such that the image of A in $\prod_{v\in S_2}\mathcal{V}(\mathcal{O}_v)$ is not dense. Let Ω be an open subset of $\prod_{v\in S_2}\mathcal{V}(\mathcal{O}_v)$ disjoint from the image of A.

Observe that, for each $j \le s$, there exists a neighborhood I_j of x_j in $\mathcal{V}(\mathcal{O}_{L,\mu_j})$ (we remark that $x_j \in \mathcal{V}(\mathcal{O}_{L,\mu_j})$) such that, for $x \in I_j$, $g_j(x)$ is not a μ_j-integer whenever it is defined: this is true because $\eta_j(x_j) = 0$, while $\xi_j(x_j) \neq 0$. Since $\mathcal{O}_{L,\mu_j} = \mathcal{O}_{k,v_j} = \mathcal{O}_{v_j}$, I_j is a neighborhood of x_j in $\mathcal{V}(\mathcal{O}_{v_j})$. By the defining property of S_0 we may find a point $\alpha \in \mathcal{V}(\mathcal{O}_k)$ such that its image in $\prod_{v\in S_1\cup S_2}\mathcal{V}(\mathcal{O}_v)$ lies in $(\prod_{j\le s} I_j) \times \Omega$. We contend that any such point provides the desired contradiction. In fact, first of all, α cannot lie in A, by our choice of Ω. In particular, α cannot lie on $\mathcal{W}$, so Φ_j^{-1} is defined at α for $j \le s$ and we have $\alpha = \Phi_j(\beta_j)$, for a uniquely determined $\beta_j \in \mathbb{A}^d$. Now, $g_j(\alpha)$ is equal to some coordinate of β_j and is not a v_j-integer. Hence α cannot be in the image of Φ_j on $\mathcal{O}_k^d$ and, since α does not lie in A, we have a contradiction with (3). ∎

R e m a r k 1. It is possible to prove Theorem 1 in an ad hoc manner, using the ordinary version of the Hilbert Irreducibility Theorem (see e.g. [La], [Sch] or [Se]) in place of Lemma 3. (In fact, the concept of very-weak approximation and the above Lemma 3 are related to Hilbert's theorem and indeed lead to a version of it; this is due to J.-L. Colliot-Thélène [CT] and T. Ekedahl [Ek]; see [Se, Thm. 3.5.7, p. 30] and [Se, Prop. 3.3.1, p. 23]).

We may roughly describe such a proof as consisting of two parts. First a *rationality* part, based on H.I.T.: we forget integrality conditions and simply show that, for certain points α on $\mathcal{V}$, the corresponding possible values of the coordinates t_i on $\mathbb{A}^d$, for points in the inverse image relative to some Φ_j, cannot be even rational (this happens when $\deg \Phi_j \ge 2$). Second, an *integrality* part, equal to the above: we show that those values of the parameters which could be possibly rational, cannot in fact all be integral (this has to do with the Φ_j having degree 1). The first part is related to Hilbert's theorem, while the argument for the second one consists essentially in a crude form of Weil's Decomposition Theorem (see [We] or [La, p. 263]),

stating roughly that the factorization of the divisor of a rational function implies a corresponding factorization of its values at algebraic points.

R e m a r k 2. It is possible to prove a sharper version of Theorem 1; namely, even letting the variables t_i run through the ring $\mathbb{O}$ of all algebraic integers in place of $\mathcal{O}_k$, we cannot obtain all solutions in $\mathcal{O}_k$; this sharper result requires a corresponding sharpening of the above Lemma 2. Namely we need the following statement: *there does not exist a finite morphism from affine* 3*-space to* $\mathcal{Q}$. A proof of this result may be obtained as in our second argument for the present Lemma 2: if such a morphism existed the form ω would induce a regular closed form ω^* on $\mathbb{A}^3$, which would be exact. Now, taking the *trace* of an equation $\omega^* = d\eta$, say, we expect to show that ω itself would be exact, a fact which we have proved to be false. However, that the trace sends regular forms into regular ones seems to me not so automatic. I have now found a proof, written in a forthcoming paper [Za]; in fact, I have found no references for the needed result. Alternatively, C. Deninger has pointed out to me that a proof of the improved lemma may be obtained (in any characteristic $\neq 2$) using étale cohomology of quadrics and the pushforward map.

To derive the above contention from the sharpened Lemma 2, we may prove an analogue of Theorem 2, assuming now that $\mathcal{V}(\mathcal{O}_k) \subset \bigcup_{j \le h} \Phi_j(\mathbb{O}^d)$, to conclude that some Φ_j is a finite morphism defined over $\overline{k}$. The proof runs like the above one, but now it is necessary to consider, in addition to the g_j, the rational functions on $\mathcal{V}$ obtained as follows. Let Φ_j be a generically surjective one among the given morphisms. Then we may view the function field of $\mathbb{A}^d$ as a finite extension of the function field of $\mathcal{V}$. So the coordinate functions t_i on $\mathbb{A}^d$ satisfy monic irreducible equations over $\overline{k}(\mathcal{V})$. By [Se], Prop. 3.3.1, p. 23, such equations remain irreducible over k if we specialize the coefficients to points in $\mathcal{V}(\mathcal{O}_k)$, except for a thin set. If for given j all the coefficients of such equations are regular functions on $\mathcal{V}$, we see that Φ_j is finite and we are done. Otherwise some such coefficient will have nontrivial divisor of poles. We must take into account precisely the set of such coefficients (which includes the set of the g_j, considered in the above proof). The rest of the argument is exactly the same as above.

R e m a r k 3. As announced in the introduction we shall sketch (conditional) arguments which show that the analogue of Theorem 1 is hardly true if five variables are allowed.

We start with the parametrization of $\mathcal{Q}$ coming from the general simple continued fraction with five partial quotients, namely the fraction

$$a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\frac{1}{a_3+}\frac{1}{a_4}.$$

If p_3/q_3 and p_4/q_4 are the last two convergents, we see, putting $x_1 = p_3, x_2 = q_4, x_3 = p_4, x_4 = q_3$, that x_1, x_2, x_3, x_4 are polynomials in $a_0, \dots, a_4$ satisfying (1). Also, we find that, identically,

$$a_0 = \frac{(1 + a_3a_4)x_1 - a_3x_3}{(1 + a_3a_4)x_4 - a_3x_2}, \qquad a_1 = (1 + a_3a_4)x_4 - a_3x_2, \tag{4}$$
$$a_2 = \frac{x_2 - a_4x_4 - 1}{(1 + a_3a_4)x_4 - a_3x_2}.$$

Let now $P^* := (x_1^*, x_2^*, x_3^*, x_4^*) \in \mathcal{Q}(\mathcal{O}_k)$. We substitute x_i^* for x_i in (4) and try to choose $a_3, a_4 \in \mathcal{O}_k$ to make $a_1 = (1 + a_3a_4)x_4^* - a_3x_2^*$ a unit $u \in \mathcal{O}_k^*$. If this may be done, then even a_0, a_2 will lie in $\mathcal{O}_k$, so the point P^* will be obtained integrally from the parametrization.

Our equation is $u = (1 + a_3a_4)x_4^* - a_3x_2^* = x_4^* + a_3(a_4x_4^* - x_2^*)$. Hence it suffices if $a_4 \in \mathcal{O}_k$ may be found with $x_4^* \equiv u \pmod{x_2^* - a_4x_4^*}$. Our problem will be solved provided it is possible to choose $a_4 \in \mathcal{O}_k$ such that $\pi := x_2^* - a_4x_4^*$ is a prime element in $\mathcal{O}_k$ with the property that the cyclic group $(\mathcal{O}_k/(\pi))^*$ is in fact equal to the reduction $\pmod{\pi}$ of the unit group: this condition is plainly sufficient for the above congruence to be solvable in u.

To fix ideas, let $k = \mathbb{Q}(\sqrt{2})$, so $\mathcal{O}_k = \mathbb{Z}[\sqrt{2}]$. Now each unit is of the form $\pm\varepsilon^m$, where $\varepsilon = 1 + \sqrt{2}$. To reach the above goal we must first produce prime elements $\pi \equiv x_2^* \pmod{x_4^*}$. This can be achieved by the generalized Dirichlet theorem, since $(x_2^*, x_4^*) = 1$ for any $P^* \in \mathcal{Q}(\mathcal{O}_k)$, but we have the much stronger restriction that ε has to be an (almost) primitive root mod π. We are faced with an analogue of Artin's well known conjecture for primitive roots. Even in the case of the rational field this remains unsolved; however, C. Hooley [Ho] has proved that, if the generalized Riemann conjecture is true for Dedekind zeta functions of suitable fields, there are primes $\pi \in \mathbb{N}$ (and actually they have the "right" density) for which a given nonsquare integer $e \neq -1$ is a primitive root. Hooley starts by observing that e is a primitive root mod π iff for any prime $l \mid \pi - 1$ the congruence $x^l \equiv e \pmod{\pi}$ is not solvable. Reversing the procedure, he then starts from all such congruences and sieves out the bad primes. Hooley's method has been followed by J. P. Weinberger [Wei], who showed (again under Riemann hypothesis) that UFD is euclidean, for rings of integers of number fields containing nontrivial units. He proves our contention when x_4^* is a prime element, but his argument works generally. One proceeds as in [Ho], but considering only primes π in the generalized progression x_2^* mod x_4^* (of course associate primes give rise to the same condition). Again one is led to the congruences $x^l \equiv \varepsilon \pmod{\pi}$, where l divides $|N_{\mathbb{Q}}^k(\pi)| - 1$. These congruences represent the essentially new part, compared to Hooley: for the existence of primes π with the required properties it is of course necessary

that each such congruence is not solvable for some of the primes in the relevant progression, a fact which is not so obvious, since lying in the progression could possibly influence the solvability (e.g. $x^2 \equiv 5 \pmod p$ is solvable for all primes $p = 5m \pm 1$). This is not so in our case and a proof may be found in Vol. II of H. Hasse's *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, 1930, reprinted 1965. Of course one needs quantitative results on the densities and remainder terms to carry out the above procedure, and it is here that Riemann's conjecture is needed.

We conclude this remark by recalling that partial, but unconditional, results towards Artin's conjecture were obtained by R. Gupta and M. Ram Murty [G-RM] and D. R. Heath-Brown [HB] for the classical case $k = \mathbb{Q}$ and by W. Narkiewicz for certain cyclotomic fields k. To my knowledge, however, no generalization of the original Gupta–Ram Murty method to number fields is already available for our application, even when k has large degree.

R e m a r k 4. As announced before, we describe a possibility for obtaining an example over $\mathbb{Z}$, starting from the one coming from Remark 3, and formulate a general problem on polynomial ideals which arises in this connection.

We assume (as in Remark 3) the existence of polynomials $P_1, \dots, P_4 \in \mathbb{Z}[t_1, \dots, t_5]$, with $P_1P_2 - P_3P_4 = 1$ and such that, for each solution $(a_1, \dots, a_4) \in \mathbb{Z}[\sqrt{2}]^4$ of (1), there exist $b_1, \dots, b_5 \in \mathbb{Z}[\sqrt{2}]$ such that $P_i(b_1, \dots, b_5) = a_i$ for $1 \le i \le 4$.

Write $t_i = u_i + \sqrt{2}v_i$, for indeterminates u_i, v_i. Then we may write

$$P_i(t_1, \dots, t_5) = Q_i + \sqrt{2}R_i$$

for polynomials $Q_i, R_i \in \mathbb{Z}[u_1, \dots, u_5, v_1, \dots, v_5]$. Now assume $(a_1, \dots, a_4) \in \mathbb{Z}^4$ is a solution of (1) in rational integers, and pick $b_1, \dots, b_5$ as above. We may put $b_i = u_i^* + \sqrt{v_i^*}$ for rational integers u_i^*, v_i^* and consequently we get, in an obvious notation,

$$Q_i(\mathbf{u}^*, \mathbf{v}^*) = a_i, \qquad R_i(\mathbf{u}^*, \mathbf{v}^*) = 0 \tag{5}$$

for all i. Define $\mathcal{R} := \mathbb{Z}[u_1, \dots, u_5, v_1, \dots, v_5]$. Now we make the following

Assumption. *There exist polynomials F, G in the ideal $\mathcal{I}$ generated by $R_1, \dots, R_4$ in $\mathcal{R}$, such that $Q_1 + F, Q_3 + G$ generate the unit ideal in $\mathcal{R}$.*

Observe that the assumption is certainly satisfied if we replace the ring $\mathcal{R}$ with the ring $\mathcal{R}[\sqrt{2}] = \mathbb{Z}[\sqrt{2}][u_1, \dots, u_5, v_1, \dots, v_5]$ (we may take $F = \sqrt{2}R_1, G = \sqrt{2}R_3$). Also, the polynomials P_i coming from Remark 3 may be easily explicitly computed, so it may be that F, G can be found without appealing to any general assertion leading to the above assumption. However, we have not succeeded in doing so at the moment, nor to disprove the assumption for the polynomials in question.

Let then F, G be as in the assumption, so we have an equation

$$X(Q_1 + F) + Y(Q_3 + G) = 1 \tag{6}$$

for suitable $X, Y \in \mathbb{Z}[u_1, \dots, u_5, v_1, \dots, v_5]$.

Since $P_1, \dots, P_4$ satisfy (1) we have in particular

$$Q_1Q_2 - Q_3Q_4 + 2R_1R_2 - 2R_3R_4 = 1. \tag{7}$$

Multiply both terms of (6) by $\Delta := 2R_1R_2 - 2R_3R_4 - FQ_2 + GQ_4 \in \mathcal{I}$. We get, using (7),

$$\begin{aligned}(\Delta X)(Q_1 + F) - (\Delta Y)(Q_3 + G) &= 2R_1R_2 - 2R_3R_4 - FQ_2 + GQ_4 \\ &= 1 - Q_1Q_2 + Q_3Q_4 - FQ_2 + GQ_4,\end{aligned}$$

which may be rewritten as

$$(Q_1 + F)(Q_2 + \Delta X) - (Q_3 + G)(Q_4 + \Delta Y) = 1,$$

namely the four polynomials $S_1 := Q_1 + F, S_2 := Q_2 + \Delta X, S_3 := Q_3 + G, S_4 := Q_4 + \Delta Y$ give a solution of (1) and lie in $\mathbb{Z}[u_1, \dots, u_5, v_1, \dots, v_5]$. Take now a solution $a_1, \dots, a_4$ of (1) in rational integers, and find rational integers u_i^*, v_i^* as above, so (5) is verified. From (5) we see that, for every polynomial $\Gamma \in \mathcal{I}$, we have $\Gamma(u_1^*, \dots, u_5^*, v_1^*, \dots, v_5^*) = 0$. Since $F, G, \Delta \in \mathcal{I}$ we finally obtain, using again (5),

$$S_i(u_1^*, \dots, u_5^*, v_1^*, \dots, v_5^*) = a_i, \qquad i = 1, 2, 3, 4,$$

so the polynomials S_i would produce the desired example over $\mathbb{Z}$.

We conclude by mentioning a simply stated problem on polynomial ideals, somewhat relevant in connection with the above "Assumption":

PROBLEM. *Let* $a, b, c \in \Omega := k[x_1, \dots, x_n]$ *generate the unit ideal. Is it necessarily true that there always exist* $u, v \in \Omega$ *such that* $a + uc, b + vc$ *generate the unit ideal?*

At first sight I would expect a negative answer, but have no counterexample. We omit natural generalizations and modifications of the problem (e.g. does the answer depend on k, or can one find a decision algorithm, given a, b, c?), also in view of the fact that they fall too far from the main topic of the paper.

References

[CT] J.-L. Colliot-Thélène, Letter to T. Ekedahl, 9/21/1988, unpublished.

[Ek] T. Ekedahl, *An effective version of Hilbert's Irreducibility Theorem*, preprint, Stockholm 1987 (see also Séminaire de Théorie des Nombres, Paris 1988–1989, Birkhäuser, 1990, 241–248).

[G-RM] R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. 78 (1984), 127–130.

[Hart] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.

[HB] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford 37 (1986), 27–38.

[Ho] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.

[La] S. Lang, *Fundamentals of Diophantine Geometry*, Springer, 1983.

[Sch] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor, 1982.

[Se] J. P. Serre, *Topics in Galois Theory*, Jones and Bartlett Publ., Boston, 1992.

[Sko] T. Skolem, *Diophantische Gleichungen*, Springer, 1938, reprint Chelsea, 1950.

[Sz] K. Szymiczek, *On some diophantine equations connected with triangular numbers*, Zeszyty Nauk. Wyż. Szkoły Ped. w Katowicach Mat. 4 (1964), 17–22 (in Polish).

[We] A. Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. 52 (1928), 281–315 = Coll. Papers, Vol. I, 2nd printing, Springer, 1980, 11–46.

[Wei] P. J. Weinberger, *On Euclidean rings of algebraic integers*, in: Proc. Sympos. Pure Math. 24, Amer. Math. Soc., 1973, 321–332.

[Za] U. Zannier, *Note on traces of regular differential forms*, preprint, 1995.

Ist. Univ. Arch. D.S.T.R.
S. Croce, 191
30135 Venezia, Italy
E-mail: zannier@dimi.uniud.it

Received on 12.2.1996
and in revised form on 2.7.1996 (2927)