Notre Dame Journal of Formal Logic
Volume 43, Number 3, 2002

Hilbert's Tenth Problem for Rings of Rational Functions

Karim Zahidi

Abstract We show that if R is a nonconstant regular (semi-)local subring of a rational function field over an algebraically closed field of characteristic zero, Hilbert's Tenth Problem for this ring R has a negative answer; that is, there is no algorithm to decide whether an arbitrary Diophantine equation over R has solutions over R or not. This result can be seen as evidence for the fact that the corresponding problem for the full rational field is also unsolvable.

1 Introduction

In 1900, in his famous address to the International Conference of Mathematicians in Paris, Hilbert asked for a general method to determine whether an arbitrary Diophantine equation with integer coefficients has an integer solution or not. This problem, otherwise known as Hilbert's Tenth Problem (HTP), was answered negatively by Matijasevich, building mainly on work of Davis, Putnam, and Robinson [5]; that is, they proved that no such algorithm could exist. Since then various authors have been interested in extending this result to other rings and fields. The main open problem in this area is probably the analogue of HTP for the field of rational numbers and its finite extensions.

Let us first introduce some definitions before we discuss some of these generalizations. Assume that R is a commutative domain (with unity); we say that a subset S of R^n is existentially definable in the language $\mathcal{L} = \{0, 1, \mathcal{C}, +, .\}$ (where $\mathcal{C}$ is a set of constants, possibly empty) if there exists a finite number of polynomials $P_1, \ldots, P_k, Q$ whose coefficients can be built up by addition and multiplication from the constants in the language such that the following equivalence holds $(\overline{x} = (x_1, \ldots, x_n), \overline{y} = (y_1, \ldots, y_m))$:

$$\overline{x} \in S \leftrightarrow \exists \overline{y} \in R^m : P_1(\overline{x}, \overline{y}) = \cdots P_k(\overline{x}, \overline{y}) = 0 \ \wedge \ Q(\overline{x}, \overline{y}) \neq 0.$$

Received June 10, 2002; accepted September 10, 2003; printed December 19, 2003
2001 Mathematics Subject Classification: Primary, 03B25; Secondary, 11U05, 12L05
Keywords: diophantine problems, function fields, undecidability

If the right-hand side of this equivalence consists only of equations, we call the set S a positive existential set; if furthermore the right-hand side consists of only one equation, we call S a Diophantine set. We say that the existential (respectively positive-existential, respectively Diophantine) theory of the ring R (in the language $\mathcal{L}$) is decidable if for every existential (respectively positive-existential, respectively Diophantine) set S we can decide whether a given point is in S or not. So from a logician's point of view, the analogue of HTP for a ring R is precisely the decidability question of the Diophantine theory (in some suitable language) of this ring. Note that the union of two Diophantine sets is again Diophantine ($P = 0 \vee Q = 0$ is equivalent with $PQ = 0$) and the same is true for the intersection in case the fraction field of R is not algebraically closed (we can find an irreducible polynomial $f(x)$ that after homogenization gives a polynomial in two variables $\overline{f}(x, y)$ such that $P = 0 \wedge Q = 0$ is equivalent with $\overline{f}(P, Q) = 0$).

As already mentioned, the outstanding open problem in this area is HTP for the field of rational numbers. Mainly motivated by the analogy between solving Diophantine equations over the rationals and over rational function fields, several authors have investigated the existential theory of such function fields. All known cases yield an undecidability result for the existential theory of $k(t)$ in the language $\mathcal{L} = \{0, 1, t, +, \cdot\}$ and include the following cases: k is a formally real field (Denef [1]), k is a finite field (Pheidas [7]), later extended to some infinite fields of positive characteristic in Kim and Roush [3], k is a p-adic field (Kim and Roush [4]), k is a field of rational functions in one variable s over the complex numbers (in this case the language contains a symbol for the extra variable s, that is, $\mathcal{L} = \{0, 1, t, s, +, \cdot\}$ (see Kim and Roush [2]). Up until now no results concerning the Diophantine theory of a rational function field over an algebraically closed field are known, so the following question remains open.

Question 1.1 *Is the existential theory of* $\mathbf{C}(t)$ *in the language* $\mathcal{L} = \{0, 1, t, +, \cdot\}$ *decidable?*

There are some results that point in the direction of an undecidability result: in [2], Kim and Roush prove that the existential theory of $\mathbf{C}(t_1, t_2)$ in the language $\mathcal{L}_{t_1 t_2} = \{0, 1, t_1, t_2, +, \cdot\}$ is undecidable. In Pheidas and Zahidi [8] it is proven that the existential theory of $\mathbf{C}(t)$ in the language $\mathcal{L}_D = \{0, 1, t, +, \cdot, D\}$ (where D is a predicate to denote the set of all rational functions which are the derivative of some other rational function) is undecidable.

In this paper we will be studying a problem related to the decidability question of the Diophantine theory of $\mathbf{C}(t)$. More precisely we will be dealing with the Diophantine theory of some "large" subrings of rational function fields over an algebraically closed field. It is a consequence of our main theorem (stated below) that the subring of the rational function field $k(t)$ (with k algebraically closed of characteristic zero) consisting of all rational functions whose denominator is not divisible by t (supposing, as usual, that the function is written in lowest fractions) has an undecidable Diophantine theory. More generally we prove our main theorem.

Theorem 1.2 (Main Theorem) *Let k be an algebraically closed field of characteristic zero. Let R, $k \subset R \subset k(t)$ be a regular local or a regular semi-local ring. Then the positive-existential theory of R is undecidable.*

It should be noted that the analogous problem for regular local or regular semi-local rings in $\mathbf{Q}$ (a semi-local ring in $\mathbf{Q}$ is simply a ring of the form $\{q \in \mathbf{Q} : \ \mathrm{ord}_{p_i}(q) \geq 0\}$

for a finite set of prime numbers $p_1, \ldots, p_n$, where ord_p denotes the p-adic valuation) or number fields is still open. In fact, showing the undecidability of the Diophantine theory of such a subring of $\mathbf{Q}$ (or any number field) would imply the undecidability of the Diophantine theory of $\mathbf{Q}$. Indeed, the results by Robinson ([10] and [11]) and Rumely [12] on definability in global fields imply that regular local and semi-local subrings in $\mathbf{Q}$ (or any number field K) are in fact Diophantinely definable in $\mathbf{Q}$ (or K). We therefore consider the following question to be important for future research.

Question 1.3 *Let K be a number field and let R, $R \subset K$ be a regular local or semi-local ring. Is the Diophantine theory of R decidable?*

In connection with this question we mention a recent result by Shlapentokh who proved that given a nontrivial totally real cyclic number field K one can construct an infinite set W of non-Archimedean primes of K such that the ring R defined by $R = \{x \in K,\ \mathrm{ord}_p x \geq 0\ ,\ \forall p \notin W\}$ has an undecidable Diophantine theory (see [13]; for a similar result for algebraic function fields of positive characteristic see [14]). This result was considerably improved by Poonen [9] who proved that one can take the set W to be of natural density 1. However, this does not imply an undecidability result for K since from the construction of W follows that $S \setminus W$ (where S denotes the set of all non-Archimedean primes of K) is also infinite and hence the ring under consideration is not a semi-local ring.

We now give a short outline of the contents of this paper. We start with a short section, reminding the reader of some general facts of local subrings of rational function fields. In Section 3 we introduce some results concerning elliptic curves. Following Denef [1], we use the theory of elliptic curves to construct a Diophantine definition of the integers in a semi-local subring of a rational function field. This is done in Section 4.

2 Local and Semi-local Rings in Function Fields

2.1 Regular local rings Let k be an algebraically closed field and let a be an element of k. The ring $\mathcal{O}_a$ of all functions $f \in k(t)$ which are defined at a is given by

$$\mathcal{O}_a = \{f \in k(t) :\ \exists f_1,\, f_2 \in k[t],\, f_2(a) \neq 0 \text{ and } f = \frac{f_1}{f_2}\}\ .$$

The subring

$$\mathcal{O}_\infty = \{f \in k(t) :\ \exists f_1,\, f_2 \in k[t], \deg(f_1) \leq \deg(f_2) \text{ and } f = \frac{f_1}{f_2}\}$$

of $k(t)$ is said to consist of the functions which are defined at ∞ (to explain this terminology, substitute t by $1/t$, then the elements of this ring become the functions which are defined at zero). The rings $\mathcal{O}_a$ and $\mathcal{O}_\infty$ are one-dimensional local subrings of $k(t)$, the maximal ideal $\mathcal{M}$, respectively, given by $(t-a)$ or (t^{-1}). Every ideal I of $\mathcal{O}_a$ ($a \in k$ or $a = \infty$) is of the form $I = \mathcal{M}^n$, for some positive integer n. Since $\mathcal{M}$ is a principal ideal, it follows that $\mathcal{O}_a$ is a principal ideal domain and hence also a unique factorization domain.

Note that $\mathcal{O}_a$ also has the structure of a discrete valuation ring: every element in $\mathcal{O}_a$ can be written uniquely as $u\pi_a^n$ with n a positive integer, u a unit, and π_a a local uniformizing parameter, that is, a generator of the maximal ideal in $\mathcal{O}_a$. Hence, $\mathcal{O}_a$

is a one-dimensional regular local ring (see p. 122 in Matsumura [6]). The valuation ord_a is given by

$$\mathrm{ord}_a = n \leftrightarrow x = u\pi^n$$

and is independent of the choice of the local uniformizing parameter. So $\mathcal{O}_a$ is the ring of all functions $f \in k(t)$ such that $\mathrm{ord}_a(f) \geq 0$.

Conversely, every regular local subring R of $k(t)$, $k \subset R \subset k(t)$, is a discrete valuation ring (see p. 122 in [6]), and any discrete valuation ring R, $k \subset R \subset k(t)$ is of the form $\mathcal{O}_a$, for some $a \in k \cup \{\infty\}$.

2.2 Regular semi-local rings Let S be a finite set of points in $k \cup \{\infty\}$. The ring $\mathcal{O}_S$ of all functions f in $k(t)$ which are defined at all the points of the set S is given by

$$\mathcal{O}_S = \bigcap_{a \in S} \mathcal{O}_a \, .$$

One easily sees that the ring $\mathcal{O}_S$ is the ring of all functions f in $k(t)$ such that $\mathrm{ord}_a(f) \geq 0$, for all $a \in S$. The ring $\mathcal{O}_S$ has the structure of a regular semi-local ring since it is the intersection of finitely many regular local rings. Furthermore, $\mathcal{O}_S$ is a noetherian unique factorization domain. The ring $\mathcal{O}_S$ has finitely many maximal ideals. The maximal ideals are exactly the ideals corresponding to the maximal ideals $\mathcal{M}_a$ of $\mathcal{O}_a$.

3 Elliptic Curves

We assume the reader is familiar with the basics of elliptic curves. We briefly recall the relevant definitions and results. For more information on the theory of elliptic curves, the reader can consult Silverman [15].

Let k be an arbitrary field (char $k \neq 2, 3$). An elliptic curve E over k is a (projective) nonsingular curve whose affine points satisfy

$$E : \gamma s^2 = f(t)$$

where γ is in k and f is a cubic polynomial with coefficients in k and with no multiple roots. It can be proven that every elliptic curve is isomorphic to an elliptic curve whose equation is given by

$$s^2 = t^3 + \alpha t + \beta \, . \tag{1}$$

This equation is called a Weierstrass equation. As is well known, the k-rational points of such a curve can be given the structure of an Abelian group, whose addition law is algebraic over k (i.e., given two points on E, the coordinates of their sum can be expressed as rational functions of the coordinates of the two points), and whose neutral element is the unique point at infinity of the curve, denoted by P_∞. Note that the endomorphism group of the group $E(k)$ is in fact a ring, denoted by $\mathrm{End}(E)$ and contains a subring isomorphic to $\mathbf{Z}$. This subring consists of the endomorphisms $\{e_n, \ n \in \mathbf{Z}\}$, with e_n defined by

$$e_n(P) = \underbrace{P + P + \cdots + P}_{n \text{ times}}$$

where the addition is, of course, the addition on the elliptic curve. If the endomorphism ring is strictly larger than $\mathbf{Z}$, we say that the curve has complex multiplication.

From now on we assume that k is a field of characteristic 0. If E is an elliptic curve the invariant

$$j_E = 1728\frac{4\alpha^3}{4\alpha^3 - 27\beta^2}$$

is called the j-invariant of the curve (the coefficients that appear in the definition are the coefficients of the Weierstrass equation (1) for E). Let E be an elliptic curve over k, defined by the equation

$$E : s^2 = f(t)$$

(with f an arbitrary cubic polynomial with no multiple roots). We associate to E an elliptic curve E_0 defined over $k(t)$ by the equation

$$E_0 : f(t)Y^2 = f(X). \tag{2}$$

If the curve E has no complex multiplication, we have the following.

Lemma 3.1 *The curve E_0 has rank one over $k(t)$. The generator is the point $(t, 1)$. Furthermore the only $k(t)$-rational torsion points are points of order two.*

Proof See [1]. □

By (x_n, y_n) we mean the point $n(t, 1)$ (addition on the curve E_0). It can be proven that for any (affine) point (t, s) on E which is not an n-torsion point on E we can write $e_n[(t, s)] = (x_n(t), sy_n(t))$ (see [8]). Below we list some of the properties of the rational functions x_n and y_n. Throughout this paragraph by order of a rational function x at a point a, we mean the unique integer l such that $x = (t-a)^l y$ with y a rational function with no pole or zero at a. We say that x has a zero or pole of order $|l|$ at a depending on whether l is positive or negative. In case $l = \pm 1$ we say that x has a simple zero or pole at a. We say that x has order l at infinity (notation ∞) if the function which is obtained by substituting t by t^{-1} in x has order $-l$ at zero. This corresponds with the valuation we defined on the ring $\mathcal{O}_a$ in Section 2.

Lemma 3.2 *Let k be a field of characteristic zero and E/k an elliptic curve defined by*

$$E : s^2 = f(t)$$

with f an arbitrary cubic polynomial with no multiple roots. For any integer n, let $e_n(t, s) = (x_n(t), sy_n(t))$ be the nth endomorphism. Let t_0 be a zero of $f(t)$.

(a) *x_n has finite poles and finite zeros of order at most 2. y_n has only finite zeros of order one and finite poles of order at most 3, x_n has a pole of order 5 and y_n a pole of order 6 at ∞.*

(b) *if n is odd neither x_n nor y_n has a pole at t_0; y_n has no zero at t_0; $x_n - t_0$ has a zero at t_0.*

(c) *if n is odd,*

$$\frac{x_n - t_0}{(t - t_0)y_n}(t_0) = n\ .$$

Proof (a) We will use the fact that $x_n' = ny_n$—where, for $x \in k(t)$, x' denotes the formal derivate of x with respect to t; see Lemma 1.2 in [8]. From this, one sees that if the order of x_n is l at a point $t = a$, then y_n has order $l - 1$ at this point. We first treat the finite poles. Suppose that x_n has a pole at $t = a$, say of order $|l|$, $l < 0$. Then the order of y_n at this point is $l - 1$. Now we will combine this with the fact that (x_n, y_n) satisfies equation (2). This implies that either $2(l-1) + 1 = 3l$

or $2(l-1) = 3l$, depending on whether a is a zero of f or not. This implies the result. For the pole at infinity, note that since $e_n(P_\infty) = P_\infty$, it is clear that x_n has a pole at ∞. Call the order of x_n at ∞ l. The order of y_n at ∞ is $l-1$. Using the fact that (x_n, y_n) satisfies equation (2) and the fact that f has order -3 at ∞ we get $-3 + 2(l-1) = 3l$, which gives $l = -5$.

(b) A proof of the first claim can be found in [8] (Lemma 1.4). The second claim follows from the fact that $(t_0, 0)$ is a point of order two, and hence $e_n((t_0, 0)) = (t_0, 0)$ (since n is odd), thus $x_n(t_0) = t_0$. Let l be the order of $x_n - t_0$ at $t = t_0$, then we have $\mathrm{d}(x_n - t_0)/\mathrm{d}t = ny_n$, hence we conclude that the order of y_n at t_0 is $l-1$. Again using the fact that (x_n, y_n) satisfies equation (2) combined with the facts that the order of $f(t)$ at $t = t_0$ is 1 and the order of $f(x_n)$ at $t = t_0$ is l, we get $l = 1$.

(c) First suppose that $t_0 \neq 0$. By (b), we know that neither x_n or y_n has a zero or pole at t_0, so we can write x_n as

$$x_n = x_{0n} + x_{1n}(t - t_0) + \cdots$$

and y_n as

$$y_n = y_{0n} + y_{1n}(t - t_0) + \cdots,$$

with $x_{jn}, y_{jn} \in k$. Since $x_n' = ny_n$ we get that

$$x_{1n} = ny_{0n}.$$

Furthermore, since $x_n(t_0) = t_0$,

$$x_{1n} = \frac{x_n(t) - t_0}{t - t_0}(t_0) \quad \text{and} \quad y_{0n} = y_n(t_0).$$

Hence,

$$\frac{x_n(t) - t_0}{(t - t_0)y_n(t)}(t_0) = n.$$

If $t_0 = 0$, it follows from our proof of (b) that x_n has a simple zero at 0. So we can write x_n, y_n as

$$\begin{aligned} x_n &= x_{1n}t + x_{2n}t^2 + \cdots, \\ y_n &= y_{0n} + y_{1n}(t - t_0) + \cdots. \end{aligned}$$

Again using the relation $x_n' = ny_n$, we obtain

$$x_{1n} = ny_{0n}.$$

Furthermore,

$$\frac{x_n}{t}(0) = x_{1n} \quad \text{and} \quad y_n(0) = y_{0n}.$$

Hence,

$$\frac{x_n}{ty_n}(0) = n.$$

□

4 Proof of the Main Theorem

Let $k(t)$ be a rational function field over an algebraically closed field of characteristic zero. We will prove that the Diophantine theory of a regular local or regular semi-local subring R, $k \subset R \subset k(t)$, of $k(t)$ (k algebraically closed) is undecidable. Since any local ring is also a semi-local ring, it is sufficient to prove the result for semi-local rings. Let R be a regular semi-local ring of $k(t)$, $k \subset R \subset k(t)$. Then R is the intersection of finitely many regular local subrings of $k(t)$, which are of the form $\mathcal{O}_a$, with $a \in k \cup \{\infty\}$ (see §2.1). After performing a change of variables of type

$$t \to \frac{t-\alpha}{t-\beta},$$

we may assume that R is in fact an intersection of local rings of the form $\mathcal{O}_a$, with $a \in k$. So without loss of generality we may always assume that the ring R is of the form

$$\bigcap_{i=1}^{n} \mathcal{O}_{a_i}\ ,\ a_1, \ldots, a_n \in k.$$

Throughout, h will denote

$$h = \prod_{i=2}^{n} (t - a_i).$$

Clearly, h is a local uniformizing parameter for the local rings $\mathcal{O}_{a_i}$, $i = 2, \ldots, a_n$.

We now need to construct an elliptic curve whose R-rational points can serve as a model for the integers. From Lemma 3.1 it follows that we have no trouble in constructing an elliptic curve whose $k(t)$-rational points can serve as a model for the integers. However the points of this curve might not all be R-rational. But Lemma 3.2 allows us to bound the order of the relevant poles of these points and this can be used to construct the desired elliptic curve. This is done in the following lemma.

Lemma 4.1 *Let E_0 be an elliptic curve defined over $k(t)$ by*

$$f(t)Y^2 = f(X),$$

with $f(X) = X^3 + \alpha X^2 + \beta X + \gamma$, $\alpha, \beta, \gamma \in k$, such that E_0 has rank one over $k(t)$ and such that $f(a_1) = 0$. Let E_0' be the curve defined by

$$f(t)hY^2 = X^3 + \alpha h^3 X + \beta h^6 X + \gamma h^9.$$

Then there exists an isomorphism φ, defined over $k(t)$, between E_0 and E_0'.

The points (X, Y) on E_0' with coordinates in R are of the following form:

1. *$(X, Y) = \varphi((x_{2r+1}, y_{2r+1}) + P)$ with r an integer and P a point of order two on E_0, $P \neq (a_1, 0)$, or*
2. *$(X, Y) = \varphi((x_{2r}, y_{2r}) + P)$, with r an integer and P a point of order two on E_0, $P \neq P_\infty$.*

Proof Consider the following map from E_0 to E_0':

$$\begin{array}{rccc} \varphi & E_0 & \to & E_0' \\ & (x, y) & \to & (X, Y) = (h^3 x, h^4 y). \end{array}$$

One checks that this is a birational map from E_0 to E_0'. It is everywhere defined and sends P_∞ to P_∞. Hence it is an isomorphism of elliptic curves. This implies that E_0' has rank one over $k(t)$ and the generator is the point (h^3t, h^4). Denoting $n(h^3t, h^4)$ by (X_n, Y_n) gives

$$\varphi((x_n, y_n)) = (X_n, Y_n).$$

By Lemma 3.1 we know that every point on E_0 can be written as

$$(x, y) = (x_n, y_n) + P,$$

with P a point of order two. Hence, every point (X, Y) on E_0' can be written as

$$(X, Y) = (h^3x_n, h^4y_n) + P',$$

with P' a point of order two on E_0'.

We first determine the points (x, y) on E_0 having no pole at $(a_1, 0)$. Let E be the curve defined by

$$E: \ s^2 = f(t).$$

To a point $(x, y) + P$ on E_0, we associate the rational function $\psi = (x, sy) + P$ of the curve E to itself. First, suppose that $(x, y) = (x_{2l+1}, y_{2l+1}) + P$. Then, since $(a_1, 0)$ is a point of order two, we have that $\psi((a_1, 0)) = (a_1, 0) + P$, so if $P \neq (a_1, o)$, we see that $\psi((a_1, 0)) \neq P_\infty$, which implies that a_1 is not a pole of x. A simple calculation shows that y has no pole at a_1 as well. If $P = (a_1, 0)$, we see that $\psi((a_1, 0)) = P_\infty$, and this implies that x has a pole at a_1. Again it follows that y has a pole at a_1.

If $(x, y) = (x_{2l}, y_{2l}) + P$, then $\psi((a_1, 0)) = P$, and hence, for $P \neq P_\infty$, $\psi((a_1, 0)) \neq P_\infty$, which implies that neither x nor y has a pole at a_1. If $P = P_\infty$, then it follows from Lemma 3.2 that x and y have a pole at a_1. Hence, the points on E_0 which have no pole at a_1 are either of the form

$$(x, y) = (x_{2l+1}, y_{2l+1}) + P \quad \text{or} \quad (x, y) = (x_{2l}, y_{2l}) + P$$

with l an integer and P a point of order two, $P \neq (a, 0)$, respectively, $P \neq P_\infty$.

Note that h has a zero of order 1 at any of the a_is, $i = 2, \ldots, n$. This together with the fact that x_n has finite poles of order at most two and y_n has finite poles of order at most 3 (see Lemma 3.2(a)) implies that neither h^3x_n nor h^4y_n has poles at any of the a_is, $i = 1, \ldots, n$. □

The following lemma is an analogue of Lemma 3.2(c) for the rational function X_n and Y_n.

Lemma 4.2 *(The notation is as in Lemma 3.2) For n an odd integer and $\omega = h(a_1)$,*

$$\left(\omega h^7 \frac{X_n - h^3a_1}{(t - a_1)Y_n}\right)(a_1) = \omega^7 n.$$

Furthermore,

$$\omega h^7 \frac{X_n - h^3a_1}{(t - a_1)Y_n} \in R.$$

Proof For n an odd integer, X_n and Y_n have no poles at any of the a_is, $i = 1, \ldots, n$. By the fact that y_n has finite zeros of order at most 3 (by Lemma 3.2(a)), it follows

that $Y_n = h^4 y_n$ has finite zeros of order at most 7. Also X_n has no poles at any of the a_is, $i = 1, \ldots, n$. It follows that the only poles of

$$\frac{X_n - h^3 a_1}{(t - a_1)Y_n}$$

among the a_is, $i = 2, \ldots, n$ are the zeros of Y_n, and since these are of order at most 7, the funtion

$$\alpha h^7 \frac{X_n - h^3 a_1}{(t - a_1)Y_n}$$

has no pole at any of the a_is, $i = 2, \ldots, n$.

Note that both $(t - a_1)Y_n$ and $X_n - h^3 a_1$ have a simple zero at a_1; hence, their quotient has no pole at a_1. This proves the second claim.

Evaluating at a_1 gives

$$\begin{aligned} \left(\frac{X_n - h^3 a_1}{(t - a_1)Y_n}\right)(a_1) &= \left(\frac{1}{h}\frac{x_n - a_1}{(t - a_1)y_n}\right)(a_1) \\ &= \frac{1}{\omega} n \end{aligned}$$

where we have used Lemma 3.2(c). □

Before we prove the Main Theorem 1.2 we still need some easy Diophantine definitions which are given in the following lemma. By $\mathcal{L}_R$ we denote the language of rings (i.e., $\mathcal{L}_R = \{0, 1, +, \ldots\}$. By $\mathcal{L}_n$ we denote the language $\mathcal{L}_R \cup \{t, a_1, \ldots, a_n\}$, where the a_is are constant symbols. A semi-local ring $R = \bigcap_{i=1}^n \mathcal{O}_{a_i}$ becomes an $\mathcal{L}_n$ structure in the obvious way.

Lemma 4.3

(a) *k is an $\mathcal{L}_R$-Diophantine subset of R.*

(b) *The relation*

$$\wedge_{i=1}^n \mathrm{ord}_{a_i}(x) > 0$$

has an $\mathcal{L}_n$-Diophantine definition.

Proof (a) We claim that the following equivalence holds:

$$x \in k \leftrightarrow \exists y \in R : \; y^2 = x^3 - x.$$

Indeed, if $x \in k$, then we can solve the equation $y^2 = x^3 - x$ for y, since k is algebraically closed. Conversely suppose that (x, y) satisfies $y^2 = x^3 - x$, then both x and y must be elements in k. Indeed, the equation $y^2 = x^3 - x$ defines an elliptic curve and hence, it does not admit a rational parametrization.

(b) Since, for any element x of R, $\mathrm{ord}_{a_i}(x) \geq 0$, the relation $\wedge_{i=1}^n \mathrm{ord}_{a_i}(x) > 0$ is equivalent with

$$\exists y \in R : \; x = (t - a_1)hy.$$

□

Theorem 4.4 *Let R be the ring $\bigcap_{i=1}^n \mathcal{O}_{a_i}$, $a_i \in k$. Then the Diophantine theory of R in the language $\mathcal{L}_n$ is undecidable.*

Proof We will prove that the ring of rational integers is an $\mathcal{L}_n$-Diophantine subset of R, which implies the result. We show that we can find an elliptic curve E_0

$$f(t)Y^2 = f(X),$$

$f(t) = t^3 + \alpha t^2 + \beta t + \gamma$, such that $f(a_1) = 0$ and such that E_0 has rank one over $k(t)$. We show that such a curve exists. Consider the elliptic curve E' defined by

$$s^2 = g(t) = t^3 - \frac{3}{2}t^2 - t$$

over $\mathbf{Q}$. The j-invariant of this curve is given by $j = -2^6 3^9 7^{-2}$. Hence, this curve has no complex multiplication. Now after a linear change of variables $t \to t - a_1$, $f(t) = g(t - a_1)$, $f(a_1) = 0$. The curve E defined by

$$s^2 = f(t)$$

is isomorphic with E' and hence has no complex multiplication. Furthermore, $f(a_1) = 0$.

Let $h = (t - a_2), \ldots, (t - a_n)$ and construct the curve E_0' as in Lemma 4.1. Note that the curve E_0' is defined over $\mathbf{Q}(a_1, \ldots, a_n)(t)$. Hence, the set of points of E_0' with coordinates in R, denoted by $E_0'(R)$, is an $\mathcal{L}_n$-Diophantine set.

Now we claim that the following equivalence holds:

$$\begin{aligned} z \in \mathbf{Z} \quad \leftrightarrow \quad & \exists\, x, y, u, v, w \in R \\ & z \in k \wedge (u, v) \in E_0' && (1) \\ & \wedge\, (x, y) \in E_0' && (2) \\ & \wedge\, (x, y) = 2(u, v) + (t, 1) && (3) \\ & \wedge\, w = \omega h^7 \frac{x - h^3 a_1}{(t - a_1)y} && (4) \\ & \bigwedge_{i=1}^{n} \operatorname{ord}_{a_i}(h(w - h^7(2z + 1))) > 0 && (5) \end{aligned}$$

where $\omega = h(a_1)$. First note that, in virtue of Lemma 4.3, the right-hand side of this equivalence is indeed $\mathcal{L}_n$-Diophantine. So once the equivalence is proved, the theorem will be proven.

We now prove the equivalence. Suppose that z is an integer, then obviously (1) is satisfied. Choose $(u, v) = (X_z, Y_z)$ or $(u, v) = (X_z, Y_z) + (h^3 a_1, 0)$, depending on whether z is odd or even and set $(x, y) = (X_{2z+1}, Y_{2z+1})$. It follows from Lemma 4.1 that (u, v) and (x, y) are indeed elements of $E_0'(R)$. Furthermore Lemma 4.2 implies that w is in R. Now note that $w(a_1) = h(a_1)^7(2z + 1)$, hence $\operatorname{ord}_{a_1}(h(w - h^7(2z + 1))) > 0$, and since $w - h^7(2z + 1)$ has no poles at any of the a_is, $i = 2, \ldots, n$, it follows that (5) is satisfied. So if z is an integer, the right-hand side of the equivalence can be satisfied.

Conversely, suppose that the right-hand side of this equivalence is satisfied, then it follows from conditions (2) and (3) and Lemma 4.1 that $(x, y) = (X_{2l+1}, Y_{2l+1})$ for some integer l. Now by (5), the fact that z is a constant and the fact that h has no zero at a_1, it follows that $\alpha^7(2z + 1) = w(a_1) = \alpha^7(2l + 1)$. So $2l + 1 = 2z + 1$, and hence, z is an integer. □

References

[1] Denef, J., "The Diophantine problem for polynomial rings and fields of rational functions," *Transactions of the American Mathematical Society*, vol. 242 (1978), pp. 391–99. Zbl 0399.10048. MR 58:10809. 182, 183, 185

[2] Kim, K. H., and F. W. Roush, "Diophantine undecidability of $\mathbf{C}(t_1, t_2)$," *Journal of Algebra*, vol. 150 (1992), pp. 35–44. Zbl 0754.11039. MR 93h:03062. 182

[3] Kim, K. H., and F. W. Roush, "Diophantine unsolvability for function fields over certain infinite fields of characteristic p," *Journal of Algebra*, vol. 152 (1992), pp. 230–39. Zbl 0768.12008. MR 93k:11114. 182

[4] Kim, K. H., and F. W. Roush, "Diophantine unsolvability over p-adic function fields," *Journal of Algebra*, vol. 176 (1995), pp. 83–110. Zbl 0858.12006. MR 96f:11165. 182

[5] Matijasevich, Y., "Enumerable sets are Diophantine," *Doklady Akademii Nauka SSSR*, vol. 191 (1970), pp. 272–82. 181

[6] Matsumura, H., *Commutative Algebra*, W. A. Benjamin, Inc., New York, 1970. Zbl 0211.06501. MR 42:1813. 184

[7] Pheidas, T., "Hilbert's Tenth Problem for fields of rational functions over finite fields," *Inventiones Mathematicae*, vol. 103 (1991), pp. 1–8. Zbl 0696.12022. MR 92e:11145. 182

[8] Pheidas, T., and K. Zahidi, "Undecidable existential theories of polynomial rings and function fields," *Communications in Algebra*, vol. 27 (1999), pp. 4993–5010. Zbl 0934.03014. MR 2000f:03125. 182, 185, 186

[9] Poonen, B., "Hilbert's Tenth Problem and Mazur's Conjecture for large subrings of $\mathbb{Q}$," preprint, 2003 183

[10] Robinson, J., "Definability and decision problems in arithmetic," *The Journal of Symbolic Logic*, vol. 14 (1949), pp. 98–114. Zbl 0034.00801. MR 11,151f. 183

[11] Robinson, J., "The undecidability of algebraic rings and fields," *Proceedings of the American Mathematical Society*, vol. 10 (1959), pp. 950–57. Zbl 0100.01501. MR 22:3691. 183

[12] Rumely, R. S., "Undecidability and definability for the theory of global fields," *Transactions of the American Mathematical Society*, vol. 262 (1980), pp. 195–217. Zbl 0472.03010. MR 81m:03053. 183

[13] Shlapentokh, A., "Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator," *Inventiones Mathematicae*, vol. 129 (1997), pp. 489–507. Zbl 0887.11053. MR 98h:11163. 183

[14] Shlapentokh, A., "Diophantine definability over holomorphy rings of algebraic function fields with infinite number of primes allowed as poles," *International Journal of Mathematics*, vol. 9 (1998), pp. 1041–66. Zbl 0920.11080. MR 99k:11190. 183

[15] Silverman, J. H., *The Arithmetic of Elliptic Curves*, vol. 106 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1986. Zbl 0585.14026. MR 87g:11070. 184

Acknowledgments

The author was supported through a Marie Curie Individual Fellowship (Contract MPMF-CT-2001-01384)

Equipe de Logique Mathématique
UFR de Mathématiques (Case7012)
Université Denis Diderot Paris VII
2 Place Jussieu
75251 Paris Cedex 05
FRANCE
zahidi@logique.jussieu.fr