Hilbert's Tenth Problem for function fields of varieties over number fields and p-adic fields [☆]

Kirsten Eisenträger

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109, USA

Received 21 April 2005

Available online 8 December 2006

Communicated by Laurent Moret-Bailly

Abstract

Let k be a subfield of a p-adic field of odd residue characteristic, and let $\mathcal{L}$ be the function field of a variety of dimension $n \geqslant 1$ over k. Then Hilbert's Tenth Problem for $\mathcal{L}$ is undecidable. In particular, Hilbert's Tenth Problem for function fields of varieties over number fields of dimension $\geqslant 1$ is undecidable.
© 2006 Elsevier Inc. All rights reserved.

Keywords: Hilbert's Tenth Problem; Undecidability; Elliptic curves; Quadratic forms

1. Introduction

Hilbert's Tenth Problem in its original form was to find an algorithm to decide, given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in the ring $\mathbb{Z}$ of integers, whether it has a solution with $x_1, \ldots, x_n \in \mathbb{Z}$. Matijasevič [12], building on earlier work by Davis, Putnam, and Robinson [4], proved that no such algorithm exists, i.e. Hilbert's Tenth Problem is undecidable.

Since then, analogues of this problem have been studied by asking the same question for polynomial equations with coefficients and solutions in other commutative rings R. We refer to this as *Hilbert's Tenth Problem over R*. Perhaps the most important unsolved question in this area is Hilbert's Tenth Problem over the field of rational numbers. The function field analogue, namely Hilbert's Tenth Problem for the function field k of a curve over a finite field, is undecidable. This was proved by Pheidas for $k = \mathbb{F}_q(t)$ with q odd [14], and by Videla [20] for $\mathbb{F}_q(t)$ with

---

q even. Shlapentokh [17] generalized Pheidas' result to finite extensions of $\mathbb{F}_q(t)$ with q odd and to certain function fields over possibly infinite constant fields of odd characteristic, and the remaining cases in characteristic 2 are treated in [7]. Hilbert's Tenth Problem is also known to be undecidable for several rational function fields of characteristic zero: In 1978 Denef proved the undecidability of Hilbert's Tenth Problem for rational function fields over formally real fields [5], and he was the first to use rank one elliptic curves to prove undecidability. Kim and Roush [9] showed that the problem is undecidable for the purely transcendental function field $\mathbb{C}(t_1, t_2)$ and in [8] their approach was generalized to finite extensions of $\mathbb{C}(t_1, \ldots, t_n)$ for $n \geqslant 2$. Kim and Roush [10] proved that the problem was undecidable for rational function fields $k(t)$, where k is a subfield of a p-adic field of odd residue characteristic. In this paper we will generalize their result to finite extensions of the rational function field in n variables over k with $n \geqslant 1$. In particular, we show that Hilbert's Tenth Problem for function fields of varieties over number fields of dimension $\geqslant 1$ is undecidable.

In Hilbert's Tenth Problem the coefficients of the equations have to be input into a Turing machine, so we restrict the coefficients to a subring A of R which is finitely generated as a $\mathbb{Z}$-algebra. We say that *Hilbert's Tenth Problem for R with coefficients in A* is undecidable if there is no algorithm that decides whether or not multivariate polynomial equations with coefficients in A have a solution in R.

Our theorem considers fields which are extensions of the rational function field $\mathbb{Q}_p(\tau)$. Since $\mathbb{Q}_p(\tau)$ is uncountable, its elements cannot be coded into a Turing machine. So just to get a non-trivial problem, we have to restrict the ring of coefficients as explained above. Let k be a subfield of a p-adic field and let $\mathcal{L}$ be a finite extension of the rational function field $k(\tau, \tau_2, \ldots, \tau_n)$, which is given via the minimal polynomial of a generator α over $k(\tau, \tau_2, \ldots, \tau_n)$. (For simplicity of notation, we assume that $\mathcal{L}/k(\tau, \tau_2, \ldots, \tau_n)$ is given to us in terms of *one* generator α.) We will choose the ring of coefficients in terms of the given transcendentals $\tau, \tau_2, \ldots, \tau_n$ and α, and we want to choose this ring as small as possible. We will define a field κ such that $\kappa(\tau)$ contains the coefficients of the minimal polynomial of α, and we will choose the ring of coefficients to be a subring of $\kappa(\tau)$. The field κ will be defined in Section 3. We will prove the following theorem.

Theorem 1.1. *Let k be a subfield of a finite extension of $\mathbb{Q}_p$ with p odd. Let $\mathcal{L}$ be a finite extension of the rational function field $k(\tau, \tau_2, \ldots, \tau_n)$. There exists a finite set $\{c_1, \ldots, c_\ell\}$ of elements of $\kappa(\tau)$, not all constant, such that Hilbert's Tenth Problem for $\mathcal{L}$ with coefficients in $\mathbb{Z}[c_1, \ldots, c_\ell]$ is undecidable.*

Notation. In the following we will let A_0 be the ring of coefficients of Theorem 1.1, and $k(\tau_1, \ldots, \tau_n)$ will denote the field of rational functions over k in n variables $\tau_1, \ldots, \tau_n$. We refer to a subfield k of a finite extension F of $\mathbb{Q}_p$ as a *p-adic field*, and we assume that k is given together with an embedding into F. The p-adic valuation on F induces a valuation on k, which we normalize so that the value group of k is $\mathbb{Z}$. For an integral domain R, we denote its field of fractions of R by $\mathrm{Frac}(R)$.

1.1. Idea of proof

First we will define two notions that will appear frequently in the remainder of this paper.

Definition 1.2.

(1) If R is a commutative ring, a *diophantine equation over R* is an equation $f(x_1, \ldots, x_n) = 0$ where f is a polynomial in the variables $x_1, \ldots, x_n$ with coefficients in R.
(2) A subset S of R^k is *diophantine over R* if there exists a polynomial $f(x_1, \ldots, x_k, y_1, \ldots, y_m) \in R[x_1, \ldots, x_k, y_1, \ldots, y_m]$ such that

$$S = \big\{ (x_1, \ldots, x_k) \in R^k \colon \exists y_1, \ldots, y_m \in R, \ \big(f(x_1, \ldots, x_k, y_1, \ldots, y_m) = 0 \big) \big\}.$$

Let A be a subring of R and suppose that f can be chosen such that its coefficients are in A. Then we say that S is *diophantine over R with coefficients in A*.

We will prove Theorem 1.1 by constructing a diophantine model of the integers with addition and multiplication over $\mathcal{L}$. A *diophantine model* is defined as follows:

Definition 1.3. A *diophantine model* of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ over $\mathcal{L}$ is a diophantine subset $S \subseteq \mathcal{L}^m$ for some m, equipped with a bijection $\phi \colon \mathbb{Z} \to S$ such that under ϕ, the graphs of addition and multiplication correspond to diophantine subsets of S^3.

Let A be a subring of $\mathcal{L}$. A *diophantine model* of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ over $\mathcal{L}$ *with coefficients in A* is a diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$, where in addition S and the graphs of addition and multiplication are diophantine over $\mathcal{L}$ with coefficients in A.

Since Hilbert's Tenth Problem over $\mathbb{Z}$ is undecidable, it follows that the structure $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ has an undecidable existential theory. Hence constructing a diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ over $\mathcal{L}$ with coefficients in $A_0 = \mathbb{Z}[c_1, \ldots, c_\ell]$ is enough to prove that Hilbert's Tenth Problem for $\mathcal{L}$ with coefficients in A_0 is undecidable. We have to check that the diophantine definition of the set S which is in bijection to $\mathbb{Z}$ and the diophantine definitions of addition and multiplication have coefficients in A_0. We specify the ring A_0 in Sections 7 and 8.

We will use the rational points on a rank one elliptic curve over $\mathcal{L}$ as our set S. This elliptic curve is constructed in Section 4. In Section 5 we will generalize a theorem in [10] to construct a diophantine set over $\mathcal{L}$ whose intersection with $\mathbb{Q}$ is dense in any finite product of p-adic fields. In Section 6 we prove a result about quadratic forms that will be needed in the proof of Theorem 1.1. In Section 7 we address the ring of coefficients A_0, and in Section 8 we prove Theorem 1.1. We will first prove Theorem 1.1 when $\mathcal{L}/k$ has transcendence degree one, and then generalize it to higher transcendence degree.

Note. When she was completing the proof of Theorem 1.1 the author worked with an earlier version of [13] that did not contain the section on p-adic fields.

2. Preliminaries

We need two general facts about diophantine equations that allow us to combine several diophantine equations into one.

Lemma 2.1. *Let R be an integral domain. Let A be a subring of R, and assume that* Frac R *does not contain the algebraic closure of* Frac(A). *Then for each system*

$f_1(x_1, \ldots, x_n) = 0, \ldots, f_k(x_1, \ldots, x_n) = 0$ *of diophantine equations with coefficients in A there exists a single diophantine equation* $g(x_1, \ldots, x_n) = 0$ *with coefficients in A such that the system of the* f_i's *has a solution in R if and only if g has a solution in R.*

Proof. We will show how to combine two equations into one, which is enough. Let $h(x)$ be a polynomial in one variable with coefficients in A which has no zero in R. Let $\tilde{h}(x, y)$ be the homogenization of h. Then for all x and y in R, $\tilde{h}(x, y) = 0$ if and only if $x = 0$ and $y = 0$. Hence for $\vec{x} \in R^n$

$$\big(f_1(\vec{x}) = 0 \wedge f_2(\vec{x}) = 0\big) \quad \Longleftrightarrow \quad \big(\tilde{h}\big(f_1(\vec{x}), f_2(\vec{x})\big) = 0\big). \qquad \square$$

Remark 2.2. Similarly, if R is an integral domain and $f_1 = 0$, and $f_2 = 0$ are diophantine equations with coefficients in some subring A of R, then

$$f_1 = 0 \vee f_2 = 0 \quad \Longleftrightarrow \quad f_1 \cdot f_2 = 0,$$

and $f_1 \cdot f_2$ has coefficients in A.

3. Algebraic function fields

An *algebraic function field* in one variable over F is a field K containing F and at least one transcendental element τ such that $K/F(\tau)$ is a finite algebraic extension, and such that F is algebraically closed in K. The field F is the *constant field* of K. Whenever K/F is an algebraic function field, we fix an algebraic closure $\overline{K}$ of K. For any field $E \subseteq \overline{K}$, we set KE equal to the *compositum* of K and E inside $\overline{K}$.

We first need a general theorem about extensions of function fields.

Theorem 3.1. *Let* K/F *be a function field of characteristic zero with constant field F. Let E be an extension of F, and let $L = KE$. Let $\mathcal{T}$ be a prime of L lying above a prime $\mathfrak{T}$ of K. Let $L_{\mathcal{T}}$ and $K_{\mathfrak{T}}$ be the corresponding residue fields.*

(1) *If E/F is finite, then $L_{\mathcal{T}}$ is the composite of the two subfields $K_{\mathfrak{T}}$ and E.*
(2) *If E is algebraically closed in L and $E \cap K = F$, then $L_{\mathcal{T}} = K_{\mathfrak{T}} E$.*

Proof. The first part is proved in [16, p. 106], and the second part is proved in [6, p. 128]. $\square$

3.1. Definition of the field κ

Assume that k is a field of characteristic zero and that $\mathcal{L}/k$ is an algebraic function field with constant field k. We will assume that $\mathcal{L}$ is specified as $k(\tau)(\alpha)$, where τ is transcendental over k and α generates $\mathcal{L}$ over $k(\tau)$. Let $\beta_1, \ldots, \beta_n \in k(\tau)$ be the coefficients of the minimal polynomial of α. Then $\beta_i = p_i(\tau)/q_i(\tau)$, with $p_i, q_i \in k[\tau]$. Let κ be the subfield of k generated by the coefficients of all the $p_i, q_i, i = 1, \ldots, n$. Then κ is a finitely generated extension of $\mathbb{Q}$, and $\kappa(\tau)$ contains the coefficients of the minimal polynomial of α. Let K be the subfield of $\mathcal{L}$ defined by $K := \kappa(\tau, \alpha)$. By construction, the field K is an algebraic function field with constant field κ.

Proposition 3.2. *The field $\mathcal{L}/k$ is a constant field extension of K/κ, i.e. $Kk = \mathcal{L}$, and $k \cap K = \kappa$.*

Proof. We have $Kk = \mathcal{L}$ by construction. It remains to show that $k \cap K = \kappa$. We will show this by showing that k is linearly disjoint from K over κ. By [6, Lemma 3, p. 123] applied to $\kappa \subset \kappa(\tau) \subset K$ and $\kappa \subset k$, it suffices to show that $\kappa(\tau)$ is linearly disjoint from k over κ, and that $k(\kappa(\tau)) = k(\tau)$ is linearly disjoint from K over $\kappa(\tau)$. Since τ is transcendental over k, $\kappa(\tau)$ is linearly disjoint from k over κ [6, Lemma 2(a), p. 122]. By construction of κ and K, $\mathcal{L} = k(\tau)(\alpha)$, $K = \kappa(\tau)(\alpha)$, and $[k(\tau)(\alpha) : k(\tau)] = [\kappa(\tau)(\alpha) : \kappa(\tau)]$. Hence $k(\tau)$ is linearly disjoint from K over $\kappa(\tau)$ by [6, Lemma 1, p. 122]. $\square$

Proposition 3.3. *Let $K/\kappa(\tau)$ and $\mathcal{L}/k(\tau)$ be as before, and assume that there is a prime $\mathcal{T}$ of K above τ which is unramified. Then there exists a prime $\mathcal{T}'$ of $\mathcal{L}$ above τ which is unramified.*

Moreover, there exists a finite extension κ_1 of κ such that in the compositum of $\mathcal{L}$ and $k\kappa_1$, the residue field of any prime extending $\mathcal{T}'$ is $k\kappa_1$.

Proof. By Proposition 3.2, the extension $\mathcal{L}/k$ is a constant field extension of K/κ. Hence the prime $\mathcal{T}'$ of $\mathcal{L}$ extending $\mathcal{T}$ is unramified [6, p. 113], and hence $\mathcal{T}'$ over τ is unramified.

Let $K_{\mathcal{T}}$ be the residue field of the prime $\mathcal{T}$ of K. Then $K_{\mathcal{T}}$ is a finite extension of κ. By Theorem 3.1(2), the residue field $\mathcal{L}_{\mathcal{T}'}$ of the prime $\mathcal{T}'$ above $\mathcal{T}$ is $K_{\mathcal{T}}k$. Similarly, let k' be a finite extension of k, and let $\mathfrak{Q}$ be a prime of $\mathcal{L}k'$ extending $\mathcal{T}'$. By Theorem 3.1(1), the residue field of $\mathfrak{Q}$ is the compositum of $\mathcal{L}_{\mathcal{T}'}$ and k'. Now let κ_1 be a finite (normal) extension of κ, such that $K_{\mathcal{T}}\kappa_1 = \kappa_1$. Then by the above arguments, κ_1 has the right properties. $\square$

3.2. Higher transcendence degree

When $\mathcal{L}$ is a finite extension of $k(\tau, \tau_2 \ldots, \tau_n)$ (with k algebraically closed in $\mathcal{L}$), which is given as $\mathcal{L} = k(\tau, \tau_2, \ldots, \tau_n)(\alpha)$, then the coefficients β_i of the minimal polynomial of α over $k(\tau, \tau_2, \ldots, \tau_n)$ are elements of $k(\tau, \tau_2, \ldots, \tau_n)$. So each β_i is of the form

$$\beta_i = p_i(\tau, \tau_2, \ldots, \tau_n)/q_i(\tau, \tau_2, \ldots, \tau_n) \quad \text{with } p_i, q_i \in k[\tau, \tau_2, \ldots, \tau_n].$$

Let κ_0 be the subfield of k which is generated by the coefficients of the p_i, q_i.

Proposition 3.4. *Let k_1 be the algebraic closure of $k(\tau_2, \ldots, \tau_n)$ in $\mathcal{L}$. There exists a finite extension κ of $\kappa_0(\tau_2, \ldots, \tau_n)$ and a finite extension K of $\kappa(\tau)$ such that the algebraic function field $\mathcal{L}/k_1$ is a constant field extension of K/κ.*

Proof. The field k_1 is a finite extension of $k(\tau_2, \ldots, \tau_n)$. The coefficients of the minimal polynomial of α over $k_1(\tau)$ are algebraic over $\kappa_0(\tau, \tau_2, \ldots, \tau_n)$, and generate some finite extension K_1 of $\kappa_0(\tau, \tau_2, \ldots, \tau_n)$ which is contained in $k_1(\tau)$. Let $K := K_1(\alpha) \subseteq \mathcal{L}$, and let κ be the algebraic closure of $\kappa_0(\tau_2, \ldots, \tau_n)$ in K.

Then with the same argument as in the proof of Proposition 3.2, the algebraic function field $\mathcal{L}/k$ is a constant field extension of K/κ. $\square$

Remark 3.5. Exactly the same proof as the proof of Proposition 3.3 shows that Proposition 3.3 also holds for the extension $\mathcal{L}/k_1(\tau)$ of $K/\kappa(\tau)$.

4. Elliptic curve setup

To construct a diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ over $\mathcal{L}$ with coefficients in A_0 we need a diophantine set $\mathcal{S}$ and a bijection $\mathbb{Z} \to \mathcal{S}$. We will choose as our set $\mathcal{S}$ the $\mathcal{L}$-rational points on an elliptic curve $\mathcal{E}_0$, and so we need an elliptic curve $\mathcal{E}_0$ over $\mathcal{L}$ of rank one. The following theorem uses a theorem by Moret-Bailly [13, Theorem 1.8] and allows us to construct elliptic curves of rank one:

Theorem 4.1. *Let k be a field of characteristic zero, and let $\mathcal{L}$ be a finite extension of the rational function field $k(\tau)$. Let κ and K be as in Proposition 3.3, and let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and with Weierstrass equation*

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{Q}$, $b \neq 0$. Then there exists a nonconstant element $T \in K$ such that the elliptic curve given by the affine equation

$$\mathcal{E}: \quad \left(T^3 + aT + b\right)Y^2 = X^3 + aX + b$$

has rank one over $\mathcal{L}$ with generator $(T, 1)$ modulo 2-torsion. Moreover, T can be chosen such that the extension $\mathcal{L}/k(T)$ is unramified above the primes T, T^{-1} of $k(T)$.

Proof. Let C_0 be a smooth projective geometrically connected curve over κ with function field K.

To get the desired element T, pick an "admissible element" $f \in K$ [13, Definition 1.5.2], pick an element $\lambda \in \mathbb{Z} \cap \mathrm{GOOD}(\kappa)$ [13, Theorem 1.8], and let $T := \lambda \cdot f$. Then $\mathcal{E}(K)$ is generated by $(T, 1)$. Since T is admissible in the sense of [13, Definition 1.5.2], it follows that $T : C_0 \to \mathbb{P}^1_\kappa$ is étale above 0 and ∞.

Moreover, the group $\mathcal{E}(\mathcal{L})$ is generated by $(T, 1)$: Indeed, the field k is an extension of κ, and by [13, Corollary 1.5.5(ii)], $\mathrm{GOOD}(k) \cap \kappa = \mathrm{GOOD}(\kappa)$, so $T \in \mathrm{GOOD}(k)$. By the definition of "GOOD," this means that the natural inclusion $\mathcal{E}(k(T)) \hookrightarrow \mathcal{E}(\mathcal{L})$ is a bijection, so $\mathcal{E}(\mathcal{L})$ is generated by $(T, 1)$. □

Note. Our notation follows Moret-Bailly's equivalent setup in his preprint of [13] from December 2003: We assume that the polynomial $R(t)$ defining Γ in 1.4.4 is without multiple roots and satisfies $R(0) \neq 0$. We are also in the situation $\Gamma = E$, but the double cover π is given by the x-coordinate. With this notation, we have $R(t) = P(t)$ and the twisted curve $y^2 = R(t)P(x)$ in [13, 1.4.6] is isomorphic to $R(t)y^2 = P(x)$ (which is the twist that we use) via $(X, Y) \mapsto (X, Y/R(t))$.

Notation. For $k, \mathcal{L}, T, \mathcal{E}$ as above let $P := (T, 1)$. Let $P_m := m \cdot (T, 1) = (X_m, Y_m)$, and for $m \neq 0$ let $\psi_m := X_m/TY_m$.

Since $\psi_m \in k(T)$, we can interpret ψ_m as a function on the projective line. We will need a proposition by Denef, which determines $\psi_m(\infty)$.

Proposition 4.2. *The function ψ_m takes the value m at ∞. I.e., when we expand ψ_m as a power series in T^{-1}, the constant term is m.*

Proof. This is Lemma 3.2 in [5, p. 396]. □

In the proof of Theorem 1.1 we will need more properties of the points on the elliptic curve, so we will work with a specific curve that has these properties. From now on we will fix E_0 to be the smooth projective model of

$$y^2 = x^3 + x + 1.$$

Then E_0 has no complex multiplication, and the point $(0, 1) \in E_0(k)$ has infinite order [3, 496A1]. We will fix an element $T \in \mathcal{L}$ as in Theorem 4.1. Let $\mathcal{E}_0$ be the elliptic curve given by

$$\mathcal{E}_0: \quad (T^3 + T + 1)Y^2 = X^3 + X + 1.$$

By our choice of T, a generator for $\mathcal{E}_0(\mathcal{L})$ (modulo 2-torsion) is $(T, 1)$.

Lemma 4.3. *Given $E_0, \mathcal{E}_0$, let ψ_m be defined as above. Given $m, n, r \in \mathbb{Z} - \{0, 1, -1\}$, let*

$$u := u_{(m,n,r)} = \psi_m \psi_n - \psi_r + (1/2) \cdot T^{-1},$$

$$v := v_{(m,n,r)} = \psi_m \psi_n - \psi_r + (1/3) \cdot T^{-1}.$$

Let ord_T, $\mathrm{ord}_{T^{-1}}$ be the discrete valuations on $k(T)$ associated to T, T^{-1}, normalized so that the value group is $\mathbb{Z}$. Then

(1) $\mathrm{ord}_T(u) = -2$, $\mathrm{ord}_T(v) = -2$.
(2) $n \cdot m = r$ *if and only if* $(\mathrm{ord}_{T^{-1}}(u) = 1$ *or* $\mathrm{ord}_{T^{-1}}(v) = 1)$.
     $n \cdot m \neq r$ *if and only if* $(\mathrm{ord}_{T^{-1}}(u) = 0$ *and* $\mathrm{ord}_{T^{-1}}(v) = 0)$.

Proof. (1) When we reduce the equation of the curve $\mathcal{E}_0$ modulo T we just obtain E_0, so the reduction of $\mathcal{E}_0/k(T)$ modulo T gives us the nonsingular curve E_0/k. We have a map $\pi : \mathcal{E}_0 \to E_0$ that sends a point $Q \in E_0(k(T))$ to a point $\tilde{Q}$, its reduction modulo T, and this map is a group homomorphism. The reduction of the point $P = (T, 1)$ on $\mathcal{E}_0$ is the point $(0, 1)$ on E_0, and since $(0, 1)$ has infinite order, this means that no nonzero multiple of P can map to **O**. Hence X_m, Y_m have nonnegative order at T for all $m \in \mathbb{Z} - \{0\}$. Since the reduction of P has infinite order it follows that Y_m has order zero at T. If X_m has positive order at T, then under π it gets mapped to a point on E_0 whose x-coordinate is zero. The only such points on E_0 are $(0, 1)$ and $(0, -1)$ which are the images of P_1 and P_{-1}, respectively. Since $(0, 1) \in E_0(k)$ has infinite order and since π is a group homomorphism this implies that no other multiples of P can reduce to $(0, \pm 1)$. So for $m \in \mathbb{Z} - \{0, 1, -1\}$ we have that X_m, Y_m have order 0 at T. Hence for all $m \in \mathbb{Z} - \{0, 1, -1\}$, ψ_m has order -1 at T, and so $u = \psi_m \psi_n - \psi_r + (1/2) \cdot T^{-1}$ has order -2 at T. Similarly, $\mathrm{ord}_T(v) = -2$.

(2) If $n \cdot m = r$, then by Proposition 4.2, $\psi_m \psi_n - \psi_r$ has nonnegative order in T^{-1} and the constant coefficient cancels, so the order at T^{-1} is positive. Hence at least one of the power series expansion of u and v in T^{-1} has a linear term, and so $\mathrm{ord}_{T^{-1}}(u) = 1$ or $\mathrm{ord}_{T^{-1}}(v) = 1$.

If $n \cdot m \neq r$, then by Proposition 4.2, $\psi_m \psi_n - \psi_r$ has nonnegative order in T^{-1} and the constant term in the power series expansion in T^{-1} is nonzero. Hence $\mathrm{ord}_{T^{-1}}(u) = 0$, $\mathrm{ord}_{T^{-1}}(v) = 0$. □

5. A set, diophantine over $\mathcal{L}$, which is dense in any finite product of p-adic fields

The goal of this section is to prove Theorem 5.5, which will be needed in the proof of Theorem 1.1.

Proposition 5.1. *Let k be a field of characteristic zero, and let $\mathcal{L}$ be a finite extension of the rational function field $k(T)$. Assume that k is algebraically closed in $\mathcal{L}$. There exists a finite set $\mathcal{A}$ of elliptic curves over $\mathbb{Q}$ with the property that if $E/\mathbb{Q}$ is an elliptic curve which is not $\overline{\mathbb{Q}}$ isogenous to any of the curves in $\mathcal{A}$, then $E(k) = E(\mathcal{L})$.*

Proof. Let C be a smooth, projective, geometrically connected curve defined over k whose function field is $\mathcal{L}$. Let E be an elliptic curve defined over $\mathbb{Q}$. A nonconstant point $P \in E(\mathcal{L})$ corresponds to a nonconstant morphism $\alpha : C \to E$ defined over k. The morphism α induces a nonzero homomorphism $\beta : \mathrm{Jac}(C) \to \mathrm{Jac}(E) \cong E$ defined over k. We can decompose $\mathrm{Jac}(C)$ into simple factors over k. In order to have a nonzero homomorphism $\beta : \mathrm{Jac}(C) \to \mathrm{Jac}(E)$ one of the simple factors A_0 of $\mathrm{Jac}(C)$ has to be k-isogenous to E. So if E is not k-isogenous to any of the k-simple factors of $\mathrm{Jac}(C)$, then $E(k) = E(\mathcal{L})$.

If two elliptic curves E_0, E_1 defined over $\mathbb{Q}$ are both k-isogenous to a simple factor A of $\mathrm{Jac}(C)$, then E_0 and E_1 are k-isogenous. But then E_0 and E_1 must already be isogenous over $\overline{\mathbb{Q}}$ [2, Theorem 2.1]. So requiring that an elliptic curve $E/\mathbb{Q}$ not be isogenous to any of the simple factors of $\mathrm{Jac}(C)$ over k excludes finitely many $\overline{\mathbb{Q}}$ isogeny classes of elliptic curves defined over $\mathbb{Q}$.   □

Remark 5.2. We can use a similar argument as above to prove Proposition 5.1 when $\mathcal{L}$ is a finite extension of the rational function field $k(T_1, \dots, T_n)$ in n variables with k algebraically closed in $\mathcal{L}$:

Let $k_i := k(T_1, \dots, \hat{T}_i, \dots, T_n)$ for $i = 1, \dots, n$. (Here $\hat{T}_i$ means that T_i is omitted.) For $i = 1, \dots, n$, let K_i be the algebraic closure of k_i in $\mathcal{L}$ and let C_i be a smooth, projective, geometrically connected curve defined over K_i whose function field is $\mathcal{L}$. Let $E/\mathbb{Q}$ be an elliptic curve. A nonconstant point $P \in E(\mathcal{L})$ will have coordinates transcendental over some K_i $(i \in \{1, \dots, n\})$, inducing a nonconstant morphism $\alpha_i : C_i \to E$ defined over K_i. This gives a nonzero homomorphism $\beta_i : \mathrm{Jac}(C_i) \to E$ defined over K_i. As argued above, requiring that E not be K_i-isogenous to any of the simple-factors of $\mathrm{Jac}(C_i)$ excludes finitely many $\overline{\mathbb{Q}}$ isogeny classes of elliptic curves over $\mathbb{Q}$. Hence excluding all elliptic curves $E/\mathbb{Q}$ which are K_i-isogenous to some factor of $\mathrm{Jac}(C_i)$ for some $i \in \{1, \dots, n\}$ still only excludes finitely many $\overline{\mathbb{Q}}$ isogeny classes.

Proposition 5.3. *Let $E/\mathbb{Q}$ be an elliptic curve with global minimal Weierstrass equation*

$$E: \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Assume that $E(\mathbb{Q})$ is infinite. Let $S := \{x/y : (x, y) \in E(\mathbb{Q}),\ y \neq 0\}$, and $U := \{s_1/s_2 : s_1, s_2 \in S,\ s_2 \neq 0\}$.

(1) *Let p be a prime. The p-adic closure of S in $\mathbb{Q}_p$ contains a neighborhood of the origin, and U is dense in $\mathbb{Q}_p$.*

(2) *Let $p_1, \ldots, p_r$ be a finite set of primes. The closure of the set S (embedded into $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$ diagonally) contains a neighborhood of the origin, and U is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$.*

Proof. (1) Consider the curve E as a curve over $\mathbb{Q}_p$, and let $\tilde{E}_{ns}(\mathbb{F}_p)$ be the nonsingular part of the reduction of E modulo p. Let $P \mapsto \tilde{P}$ be the reduction map as in [19, p. 173]. Let $E_1(\mathbb{Q}_p) :=$ $\{P \in E(\mathbb{Q}_p) : \tilde{P} = \tilde{\mathbf{O}}\}$, and let $P_0 \in E(\mathbb{Q})$ be a point of infinite order. Some multiple of P_0 reduces to the identity, say $m\tilde{P}_0 = \tilde{\mathbf{O}}$. Let $\hat{E}/\mathbb{Z}_p$ be the formal group associated to E. Then $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p)$ (as groups) via $(x, y) \mapsto -(x/y)$ [19, p. 175]. Hence the subgroup of $E(\mathbb{Q}_p)$ generated by mP_0 corresponds to an infinite subgroup G of the formal group. Since the formal group associated to an elliptic curve is a one-dimensional compact p-adic Lie group, it follows that the closure of G (and hence the closure of S) contains a neighborhood of the origin.

Since the closure of S contains $p^n\mathbb{Z}_p$, it follows immediately that U is dense in $\mathbb{Q}_p$.

(2) We can take a large enough multiple mP_0 of the point $P_0 \in E(\mathbb{Q})$ of infinite order such that mP_0 reduces to the identity in the nonsingular part of the reduction of E modulo p_i for $i = 1, \ldots, r$. Let $R := \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$. The subgroup of $E(\mathbb{Q})$ generated by mP_0 corresponds to an additive subgroup M of R via

$$P = (x, y) \mapsto (x/y, \ldots, x/y).$$

Let $\overline{M}$ be the closure of M in R. Then $\overline{M}$ is stable under multiplication by $\mathbb{Z}$. By the strong approximation theorem [1, p. 67] $\mathbb{Z}$ is dense in R, so it follows that $\overline{M}$ is stable under multiplication by elements of R. So $\overline{M}$ is an ideal of $R = \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_r}$. Then $\overline{M} = I_1 \times \cdots \times I_r$, with I_i an ideal of $\mathbb{Z}_{p_i}$. By part (1) the ith projection of $\overline{M}$ contains a neighborhood of the origin, so all the I_i's are nonzero ideals of $\mathbb{Z}_{p_i}$, i.e. $I_i = p_i^{n_i}\mathbb{Z}_{p_i}$. Hence $\overline{M}$ contains a neighborhood of the origin, and U is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$.   □

Theorem 5.4. *Let F be a number field, E_0/F an elliptic curve without geometric complex multiplication. Let F' be an extension of F. The set of F-isomorphism classes of elliptic curves E/F which are F'-isogenous to E_0 is finite up to quadratic twist. I.e., the set of possible j-invariants for E is finite.*

Proof. By replacing F' with an extension we may assume that F' is algebraically closed. Then $F' \supseteq \overline{F}$. If two elliptic curves over F become isogenous over F' then they are already isogenous over $\overline{F}$ [2, Theorem 2.1], so we may assume $F' = \overline{F}$. Let E/F be an elliptic curve as in the theorem, so E_0 and E are $\overline{F}$-isogenous. Let $G_F := \text{Gal}(\overline{F}/F)$. Since E_0 does not have geometric complex multiplication, $\text{Hom}_{\overline{F}}(E_0, E)$ is a free $\mathbb{Z}$-module of rank one. Thus, the natural continuous action by G_F is through $G_F \to \text{Aut}(\text{Hom}_{\overline{F}}(E_0, E)) = \mathbb{Z}^\times = \langle \pm 1 \rangle$. That is, E_0 and E become isogenous over a quadratic extension K of F. Let E' be the twist of E by the quadratic character χ associated with K/F.

We can show that over F, E_0 is isogenous either to E or to E': To see this, assume that E_0 is not isogenous to E over F. Then the nontrivial F-automorphism of K, σ, acts by -1 on $\text{Hom}_{\overline{F}}(E_0, E)$. Since E is not isogenous to E' over F, σ also acts by -1 on $\text{Hom}_{\overline{F}}(E, E')$. Hence, after composing we see that σ acts trivially on $\text{Hom}_{\overline{F}}(E_0, E')$, i.e. E_0 is F-isogenous to E'.

But by a theorem of Shafarevich (see [19, IX.6]) there are only finitely many F-isomorphism classes of elliptic curves defined over F which are F-isogenous to E_0.   □

Now we can prove the theorem that we will need in Section 8.

Theorem 5.5. *Let $p_1, \ldots, p_r$ be a finite set of primes. Let k be a subfield of a p-adic field, and let $\mathcal{L}$ be a finite extension of $k(T)$. Assume that k is algebraically closed in $\mathcal{L}$. There exists a set $U_0 \subseteq k$ such that U_0 is diophantine over $\mathcal{L}$ with coefficients in $\mathbb{Z}$ and such that $U_0 \cap \mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$.*

Proof. Let $\mathcal{E}_\eta$ be an elliptic curve over $\mathbb{Q}(T)$, and let $\tilde{\mathcal{E}} \to \mathbf{P}^1_{\mathbb{Q}}$ be an elliptic surface whose generic fiber is $\mathcal{E}_\eta$. Assume that the j-invariant $j_{\tilde{\mathcal{E}}}$ of $\tilde{\mathcal{E}}$ is nonconstant, and that rank($\mathcal{E}_\eta(\mathbb{Q}(T))) \geqslant 1$. For all but finitely many $t \in \mathbf{P}^1(\mathbb{Q})$, the specialization $\mathcal{E}_t$ is an elliptic curve over $\mathbb{Q}$. By Silverman's specialization theorem [18], rank($\mathcal{E}_\eta(\mathbb{Q}(T))) \leqslant$ rank($\mathcal{E}_t(\mathbb{Q})$) for all but finitely many $t \in \mathbb{Q}$, and so $\mathcal{E}_t$ has positive rank for all but finitely many $t \in \mathbb{Q}$. We will now use Proposition 5.1 and Theorem 5.4 to show that there exists a value $t \in \mathbb{Q}$ such that $\mathcal{E}_t$ has positive rank, and such that $\mathcal{E}_t(k) = \mathcal{E}_t(\mathcal{L})$: Let M be the set of all t for which $\mathcal{E}_t$ has positive rank and no geometric CM. Up to isomorphism over $\overline{\mathbb{Q}}$ there are only a finite number of elliptic curves $E/\mathbb{Q}$ with complex multiplication [19, p. 340], so since $j_{\tilde{\mathcal{E}}}$ is nonconstant, Silverman's theorem implies that M is infinite and that $\{j(\mathcal{E}_t) : t \in M\}$ is also infinite. If we want to ensure $\mathcal{E}_t(k) = \mathcal{E}_t(\mathcal{L})$, then by Proposition 5.1 and Theorem 5.4 this excludes only finitely many j-invariants $j(\mathcal{E}_t)$. Hence there is a $t \in M$ with the desired properties.

Take such a $t \in \mathbb{Q}$ and a corresponding elliptic curve $\mathcal{E}_t/\mathbb{Q}$. Let

$$U_0 := \big\{ (x/y) \cdot (y'/x') : (x, y) \in \mathcal{E}_t(\mathcal{L}), \ (x', y') \in \mathcal{E}_t(\mathcal{L}), \ y \cdot x' \neq 0 \big\}.$$

Since the elliptic curve $\mathcal{E}_t$ has coefficients in $\mathbb{Q}$, we can clear the denominators in its equation, and so U_0 is diophantine over $\mathcal{L}$ with coefficients in $\mathbb{Z}$. Also $U_0 \subseteq k$, and by Proposition 5.3, part (2), $U_0 \cap \mathbb{Q}$ is dense in $\mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_r}$. $\quad\square$

Remark 5.6. This theorem also holds for fields $\mathcal{L}$ which are finite extensions of $k(T_1, \ldots, T_n)$ with k algebraically closed in $\mathcal{L}$: Let $\mathcal{E}_\eta$ and $\tilde{\mathcal{E}}$ be as in the proof of Theorem 5.5. By the remark after Proposition 5.1 and Theorem 5.4, to find an element t with $\mathcal{E}_t(k) = \mathcal{E}_t(\mathcal{L})$ we only have to exclude finitely many j-invariants, and the proof proceeds exactly as before.

6. Quadratic forms over function fields

The following lemma deals with quadratic forms over $\mathcal{L}$ and generalizes Proposition 7 in [10]. This lemma will be needed to define multiplication on our set $\mathcal{S}$. Our notation for quadratic forms follows [11].

Lemma 6.1. *Let k be a field of characteristic zero, and suppose there is a quadratic form $\langle 1, -a \rangle \langle 1, b \rangle$ over k, which is anisotropic over k. Let $\mathcal{L}$ be a finite extension of $k(T)$, and let $\mathfrak{T}$ be a prime above T which is unramified. Assume that the residue field of $\mathcal{L}$ at $\mathfrak{T}$ is k. Let $g \in k(T)$ be such that $\text{ord}_T(g)$ is nonnegative and even. Then one of the following two quadratic forms*

$$\begin{aligned} q_1 &= \langle T, -aT, -1, -g \rangle \langle 1, b \rangle, \\ q_2 &= \langle T, -aT, -1, -ag \rangle \langle 1, b \rangle \end{aligned} \tag{1}$$

is anisotropic over $\mathcal{L}$.

Proof. Let $\operatorname{ord}_{\mathfrak{T}} : \mathcal{L}^* \twoheadrightarrow \mathbb{Z}$ be the discrete valuation associated to $\mathfrak{T}$. Since $\mathfrak{T}$ over T is unramified, the element T is a uniformizer for $\operatorname{ord}_{\mathfrak{T}}$. Since $g \in k(T)$ has even order in T, we may replace it by $T^{2n}g$ to ensure $g(0)$ is nonzero. Changing the coefficients of the quadratic forms by squares does not change the solvability. Assume both forms represented in (1) are isotropic over $\mathcal{L}$. We will derive a contradiction from this. Rewrite q_1 and q_2 as

$$Tx_1^2 - Tax_2^2 + Tbx_3^2 - Tabx_4^2 = x_5^2 + bx_6^2 + gx_7^2 + bgx_8^2, \tag{2}$$

$$Ty_1^2 - Tay_2^2 + Tby_3^2 - Taby_4^2 = y_5^2 + by_6^2 + agy_7^2 + bagy_8^2. \tag{3}$$

We can take a solution $(x_1, \ldots, x_8)$ of q_1 in $\mathcal{L}$ such that $\operatorname{ord}_{\mathfrak{T}}(x_i) \geqslant 0$ and such that $\operatorname{ord}_{\mathfrak{T}}(x_i) = 0$ for some i. Similarly we can take a solution $(y_1, \ldots, y_8)$ of q_2 in $\mathcal{L}$ such that $\operatorname{ord}_{\mathfrak{T}}(y_i) \geqslant 0$ and such that $\operatorname{ord}_{\mathfrak{T}}(x_i) = 0$ for some i. Reduce (2) and (3) modulo $\mathfrak{T}$ for these solutions. Let $g(0) = \ell$. After reducing modulo $\mathfrak{T}$ the right-hand side of (2) and (3) becomes $\langle 1, a^e\ell \rangle \langle 1, b \rangle$ ($e \in \{0, 1\}$), which is a quadratic form over k by our assumptions on the residue field at the prime $\mathfrak{T}$. Suppose that after reducing modulo $\mathfrak{T}$ the right-hand side of (2) and (3) is isotropic over k. The quaternion algebras associated to $\langle 1, a\ell \rangle \langle 1, b \rangle$ and $\langle 1, \ell \rangle \langle 1, b \rangle$ are $\left(\frac{-b, -a\ell}{k} \right)$ and $\left(\frac{-b, -\ell}{k} \right)$. (See Definitions A.1 and A.2 in Appendix A.) Since $\langle 1, a\ell \rangle \langle 1, b \rangle$ and $\langle 1, \ell \rangle \langle 1, b \rangle$ are isotropic over k, this implies that the quaternion algebras $\left(\frac{-b, -a\ell}{k} \right)$ and $\left(\frac{-b, -\ell}{k} \right)$ are split over k (see Proposition A.3). But this implies that their tensor product is isomorphic to a matrix algebra as well, and by Proposition A.4, this tensor product is

$$\left(\frac{-b, -a\ell}{k} \right) \otimes \left(\frac{-b, -\ell}{k} \right) \cong \left(\frac{-b, a\ell^2}{k} \right) \otimes M_2(k).$$

This implies that $\left(\frac{-b, a\ell^2}{k} \right)$ is split over k. By Proposition A.3 from Appendix A its associated norm form $\langle 1, b, -a\ell^2 - ab\ell^2 \rangle$ is isotropic over k, which means that $\langle 1, b, -a - ab \rangle$ is isotropic over k, contradicting our assumptions made in the statement of the lemma.

Therefore, the right-hand side modulo $\mathfrak{T}$ is anisotropic for some $e \in \{0, 1\}$. We may assume that the right-hand side of q_1 is anisotropic modulo $\mathfrak{T}$. This can only happen if $\operatorname{ord}_{\mathfrak{T}}(x_i) > 0$ for $i = 5, \ldots, 8$. Let $\tilde{x}_i = x_i / T$ for $i = 5, \ldots, 8$. Since $\operatorname{ord}_{\mathfrak{T}} T = 1$, $\operatorname{ord}_{\mathfrak{T}}(\tilde{x}_i) \geqslant 0$ for $i = 5, \ldots, 8$. We can rewrite (2) as

$$x_1^2 - ax_2^2 + bx_3^2 - abx_4^2 = T\left(\tilde{x}_5^2 + b\tilde{x}_6^2 + g\tilde{x}_7^2 + bg\tilde{x}_8^2 \right).$$

If we reduce modulo $\mathfrak{T}$ then we get

$$\bar{x}_1^2 - a\bar{x}_2^2 + b\bar{x}_3^2 - ab\bar{x}_4^2 = 0.$$

Since $\langle 1, -a \rangle \langle 1, b \rangle$ was assumed to be anisotropic over k the same argument as before implies that $\operatorname{ord}_{\mathfrak{T}}(x_i) > 0$ for $i = 1, \ldots, 4$. That means all the x_i ($i = 1, \ldots, 8$) in the solution of q_1 satisfy $\operatorname{ord}_{\mathfrak{T}}(x_i) > 0$, contradicting our choice of the x_i. $\quad\square$

7. Enlarging the constant field and coefficients of equations

We say that a subfield k of a p-adic field satisfies *Hypothesis* ($\mathcal{H}$) [10, p. 92], if the following conditions are satisfied:

There exists a four-dimensional anisotropic quadratic form q over k,

$$q = \langle 1, a \rangle \langle 1, \mathfrak{p} \rangle = x^2 + \mathfrak{p} y^2 + a z^2 + a \mathfrak{p} w^2.$$

We require that $\mathfrak{p} \in k$ is an element of odd valuation, which is algebraic over $\mathbb{Q}$. The element a is a 2^r th root of unity for some $r \geqslant 1$, and k contains a square root i of -1. We also require that q is locally isotropic at all 2-adic primes of $\mathbb{Q}(i, a, \mathfrak{p})$. Kim and Roush [10, p. 92] proved:

Proposition 7.1. *Let k be a subfield of a p-adic field of odd residue characteristic p. Then k has a finite extension $k' = k(i, a, \mathfrak{p})$ over which Hypothesis $(\mathcal{H})$ is true.*

We will now show that for the purpose of proving Theorem 1.1, we may enlarge the constant field k (and hence $\mathcal{L}$). In particular, we may assume that our field k satisfies Hypothesis $(\mathcal{H})$. Since we want to use the coefficients of the quadratic form q in our diophantine definitions, we want to have a and $\mathfrak{p}$ in our ring of coefficients.

Proposition 7.2. *Let K be a field and let $A_0 \subseteq K$ be a subring.*

(1) *Let $c_1, \ldots, c_m$ be elements of K which are algebraic over $\mathrm{Frac}(A_0)$. If Hilbert's Tenth Problem for K with coefficients in $A_0[c_1, \ldots, c_m]$ is undecidable, then Hilbert's Tenth Problem for K with coefficients in A_0 is undecidable.*
(2) *Let L/K be an extension which is generated by elements $b_1, \ldots, b_r$ which are algebraic over $\mathrm{Frac}(A_0)$. If Hilbert's Tenth Problem for L with coefficients in $A_0[b_1, \ldots, b_r]$ is undecidable, then Hilbert's Tenth Problem for K with coefficients in A_0 is undecidable.*

Proof. (1) Since c_i is algebraic over $\mathrm{Frac}(A_0)$ for $i = 1, \ldots, m$, we can consider its minimal polynomial over $\mathrm{Frac}(A_0)$. After multiplying by a common denominator we get an irreducible polynomial $p_i(x)$ over $\mathrm{Frac}(A_0)$ with coefficients in A_0. Given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in $A_0[c_1, \ldots, c_m]$, we can construct a system of polynomial equations with coefficients in A_0 by replacing, for $i = 1, \ldots, m$, each occurrence of c_i in f with a new variable y_i. Let $g(x_1, \ldots, x_n, y_1, \ldots, y_m)$ be this new equation obtained from f, and for $i = 1, \ldots, m$, add the equation $p_i(y_i) = 0$. Then the system of equations $g = 0$, $p_i(y_i) = 0$, $i = 1, \ldots, m$, has a solution in K if and only if $f(x_1, \ldots, x_n) = 0$ has a solution in K. By Lemma 2.1 the system of equations can be replaced with one single polynomial equation with coefficients in A_0.

(2) Since the b_i's are algebraic over $\mathrm{Frac}(A_0)$, the minimal polynomials of the b_i's over K have coefficients $d_1, \ldots, d_\ell$ which are algebraic over $\mathrm{Frac}(A_0)$. Now use the *Technical Lemma* in Pheidas [15, p. 379] together with the first part of this proposition. □

So in the following, whenever we pass to an extension $\mathcal{L}'/\mathcal{L}$, we will choose the ring of coefficients A_0 large enough to ensure that the elements generating $\mathcal{L}'/\mathcal{L}$ are algebraic over A_0. We can work with an enlarged constant field k that satisfies Hypothesis $(\mathcal{H})$, since the elements $i, a, \mathfrak{p}$ specified there are algebraic over $\mathbb{Q}$.

8. Proof of main theorem

We need one more result from [10] before we can prove Theorem 1.1:

Theorem 8.1. *Let k be a subfield of a p-adic field which satisfies Hypothesis $(\mathcal{H})$, and let $a, \mathfrak{p}$ be as in Hypothesis $(\mathcal{H})$. Let $g \in k(T)$ be such that $\mathrm{ord}_{T^{-1}}(g) = -2$. For $c_3, c_5 \in k$ let*

$$f(T) = f_{c_3,c_5}(T) = (1+T)^3 g(T) + c_3 T^3 + c_5 T^5.$$

Let U_0 be as in Theorem 5.5. If $\mathrm{ord}_T(g) = 1$, then there exist $c_3, c_5 \in U_0$ such that the two quadratic forms

$$\langle T, Ta, -1, -f \rangle \langle 1, \mathfrak{p} \rangle, \tag{4}$$

$$\langle T, Ta, -1, -af \rangle \langle 1, \mathfrak{p} \rangle \tag{5}$$

are isotropic over $k(T)$ (and hence over any finite extension of $k(T)$).

Proof. This theorem follows immediately from Theorems 9, 17, and 21 of [10]. □

8.1. Proof for transcendence degree one

We will now prove Theorem 1.1 when $\mathcal{L}$ is a finite extension of the rational function field $k(\tau)$. Let $\kappa \subseteq k$ be defined as in Section 3.1.

Theorem 8.2. *Let k be a subfield of a p-adic field of odd residue characteristic, and let $\mathcal{L}$ be a finite extension of $k(\tau)$. There exists a finite set $\{c_1, \ldots, c_\ell\}$ of elements of $\kappa(\tau)$, not all constant, such that Hilbert's Tenth Problem for $\mathcal{L}$ with coefficients in $\mathbb{Z}[c_1, \ldots, c_\ell]$ is undecidable.*

Proof. Let $E_0, \mathcal{E}_0, T$ be as in Section 4, i.e.

$$\mathcal{E}_0: \quad (T^3 + T + 1)Y^2 = X^3 + X + 1$$

has rank one over $\mathcal{L}$ with generator $P := (T, 1)$ (modulo 2-torsion) and there exists a prime $\mathfrak{Q}$ above T^{-1} which is unramified. By Theorem 4.1, T can be chosen to be algebraic over $\kappa(\tau)$. After making a constant field extension as in Proposition 3.3 we may assume that the residue field of $\mathcal{L}$ at the prime $\mathfrak{Q}$ is k, and that k is algebraically closed in $\mathcal{L}$. After extending the constant field k further, if necessary, we obtain an extension k' that satisfies Hypothesis $(\mathcal{H})$. After these constant field extensions $\mathfrak{Q}$ remains unramified, and by Moret-Bailly's theorem [13, Theorem 1.8] the group $\mathcal{E}_0(\mathcal{L})$ is still generated by $(T, 1)$. Let $\mathcal{L}' := \mathcal{L}k'$. We apply Proposition 7.2(2) to the finite extension $\mathcal{L}'/\mathcal{L}$, and we choose a ring of coefficients A_0 that satisfies the hypotheses of Proposition 7.2, i.e. A_0 contains the coefficients of the minimal polynomial of T over $\kappa(\tau)$ and the coefficients of the minimal polynomials of the elements generating $\mathcal{L}'/\mathcal{L}$. By Proposition 3.3, A_0 can be chosen to be of the form $A_0 = \mathbb{Z}[c_1, \ldots, c_\ell]$ with $c_1, \ldots, c_\ell \in \kappa(\tau)$, with κ as in Section 3.1. Let $a, \mathfrak{p}$ be the elements of k' as in Hypothesis $(\mathcal{H})$ and let $A := A_0[T, a, \mathfrak{p}]$. The elements $a, \mathfrak{p}$ are algebraic over $\mathbb{Q}$. By Proposition 7.2, proving that Hilbert's Tenth Problem for $\mathcal{L}'$ with coefficients in A is undecidable is enough to prove undecidability for $\mathcal{L}$ with coefficients in A_0. For simplicity of notation, we rename $\mathcal{L}'$ and k' as $\mathcal{L}$ and k again, respectively.

Let $P_m := m(T, 1) = (X_m, Y_m)$ and $\psi_m := X_m / T Y_m$. We will construct a diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ in $\mathcal{L}$ with coefficients in A.

The elliptic curve $\mathcal{E}_0$ is a projective variety, but any projective algebraic set can be partitioned into finitely many affine algebraic sets, which can then be embedded into a single affine algebraic

set. This implies that the set $\mathcal{E}_0(\mathcal{L})$ is diophantine over $\mathcal{L}$, since we can take care of the point at infinity $\mathbf{O}$ of $\mathcal{E}_0$. Hence the set

$$\mathcal{S}' := \{(X_{2n}, Y_{2n}): n \in \mathbb{Z}\}$$
$$= \{(x, y) \in \mathcal{L}^2 : \exists u, v \in \mathcal{L}: (u, v) \in \mathcal{E}_0(\mathcal{L}) \wedge (x, y) = 2(u, v)\}$$

is diophantine over $\mathcal{L}$ with coefficients in $\mathbb{Z}[T]$. Then the set

$$\mathcal{S} := \{(X_n, Y_n): n \in \mathbb{Z}\}$$
$$= \{(x, y) \in \mathcal{L}^2 : \exists n \in \mathbb{Z}: ((x, y) = (X_{2n}, Y_{2n}) \vee (x, y) = (X_{2n}, Y_{2n}) + (T, 1))\}$$

is diophantine over $\mathcal{L}$ with coefficients in $\mathbb{Z}[T]$ as well.

By associating the point $P_n = (X_n, Y_n)$ to an integer n we obtain a bijection between $\mathbb{Z}$ and $\mathcal{S}$, and addition of elements of $\mathcal{S}$ is existentially definable, because it is given by the group law on the elliptic curve. It remains to show that multiplication of elements of $\mathcal{S}$ is existentially definable. Let $t := T^{-1}$. We can consider $\mathcal{L}$ as an extension of $k(t)$. By the above discussion, the prime $\mathfrak{Q}$ above t is unramified, and the residue field of $\mathcal{L}$ at $\mathfrak{Q}$ is k.

Let $q := \langle 1, a \rangle \langle 1, \mathfrak{p} \rangle$ be the quadratic form over k as in Hypothesis $(\mathcal{H})$.

For $w \in \mathcal{L}$ let $\Phi(w)$ be the formula expressing that the quadratic forms

$$\langle t, -at, -1, -w \rangle \langle 1, \mathfrak{p} \rangle \quad \text{and} \quad \langle t, -at, -1, -aw \rangle \langle 1, \mathfrak{p} \rangle$$

are isotropic over $\mathcal{L}$. Clearly this is an existential formula. We will show that $n \cdot m = r$ if and only of $\Phi(w)$ holds for a certain function w that is formed from the x- and y-coordinates of the points $n \cdot (T, 1)$, $m \cdot (T, 1)$, and $r \cdot (T, 1)$.

As before, given $n, m, r \in \mathbb{Z} - \{0, 1, -1\}$ let $u := \psi_m \psi_n - \psi_r + (1/2) \cdot t$ and let $v := \psi_m \psi_n - \psi_r + (1/3) \cdot t$. Let ord_t, $\mathrm{ord}_{t^{-1}}$ be the normalized discrete valuations of $k(t)$ associated to t and t^{-1}. By Lemma 4.3, $\mathrm{ord}_{t^{-1}}(u) = -2$, $\mathrm{ord}_{t^{-1}}(v) = -2$ and if $n \cdot m = r$, then $\mathrm{ord}_t(u) = 1$ or $\mathrm{ord}_t(v) = 1$. If $n \cdot m \neq r$, then $\mathrm{ord}_t(u) = 0$ and $\mathrm{ord}_t(v) = 0$. (The cases where n, m or r are in $\{0, 1, -1\}$ can be handled separately.) Let U_0 be as in Theorem 5.5. For $c_3, c_5 \in U_0$ let

$$f_{(u, c_3, c_5)} := (1 + t)^3 u + c_3 t^3 + c_5 t^5,$$

and let

$$f_{(v, c_3, c_5)} := (1 + t)^3 v + c_3 t^3 + c_5 t^5.$$

We will show that

$$n \cdot m = r \quad \leftrightarrow \quad \exists c_3, c_5 \in U_0: \ \left(\Phi(f_{(u, c_3, c_5)}) \vee \Phi(f_{(v, c_3, c_5)})\right). \tag{6}$$

Since U_0 is diophantine over $\mathcal{L}$ with coefficients in $\mathbb{Z}$, it is easy to see that the condition that there exist $c_3, c_5 \in U_0$ for which the quadratic form

$$\langle t, -at, -1, -f_{(u, c_3, c_5)} \rangle \langle 1, \mathfrak{p} \rangle$$

has a solution in $\mathcal{L}$ can be described by an existential definition with coefficients in A. Hence the right-hand side of (6) is an existential definition with coefficients in A.

Suppose that $n \cdot m = r$. Then at least one of u, v has order 1 at t. Say $\mathrm{ord}_t(u) = 1$. Then $f_{(u,c_3,c_5)}$ is an element of $k(t)$, and so the quadratic forms

$$\langle t, -at, -1, -f_{(u,c_3,c_5)} \rangle \langle 1, \mathfrak{p} \rangle \quad \text{and} \quad \langle t, -at, -1, -af_{(u,c_3,c_5)} \rangle \langle 1, \mathfrak{p} \rangle \tag{7}$$

are quadratic forms over $k(t)$. By Theorem 8.1, applied with $g = u$, there exist $c_3, c_5 \in U_0$ such that $\Phi(f_{(u,c_3,c_5)})$ holds.

Conversely, assume that $n \cdot m \neq r$. Then by Lemma 4.3, u and v have order 0 at t, and so $f_{(u,c_3,c_5)}$ and $f_{(v,c_3,c_5)}$ have order 0 at t for any choice of $c_3, c_5 \in U_0$. Then by Lemma 6.1, applied with $g = f_{(u,c_3,c_5)}$, for any choice of $c_3, c_5 \in U_0$, one of the two quadratic forms in (7) is anisotropic over $\mathcal{L}$, so $\Phi(f_{(u,c_3,c_5)})$ does not hold. Similarly, $\Phi(f_{(v,c_3,c_5)})$ does not hold for any choice of $c_3, c_5 \in U_0$. $\square$

8.2. Generalization to higher transcendence degree

Let k be a subfield of a p-adic field of odd residue characteristic, and let $\mathcal{L}$ be a finite extension of the rational function field $k(\tau, \tau_2, \ldots, \tau_n)$. Let k_1 be the algebraic closure of $k(\tau_2, \ldots, \tau_n)$ in $\mathcal{L}$. Then $\mathcal{L}$ is a finite extension of $k_1(\tau)$. Let κ be as in Section 3.2. We can apply Theorem 4.1 to the elliptic curve E_0 defined in Section 4 and with $\mathcal{L}/k_1(\tau)$ to obtain an element T_1 which is algebraic over $\kappa(\tau)$. Consider the elliptic curve $\mathcal{E}_0$ defined by the affine equation $(T_1^3 + T_1 + 1)Y^2 = X^3 + X + 1$. By Theorem 4.1, $\mathcal{E}_0(\mathcal{L})$ is generated by $(T_1, 1)$ (modulo 2-torsion).

To prove Theorem 1.1 when the transcendence degree of $\mathcal{L}/k$ is $\geqslant 2$, we have to prove the following lemma.

Lemma 8.3. *Let k be a subfield of a p-adic field, and let K be a finite extension of the rational function field $k(\tau_2, \ldots, \tau_n)$. There exists a finite extension k'/k such that k' satisfies Hypothesis $(\mathcal{H})$, and such that the form $q = \langle 1, a \rangle \langle 1, \mathfrak{p} \rangle$ as in Hypothesis $(\mathcal{H})$ remains anisotropic over $K' = Kk'$.*

Proof. Let $\mathfrak{T}_2$ be a prime of K lying above the prime τ_2 of the rational function field $k(\tau_3, \ldots, \tau_n)(\tau_2)$, and let $k_{\mathfrak{T}_2}$ be the residue field of $\mathfrak{T}_2$. Then $k_{\mathfrak{T}_2}$ is a finite extension of $k(\tau_3, \ldots, \tau_n)$. Now let $\mathfrak{T}_3$ be a prime of $k_{\mathfrak{T}_2}$ lying above the prime τ_3 of $k(\tau_4, \ldots, \tau_n)(\tau_3)$. Let $k_{\mathfrak{T}_3}$ be the residue field of $\mathfrak{T}_3$. The field $k_{\mathfrak{T}_3}$ is a finite extension of $k(\tau_4, \ldots, \tau_n)$. After repeating this process we obtain a finite extension $k_{\mathfrak{T}_n}$ of k. From the proof of [10, Proposition 8] it follows that we can find a finite extension k' of k which is generated by elements algebraic over $\mathbb{Q}$ such that both k' and $k_{\mathfrak{T}_n}k'$ satisfy Hypothesis $(\mathcal{H})$.

Claim. The field k' has the desired property.

Proof of Claim. Let $\mathfrak{T}_2'$ be a prime of K' extending $\mathfrak{T}_2$. Let $k_{\mathfrak{T}_2'}$ be the residue field of $\mathfrak{T}_2'$. Then $k_{\mathfrak{T}_2'} = k'k_{\mathfrak{T}_2}$ by Theorem 3.1. Let $\mathfrak{T}_3'$ be a prime of $k_{\mathfrak{T}_2'}$ extending $\mathfrak{T}_3$, and let $k_{\mathfrak{T}_3'}$ be the residue field. Define $\mathfrak{T}_4', k_{\mathfrak{T}_4'}, \ldots, \mathfrak{T}_n', k_{\mathfrak{T}_n'}$ similarly. We have $k_{\mathfrak{T}_n'} = k'k_{\mathfrak{T}_n}$. Assume by contradiction that q is isotropic over K'. Take a solution $f_1, \ldots, f_4$ in K'. By scaling the f_i's with the same factor

we can arrange it so that $\mathrm{ord}_{\mathfrak{T}_2'}\, f_i \geqslant 0$ for $i = 1, \ldots, 4$, and by changing the f_i's further we may assume that $\mathrm{ord}_{\mathfrak{T}_2'}\, f_i = 0$ for some i. Now look at $\overline{f_i} = f_i \bmod \mathfrak{T}_2'$, $i = 1, \ldots, 4$. This gives us that q is isotropic over $k_{\mathfrak{T}_2'}$. By repeating this we obtain that q is isotropic over $k_{\mathfrak{T}_n'}$, contradiction. □

Now we can generalize the proof of Theorem 8.2 and prove Theorem 1.1:

Proof of Theorem 1.1. Let $k, k_1, \mathcal{L}, E_0, \mathcal{E}_0$ be as above. The proof proceeds as in Theorem 8.2. Let $\mathfrak{Q}$ be a prime of $\mathcal{L}$ above the prime T_1^{-1} of $k(\tau_2, \ldots, \tau_n)(T_1)$ which is unramified. Let $m(T_1, 1) = (X_m, Y_m)$ and $\psi_m := X_m / T_1 Y_m$. As in Remark 3.5, we enlarge k_1 to a finite extension k_1' such that the prime $\mathfrak{Q}'$ of the compositum $\mathcal{L}k_1'$ (extending $\mathfrak{Q}$) has residue field k_1'. Let $\mathcal{L}' := \mathcal{L}k_1'$. We now pass to an extension k' of the constant field k (and hence enlarge k_1' and $\mathcal{L}'$ further) such that k' is as in Lemma 8.3 for the extension $k_1'/k(\tau_2, \ldots, \tau_n)$. By the proof of Lemma 8.3, k'/k can be generated by elements which are algebraic over $\mathbb{Q}$. By [16, Proposition 8.3], k_1' is algebraically closed in $\mathcal{L}'$.

Now we choose our ring of coefficients A_0 such that $\mathcal{L}'/\mathcal{L}$ is generated by elements algebraic over A_0, and such that A_0 contains the coefficients of the minimal polynomial of T_1. By the above arguments, together with Remark 3.5 and Theorem 4.1, A_0 is of the form $A_0 = \mathbb{Z}[c_1, \ldots, c_\ell]$, with $\{c_1, \ldots, c_\ell\} \in \kappa(\tau)$. We let $A := A_0[T_1, a, \mathfrak{p}]$, with $a, \mathfrak{p}$ the elements as in Hypothesis $(\mathcal{H})$. For simplicity of notation we rename $\mathcal{L}', k_1', k'$, and $\mathfrak{Q}'$ as $\mathcal{L}, k_1, k$, and $\mathfrak{Q}$.

By the remark after Theorem 5.5 we can still construct $U_0 \subseteq k$ which is diophantine over $\mathcal{L}$ with coefficients in $\mathbb{Z}$ and whose intersection with $\mathbb{Q}$ is dense in any finite product of p-adic fields.

To prove the theorem we will construct a diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ in $\mathcal{L}$ with coefficients in A. As before let $\mathcal{S} := \{(X_n, Y_n): n \in \mathbb{Z}\}$. This set is diophantine over $\mathcal{L}$ with coefficients in $\mathbb{Z}[T_1]$, and it remains to show that multiplication of elements of $\mathcal{S}$ is existentially definable. Let $t_1 := T_1^{-1}$. Then $\mathcal{L}$ is a finite extension of $k_1(t_1)$ and the prime $\mathfrak{Q}$ of $\mathcal{L}$ above t_1 is unramified.

Let $q := \langle 1, a \rangle \langle 1, \mathfrak{p} \rangle$ be the quadratic form over k as in Hypothesis $(\mathcal{H})$.

For $w \in \mathcal{L}$ let $\Phi(w)$ be the formula expressing that the quadratic forms

$$\langle t_1, -at_1, -1, -w \rangle \langle 1, \mathfrak{p} \rangle \quad \text{and} \quad \langle t_1, -at_1, -1, -aw \rangle \langle 1, \mathfrak{p} \rangle \tag{8}$$

are isotropic over $\mathcal{L}$. Given $n, m, r \in \mathbb{Z} - \{0, 1, -1\}$ let $u := \psi_m \psi_n - \psi_r + (1/2) \cdot t_1$ and $v := \psi_m \psi_n - \psi_r + (1/3) \cdot t_1$. For $c_3, c_5 \in k$ let

$$f_{(u,c_3,c_5)} := (1 + t_1)^3 u + c_3 t_1^3 + c_5 t_1^5$$

and

$$f_{(v,c_3,c_5)} := (1 + t_1)^3 v + c_3 t_1^3 + c_5 t_1^5.$$

The elements $f_{(u,c_3,c_5)}$ and $f_{(v,c_3,c_5)}$ are elements of $k(t_1)$.

We will show that

$$n \cdot m = r \quad \leftrightarrow \quad \exists c_3, c_5 \in U_0: \ \big(\Phi(f_{(u,c_3,c_5)}) \vee \Phi(f_{(v,c_3,c_5)}) \big). \tag{9}$$

The same argument as in Theorem 8.2 shows that the right-hand side of (9) is existential with coefficients in A. Suppose that $n \cdot m = r$. Then at least one of u, v has order 1 at t_1. Say $\mathrm{ord}_{t_1}(u) = 1$.

Then $f_{(u,c_3,c_5)}$ is an element of $k(t_1)$, and the same argument as in Theorem 8.2 shows that there exist $c_3, c_5 \in U_0$ such that $\Phi(f_{(u,c_3,c_5)})$ holds.

Conversely, assume that $n \cdot m \neq r$. Then by Lemma 4.3, u and v have order 0 at t_1, and so $f_{(u,c_3,c_5)}$, $f_{(v,c_3,c_5)}$ have order 0 at t_1 for any choice of $c_3, c_5 \in U_0$. Then by Lemma 8.3, we can apply Lemma 6.1 to the extension $\mathcal{L}/k_1(t_1)$, and with $g = f_{(u,c_3,c_5)}$. Hence for any choice of $c_3, c_5 \in U_0$, $\Phi(f_{(u,c_3,c_5)})$ does not hold. Similarly, for any choice of $c_3, c_5 \in U_0$, $\Phi(f_{(v,c_3,c_5)})$ does not hold, either. $\quad\square$

Acknowledgments

Appendix A

In this appendix we will state the definitions and theorems about quaternion algebras and quadratic forms that we used in our proof. We need the following two definitions.

Definition A.1. Let F be a field of characteristic $\neq 2$, and let $a, b \in F^*$. We define the *quaternion algebra* $\left(\frac{a,b}{F}\right)$ to be the F-algebra on two generators i, j with defining relations: $i^2 = a$ and $j^2 = b$, and $ij = -ji$. The *associated norm form* of the quaternion algebra $\left(\frac{a,b}{F}\right)$ is the quadratic form $\langle 1, -a, -b, ab \rangle$.

Definition A.2. We say that a quaternion algebra $A = \left(\frac{a,b}{F}\right)$ *splits over F* if $A \cong M_2(F)$.

We can see whether a quaternion algebra is split by looking at its norm form:

Proposition A.3. *The quaternion algebra $\left(\frac{a,b}{F}\right)$ splits over F iff its associated norm form is isotropic.*

Proof. This is proved in [11, Theorem 2.7, p. 58.] $\quad\square$

Proposition A.4. *For $a, b, c \in F^*$, we have*

$$\left(\frac{a,b}{F}\right) \otimes \left(\frac{a,c}{F}\right) \cong \left(\frac{a,bc}{F}\right) \otimes M_2(F).$$

Proof. This is Corollary 2.11 in [11, p. 61]. $\quad\square$

References

[1] J.W.S. Cassels, A. Fröhlich (Eds.), Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society, NATO Adv. Study Inst., Academic Press, London, 1967, with the support of the International Mathematical Union.

[2] Brian Conrad, Gross–Zagier revisited, in: Heegner Points and Rankin L-Series, in: Math. Sci. Res. Inst. Publ., vol. 49, Cambridge Univ. Press, Cambridge, 2004, pp. 67–163, with an appendix by W.R. Mann.

[3] J.E. Cremona, Algorithms for Modular Elliptic Curves, second ed., Cambridge Univ. Press, Cambridge, 1997.

[4] Martin Davis, Hilary Putnam, Julia Robinson, The decision problem for exponential diophantine equations, Ann. of Math. (2) 74 (1961) 425–436.

[5] Jan Denef, The Diophantine problem for polynomial rings and fields of rational functions, Trans. Amer. Math. Soc. 242 (1978) 391–399.

[6] Max Deuring, Lectures on the Theory of Algebraic Functions of One Variable, Lecture Notes in Math., vol. 314, Springer-Verlag, Berlin, 1973.

[7] Kirsten Eisenträger, Hilbert's Tenth Problem for algebraic function fields of characteristic 2, Pacific J. Math. 210 (2) (2003) 261–281.

[8] Kirsten Eisenträger, Hilbert's Tenth Problem for function fields of varieties over $\mathbb{C}$, Int. Math. Res. Not. 59 (2004) 3191–3205.

[9] K.H. Kim, F.W. Roush, Diophantine undecidability of $\mathbf{C}(t_1, t_2)$, J. Algebra 150 (1) (1992) 35–44.

[10] K.H. Kim, F.W. Roush, Diophantine unsolvability over p-adic function fields, J. Algebra 176 (1) (1995) 83–110.

[11] T.Y. Lam, The Algebraic Theory of Quadratic Forms, Benjamin/Cummings Publishing Co. Inc., Advanced Book Program, Reading, MA, 1980, revised second printing, Mathematics Lecture Note Series.

[12] Yu.V. Matijasevič, The Diophantineness of enumerable sets, Dokl. Akad. Nauk SSSR 191 (1970) 279–282.

[13] Laurent Moret-Bailly, Elliptic curves and Hilbert's Tenth Problem for algebraic function fields over real and p-adic fields, J. Reine Angew. Math. 587 (2005) 77–143.

[14] Thanases Pheidas, Hilbert's tenth problem for fields of rational functions over finite fields, Invent. Math. 103 (1) (1991) 1–8.

[15] Thanases Pheidas, Extensions of Hilbert's tenth problem, J. Symbolic Logic 59 (2) (1994) 372–397.

[16] Michael Rosen, Number Theory in Function Fields, Grad. Texts in Math., vol. 210, Springer-Verlag, New York, 2002.

[17] Alexandra Shlapentokh, Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic, Pacific J. Math. 193 (2) (2000) 463–500.

[18] Joseph Silverman, Heights and the specialization map for families of abelian varieties, J. Reine Angew. Math. 342 (1983) 197–211.

[19] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 106, Springer-Verlag, New York, 1994, corrected reprint of the 1986 original.

[20] Carlos R. Videla, Hilbert's tenth problem for rational function fields in characteristic 2, Proc. Amer. Math. Soc. 120 (1) (1994) 249–253.