Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers

Bjorn Poonen*

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA,
poonen@math.berkeley.edu

Abstract. Let $F \subseteq K$ be number fields, and let $\mathcal{O}_F$ and $\mathcal{O}_K$ be their rings of integers. If there exists an elliptic curve E over F such that $\operatorname{rk} E(F) = \operatorname{rk} E(K) = 1$, then there exists a diophantine definition of $\mathcal{O}_F$ over $\mathcal{O}_K$.

1 Introduction

D. Hilbert asked, as Problem 10 of his famous list of 23 problems posed to the mathematical community in 1900, for an algorithm to decide, given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in the ring $\mathbf{Z}$ of integers, whether there exists a solution with $x_1, \ldots, x_n \in \mathbf{Z}$. In Hilbert's time, there was no formal definition of algorithm, but presumably what he had in mind was a mechanical procedure that a human could in principle carry out, given sufficient paper, pencils, erasers, and time, following a set of strict rules requiring no insight or ingenuity on the part of the human. In the 1930s, several rigorous models of computation were proposed as a substitute for the informal notion of "mechanical procedure" as above (the λ-definable functions of A. Church and S. Kleene, the recursive functions of K. Gödel and J. Herbrand, and the logical computing machines of A. Turing). These models, as well as others developed later, were shown to be equivalent; this gave credence to the *Church-Turing thesis*, which is the belief that every mechanical procedure can be carried out by a Turing machine. Therefore, the modern interpretation of Hilbert's Tenth Problem is that it asks whether a Turing machine can decide the existence of solutions.

J. Matijasevič [Mat70], building on earlier work by M. Davis, H. Putnam, and J. Robinson [DPR61] showed that there is no such Turing machine. To describe their work in more detail, we need a few definitions. A subset S of $\mathbf{Z}^n$ is called *listable* or *recursively enumerable* if there is an algorithm (Turing machine) such that S is exactly the set of $a \in \mathbf{Z}^n$ that are eventually printed by the algorithm.

* This research was supported by NSF grant DMS-9801104, and a Packard Fellowship. This article has been published as pp. 33–42 in: *Algorithmic Number Theory*, C. Fieker and D. Kohel (eds.), 5th International Symposium, ANTS-V, Sydney, Australia, July 2002, Proceedings, *Lecture Notes in Computer Science* **2369**, Springer-Verlag, Berlin, 2002.

A subset S of $\mathbf{Z}^n$ is said to be *diophantine*, or to admit a *diophantine definition*, if there is a polynomial $p(a_1, \ldots, a_n, x_1, \ldots, x_m) \in \mathbf{Z}[a_1, \ldots, a_n, x_1, \ldots, x_m]$ such that

$$S = \{\, a \in \mathbf{Z}^n : (\exists x_1, \ldots, x_m \in \mathbf{Z})\ p(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0 \,\}.$$

For example, the subset $\mathbf{Z}_{\geq 0} := \{0, 1, 2, \ldots\}$ of $\mathbf{Z}$ is diophantine, since for $a \in \mathbf{Z}$, we have

$$a \in \mathbf{Z}_{\geq 0} \iff (\exists x_1, x_2, x_3, x_4 \in \mathbf{Z})\ x_1^2 + x_2^2 + x_3^2 + x_4^2 = a.$$

One can show using "diagonal arguments" that there exists a listable subset L of $\mathbf{Z}$ whose complement is not listable. It follows that for this L, there is no algorithm that takes as input an integer a and decides in a finite amount of time whether a belongs to L; in other words, membership in L is undecidable.

Diophantine subsets of $\mathbf{Z}^n$ are listable: given p, one can write a computer program with an outer loop with B running through $1, 2, \ldots$, and an inner loop in which one tests the finitely many $(a_1, \ldots, a_n, x_1, \ldots, x_m) \in \mathbf{Z}^{n+m}$ satisfying $|a_i|, |x_j| \leq B$ for all i and j, and prints $(a_1, \ldots, a_n)$ if $p(a_1, \ldots, a_n, x_1, \ldots, x_m) = 0$. Davis [Dav53] conjectured conversely that all listable subsets of $\mathbf{Z}^n$ were diophantine, and this is what Matijasevič eventually proved. In particular, the set L is diophantine. Hence a positive answer to Hilbert's Tenth Problem would imply that membership in L is decidable. But membership in L is undecidable, so Hilbert's Tenth Problem is undecidable too; that is, there is no algorithm that takes as input a polynomial $p \in \mathbf{Z}[x_1, \ldots, x_n]$, and decides whether $p(x_1, \ldots, x_n) = 0$ has a solution in integers.

More generally, if R is any commutative ring with 1, one can define what it means for a subset of R^n to be *diophantine over* R, by replacing $\mathbf{Z}$ by R everywhere. Similarly one can speak of *Hilbert's Tenth Problem over* R provided that one has fixed some encoding of elements of R as finite strings of symbols from a finite alphabet, so that polynomials over R can be the input to a Turing machine. For some rings R (for example, uncountable rings) such an encoding may not be possible. In this case one should modify the problem, by specifying a countable subset $\mathcal{P}$ of the set of all polynomials over R and an encoding of elements of $\mathcal{P}$ as finite strings of symbols, and then asking whether there exists a Turing machine that takes as input a polynomial $p \in \mathcal{P}$ and decides whether $p(x_1, \ldots, x_n) = 0$ has a solution over R. For example, K. Kim and F. Roush [KR92] proved that Hilbert's Tenth Problem over the purely transcendental function field $\mathbf{C}(t_1, t_2)$ is undecidable when one takes $\mathcal{P}$ to be the set of polynomials with coefficients in $\mathbf{Z}[t_1, t_2]$. Usually it is not necessary to specify exactly how the elements of $\mathcal{P}$ are encoded, since usually given any two reasonable encodings, a Turing machine can convert between the two.

Perhaps the most important unsolved question in this area is Hilbert's Tenth Problem over the field $\mathbf{Q}$ of rational numbers. The majority view seems to be that it should be undecidable. To prove this, it would suffice to show that the subset $\mathbf{Z}$ of $\mathbf{Q}$ is diophantine over $\mathbf{Q}$. On the other hand, B. Mazur has suggested that perhaps for any variety X over $\mathbf{Q}$, the topological closure of $X(\mathbf{Q})$ in $X(\mathbf{R})$ has

at most finitely many connected components; if this is true, no such diophantine definition of $\mathbf{Z}$ over $\mathbf{Q}$ exists. See [Maz94] and the more recent articles [CZ00] and [Phe00] for further discussion.

The function field analogue, namely Hilbert's Tenth Problem over the function field k of a curve over a finite field, is known to be undecidable. The first result of this type is due to T. Pheidas [Phe91], who proved this for $k = \mathbf{F}_q(t)$ with q odd. His argument was adapted and generalized by C. Videla [Vid94] for $k = \mathbf{F}_q(t)$ with q even, by A. Shlapentokh [Shl92] for other function fields of odd characteristic, and finally by K. Eisenträger [Eis] for the remaining function fields of characteristic 2. Analogues are known also for many function fields over infinite fields of positive characteristic: see [Shl00a] and [Eis].

For more results concerning Hilbert's Tenth Problem, see the book [DLPVG00], and especially the survey articles [PZ00] and [Shl00b] therein. Since the publication of that book, undecidability of Hilbert's Tenth Problem has been proved also for function fields of curves X over formally real fields k_0 with $X(k_0)$ nonempty [MB] (in fact this is just one application of his results), and for function fields of surfaces over real closed or algebraically closed fields of characteristic zero [Eis].

2 Hilbert's Tenth Problem over rings of integers

In this article, our goal is to prove a result towards Hilbert's Tenth Problem over rings of integers. If F is a number field, let $\mathcal{O}_F$ denote the integral closure of $\mathbf{Z}$ in F. There is a known diophantine definition of $\mathbf{Z}$ over $\mathcal{O}_F$ for the following number fields:

1. F is totally real [Den80].
2. F is a quadratic extension of a totally real number field [DL78].
3. F has exactly one conjugate pair of nonreal embeddings [Phe88], [Shl89].

In particular, Hilbert's Tenth Problem over $\mathcal{O}_F$ is undecidable for such fields F.

It is conjectured [DL78] that for *every* number field F, there is a diophantine definition of $\mathbf{Z}$ over $\mathcal{O}_F$. Our main theorem gives evidence for this conjecture, by reducing it to a plausible conjecture about the existence of certain elliptic curves.

Before stating our theorem, let us recall the Mordell-Weil Theorem, which states that if E is an elliptic curve over a number field F, then the abelian group $E(F)$ is finitely generated. Let $\operatorname{rk} E(F)$ denote the rank of $E(F)$.

Theorem 1. *Let $F \subseteq K$ be number fields, and let $\mathcal{O}_F$ and $\mathcal{O}_K$ be their rings of integers. Suppose that there exists an elliptic curve E over F such that* $\operatorname{rk} E(F) = \operatorname{rk} E(K) = 1$. *Then there exists a diophantine definition of $\mathcal{O}_F$ over $\mathcal{O}_K$.*

Most of the rest of this paper is devoted to the proof of Theorem 1. But for now, we mention its application to Hilbert's Tenth Problem.

Corollary 2. *Under the hypotheses of Theorem 1, if in addition F is of one of the types of number fields listed above for which a diophantine definition of $\mathbf{Z}$ over $\mathcal{O}_F$ is known, then Hilbert's Tenth Problem over $\mathcal{O}_K$ is undecidable.*

Proof. Theorem 1 reduces the undecidability over $\mathcal{O}_K$ to the undecidability over $\mathcal{O}_F$. □

J. Denef, at the end of [Den80], sketches a simple proof of Theorem 1 in the case where K is totally real and $F = \mathbf{Q}$. In fact, he is also able to treat some totally real algebraic extensions K of *infinite* degree over $\mathbf{Q}$. But his proof technique does not seem to generalize easily to fields that are not totally real.

Our proof of Theorem 1 is similar to that of an older result, the theorem of [DL78], which uses a 1-dimensional torus (a Pell equation) in place of the elliptic curve. We have been inspired also by the exposition of the "weak version of the vertical method" in [Shl00b] and by the ideas in [Phe00].

2.1 Preliminaries on diophantine sets over $\mathcal{O}_K$

The subset $\mathcal{O}_K - \{0\}$ of $\mathcal{O}_K$ is diophantine over $\mathcal{O}_K$: see Proposition 1(c) of [DL78]. We have a surjective map $\mathcal{O}_K \times (\mathcal{O}_K - \{0\}) \to K$ taking (a, b) to a/b. If $S \subseteq K^n$ is diophantine over K, then the inverse image of S under $(\mathcal{O}_K \times (\mathcal{O}_K - \{0\}))^n \to K^n$ is diophantine over $\mathcal{O}_K$. In this case, we will also say that S is diophantine over $\mathcal{O}_K$. It follows that in constructing diophantine definitions over $\mathcal{O}_K$, there is no harm in using equations with some variables taking values in $\mathcal{O}_K$ and other variables taking values in K.

Given $t \in K^\times$, define the *denominator ideal* $\mathrm{den}(t) = \{\, b \in \mathcal{O}_K : bt \in \mathcal{O}_K \,\}$ and the *numerator ideal* $\mathrm{num}(t) = \mathrm{den}(t^{-1})$. Also define $\mathrm{num}(0)$ to be the zero ideal. These ideals behave in the obvious way upon extension of the field.

Lemma 3.

1. *For fixed $m, n \in \mathbf{Z}_{\geq 0}$, the set of $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ in K^{m+n} such that the fractional ideal $(x_1, \ldots, x_m)$ divides the fractional ideal $(y_1, \ldots, y_n)$ is diophantine over $\mathcal{O}_K$.*
2. *The set of $(t, u) \in K^\times \times K^\times$ such that $\mathrm{den}(t) \mid \mathrm{den}(u)$ is diophantine over $\mathcal{O}_K$.*
3. *The set of $(t, u) \in K^\times \times K$ such that $\mathrm{den}(t) \mid \mathrm{num}(u)$ is diophantine over $\mathcal{O}_K$.*
4. *The set of $(t, u) \in \mathcal{O}_K \times K^\times$ such that $t \mid \mathrm{den}(u)$ is diophantine over $\mathcal{O}_K$.*

Proof. Statement 1 is clear, since the condition is that there exist $c_{ij} \in \mathcal{O}_K$ such that $y_j = \sum_i c_{ij} x_i$ for each j. Statement 2 follows from statement 1, since $\mathrm{den}(t) \mid \mathrm{den}(u)$ if and only if the fractional ideal $(u, 1)$ divides $(t, 1)$. Statements 3 and 4 follow from statement 2: namely,

$$\begin{aligned} \mathrm{den}(t) \mid \mathrm{num}(u) &\iff u = 0 \text{ or } (\exists v)(uv = 1 \text{ and } \mathrm{den}(t) \mid \mathrm{den}(v)), \\ t \mid \mathrm{den}(u) &\iff (\exists v)(tv = 1 \text{ and } \mathrm{den}(v) \mid \mathrm{den}(u)). \end{aligned}$$

□

2.2 Bounds from divisibility in $\mathcal{O}_K$

Let $n = [K : \mathbf{Q}]$ and $s = [K : F]$. Fix $\alpha \in \mathcal{O}_K$ such that $\{1, \alpha, \ldots, \alpha^{s-1}\}$ is a basis for K over F. Let $D \in \mathcal{O}_F$ denote the discriminant of this basis. If I is an ideal in $\mathcal{O}_K$, let $N_{K/\mathbf{Q}}(I) \in \mathbf{Z}_{\geq 0}$ denote its norm.

Lemma 4. *There is a positive integer $c > 0$ depending only on F, K, and α such that the following holds. Let $I \subset \mathcal{O}_K$ be a nonzero nonunit ideal, and let $\mu \in \mathcal{O}_K$. Write $\mu = \sum_{i=0}^{s-1} a_i \alpha^i$ with $a_i \in F$. Suppose that $\mu(\mu+1)\cdots(\mu+n) \mid I$. Then $N_{K/\mathbf{Q}}(Da_i) \leq N_{K/\mathbf{Q}}(I)^c$.*

Proof. This is essentially Section 1.2 of [Shl00b]. The only differences are that we have specialized by taking $l_i = -i$, and we have generalized by replacing the element y by an ideal I: this does not affect the proof. □

The following is similar to Lemma 2.5 in [Shl00b].

Lemma 5. *There exists a constant $c' > 0$ depending only on F and K such that the following holds: Let I be a nonzero ideal of $\mathcal{O}_F$. Suppose $\mu \in \mathcal{O}_K$ and $w \in \mathcal{O}_F$. Write $\mu = \sum_{i=0}^{s-1} a_i \alpha^i$ with $a_i \in F$. Suppose $N_{K/\mathbf{Q}}(Da_i) < c' N_{K/\mathbf{Q}}(I)$ for all i, and $\mu \equiv w \pmod{I\mathcal{O}_K}$. Then $\mu \in \mathcal{O}_F$.*

Proof. Choose ideals $J_1, \ldots, J_h \subseteq \mathcal{O}_F$ representing the elements of the class group of F, and choose $c' > 0$ such that $c' N_{K/\mathbf{Q}}(J_j) < 1$ for all j. Choose j such that $J_j I^{-1}$ is principal, generated by $z \in F^\times$, say. Since $\mu \equiv w \pmod{I\mathcal{O}_K}$, we have

$$z(\mu - w) = z(a_0 - w) + (za_1)\alpha + \cdots + (za_{s-1})\alpha^{s-1} \in \mathcal{O}_K.$$

By Lemma 4.1 of [Shl00b] (an elementary lemma about discriminants), $Dza_i \in \mathcal{O}_F$ for $i = 1, 2, \ldots, s-1$. On the other hand,

$$|N_{K/\mathbf{Q}}(Dza_i)| = |N_{K/\mathbf{Q}}(Da_i) N_{K/Q}(z)| < c' N_{K/\mathbf{Q}}(I) \frac{N_{K/Q}(J_j)}{N_{K/Q}(I)} < 1,$$

by definition of c', so $Dza_i = 0$. Thus $a_i = 0$ for $i = 1, 2, \ldots, s-1$. Hence $\mu \in \mathcal{O}_F$. □

2.3 Denominators of x-coordinates of points on an elliptic curve

We assume that an elliptic curve E as in Theorem 1 exists. Thus E is defined over F, and $\operatorname{rk} E(F) = \operatorname{rk} E(K) = 1$. Hence E has a Weierstrass model of the form $y^2 = x^3 + ax + b$ and we may assume $a, b \in \mathcal{O}_F$. Let O denote the point at infinity on E, which is the identity of $E(F)$.

For each nonarchimedean place $\mathfrak{p}$ of K, let $K_\mathfrak{p}$ denote the completion of K at $\mathfrak{p}$. and let $\mathbf{F}_\mathfrak{p}$ denote the residue field. Reducing coefficients modulo $\mathfrak{p}$ yields a possibly singular curve

$$E_\mathfrak{p} := \operatorname{Proj} \frac{\mathbf{F}_\mathfrak{p}[X, Y, Z]}{(Y^2 Z - X^3 - \bar{a} X Z^2 - \bar{b} Z^3)}$$

over $\mathbf{F}_\mathfrak{p}$. Let $E_\mathfrak{p}^{\text{smooth}}$ denote the smooth part of $E_\mathfrak{p}$. Let $E_0(K_\mathfrak{p})$ be the set of points in $E(K_\mathfrak{p})$ whose reduction mod $\mathfrak{p}$ lies in $E_\mathfrak{p}^{\text{smooth}}(\mathbf{F}_\mathfrak{p})$.

Lemma 6.

1. *$E_0(K_\mathfrak{p})$ is a subgroup of $E(K_\mathfrak{p})$.*
2. *$E_\mathfrak{p}^{\mathrm{smooth}}(\mathbf{F}_\mathfrak{p})$ is an abelian group under the usual chord-tangent law.*
3. *Reduction modulo $\mathfrak{p}$ gives a surjective group homomorphism $\mathrm{red}_\mathfrak{p} : E_0(K_\mathfrak{p}) \to E_\mathfrak{p}^{\mathrm{smooth}}(\mathbf{F}_\mathfrak{p})$.*
4. *Both $E_0(K_\mathfrak{p})$ and $E_1(K_\mathfrak{p}) := \ker(\mathrm{red}_\mathfrak{p})$ are of finite index in $E(K_\mathfrak{p})$.*

Proof. For the first three statements, see Proposition VII.2.1 in [Sil92]. We have not assumed that our Weierstrass model is minimal at $\mathfrak{p}$, so our definition of E_0 is different from the standard one in [Sil92], but this does not matter in the proofs. To prove statement 4, observe that $E_0(K_\mathfrak{p})$ and $E_1(K_\mathfrak{p})$ are open subgroups of the compact group $E(K_\mathfrak{p})$ in the $\mathfrak{p}$-adic topology. □

From now on, $r \in \mathbf{Z}_{\geq 1}$ is assumed to be a multiple of $\#E(K)_{\mathrm{tors}}$, of the index $(E(K) : E(F))$, and of the index $(E(K_\mathfrak{p}) : E_0(K_\mathfrak{p}))$ for each bad nonarchimedean place $\mathfrak{p}$. Then $rE(K)$ is a subgroup of $E(F)$ that is free of rank 1, and $rE(K)$ is contained in $E_0(K_\mathfrak{p})$ for every $\mathfrak{p}$.

We will need a diophantine approximation result. First we define the norm $\| \ \|_v : K \to \mathbf{R}_{\geq 0}$ for each place v of K; it will be characterized by its values on $a \in \mathcal{O}_K$. If v is nonarchimedean and $a \in \mathcal{O}_K - \{0\}$, then $\|a\|_v := q^{-v(a)}$ where q is the size of the residue field, and the discrete valuation v is normalized to take values in $\mathbf{Z}$. If v is real, then $\|a\|_v$ is the standard absolute value of the image of a under $K \to \mathbf{R}$. If v is complex, then $\|a\|_v$ is the square of the standard absolute value of the image of a under $K \to \mathbf{C}$. Define the naive logarithmic height of $a \in K$ by

$$h(a) := \sum_{\text{places } v \text{ of } K} \log \max\{\|a\|_v, 1\}.$$

If one sums over only the nonarchimedean places v, one obtains $\log N_{K/\mathbf{Q}} \operatorname{den}(a)$.

Proposition 7. *Let X be a smooth, projective, geometrically integral curve over K of genus ≥ 1. Fix a place v of K. Let ϕ be a nonconstant rational function on X. Let $P_1, P_2, \ldots$ be a sequence of distinct points in $X(K)$. For sufficiently large m, P_m is not a pole of ϕ, so $z_m := \phi(P_m)$ belongs to K. Then*

$$\lim_{m \to \infty} \frac{\log \|z_m\|_v}{h(z_m)} = 0.$$

Proof. See Section 7.4 of [Ser97]. □

Lemma 8. *The following holds if r is sufficiently large: If $P \in rE(K) - \{O\}$ and $m \in \mathbf{Z} - \{-1, 0, 1\}$, then*

$$\log N_{K/\mathbf{Q}} \operatorname{den}(x(mP)) \geq \frac{9}{10} m^2 \log N_{K/\mathbf{Q}} \operatorname{den}(x(P)) > 0;$$

in particular $\operatorname{den}(x(mP)) \neq \operatorname{den}(x(P))$ and $\operatorname{den}(x(P)) \neq (1)$.

Proof. Let P_1 be a generator of $rE(K)$. The theory of the canonical height in Chapter 8, Section 9 of [Sil92] implies that there is a real number $\hat{h}(P_1) > 0$ (namely, the canonical height of P_1, suitably normalized) such that $h(x(mP_1)) = m^2\hat{h}(P_1) + O(1)$, where the implied constant is independent of $m \in \mathbf{Z}$. Proposition 7 applied to each archimedean v, with $X = E$ and $\phi = x$, shows that if we forget to include the (finitely many) archimedean places in the sum defining h, we obtain

$$\log N_{K/\mathbf{Q}} \operatorname{den}(x(mP_1)) = (1 - o(1))h(x(mP_1)) = (1 - o(1))m^2\hat{h}(P_1)$$

as $|m| \to \infty$. The results follow for large r. □

Of course, there is nothing special about 9/10; any real number in the interval $(1/4, 1)$ would have done just as well.

2.4 Divisibility of denominators

From now on, we suppose that r is large enough that Lemma 8 holds.

Lemma 9. *Let $P, P' \in rE(K) - \{O\}$. Then $\operatorname{den}(x(P)) \mid \operatorname{den}(x(P'))$ if and only if P' is an integral multiple of P.*

Proof. We first show that for any ideal $I \subseteq \mathcal{O}_K$, the set

$$G_I := \{\, Q \in rE(K) : I \mid \operatorname{den}(x(Q)) \,\}$$

is a subgroup of $rE(K)$. (By convention, we consider O to be an element of G_I.) Since an intersection of subgroups is a subgroup, it suffices to prove this when $I = \mathfrak{p}^n$ for some prime $\mathfrak{p}$ and some $n \in \mathbf{Z}_{\geq 1}$. Let $\mathcal{O}_\mathfrak{p}$ be the completion of $\mathcal{O}_K$ at $\mathfrak{p}$. Let $\mathcal{F} \in \mathcal{O}_K[[z_1, z_2]]$ denote the formal group of E with respect to the parameter $z := -x/y$, as in Chapter 4 of [Sil92]. Then there is an isomorphism $\mathcal{F}(\mathfrak{p}\mathcal{O}_\mathfrak{p}) \simeq E_1(K_\mathfrak{p})$, given by $z \mapsto (x(z), y(z))$ where $x(z) = z^{-2} + \dots$ and $y(z) = -z^{-3} + \dots$ are Laurent series with coefficients in $\mathcal{O}_K$. It follows that $G_{\mathfrak{p}^n}$ is the set of points in $rE(K)$ lying in the image of $\mathcal{F}(\mathfrak{p}^{\lceil n/2 \rceil}\mathcal{O}_\mathfrak{p})$. In particular $G_{\mathfrak{p}^n}$ is a subgroup of $rE(K)$.

The "if" part of the lemma follows from the preceding paragraph. Now we prove the "only if" part. Let $G = G_{\operatorname{den}(x(P))}$. Then G is a subgroup of $rE(K) \simeq \mathbf{Z}$, so G is free of rank 1. Let Q be a generator of G. By definition of G, we have $P \in G$, so P is a multiple of Q. By the "if" part already proved, $\operatorname{den}(x(Q)) \mid \operatorname{den}(x(P))$. On the other hand, $Q \in G$, so $\operatorname{den}(x(P)) \mid \operatorname{den}(x(Q))$ by definition of G. Thus $\operatorname{den}(x(Q)) = \operatorname{den}(x(P))$. By Lemma 8, $Q = \pm P$. If $\operatorname{den}(x(P)) \mid \operatorname{den}(x(P'))$, then $P' \in G = \mathbf{Z}Q = \mathbf{Z}P$. □

Lemma 10. *If $I \subseteq \mathcal{O}_K$ is a nonzero ideal, then there exists $P \in rE(K) - \{O\}$ such that $I \mid \operatorname{den}(x(P))$.*

Proof. We use the notation of the previous proof. It suffices to show that $G_{\mathfrak{p}^n}$ is nontrivial. This holds since the image of $\mathcal{F}(\mathfrak{p}^{\lceil n/2 \rceil}\mathcal{O}_\mathfrak{p})$ under $\mathcal{F}(\mathfrak{p}\mathcal{O}_\mathfrak{p}) \simeq E_1(K_\mathfrak{p})$ is an open subgroup of $E(K_\mathfrak{p})$, hence of finite index. □

Lemma 11. *Suppose $P \in rE(K) - \{O\}$ and $m \in \mathbf{Z} - \{0\}$. Let $t = x(P)$ and $t' = x(mP)$. Then* $\mathrm{den}(t) \mid \mathrm{num}((t/t' - m^2)^2)$.

Proof. Suppose that $\mathfrak{p}$ is a prime dividing $\mathrm{den}(t)$. Let $v_\mathfrak{p} : K_\mathfrak{p} \to \mathbf{Z} \cup \{\infty\}$ denote the discrete valuation associated to $\mathfrak{p}$. Then $n := v_\mathfrak{p}(z(P))$ is positive. Since $x = z^{-2} + \dots$ is a Laurent series with coefficients in $\mathcal{O}_K$, we have $x(P) \in z(P)^{-2}(1+\mathfrak{p}^n\mathcal{O}_\mathfrak{p})$. Using the formal group, we see that $z(mP) \in mz(P)+\mathfrak{p}^{2n}\mathcal{O}_\mathfrak{p}$; in particular $v_\mathfrak{p}(z(mP)) \geq n$, so $x(mP) \in z(mP)^{-2}(1 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p})$. Thus

$$\frac{t}{t'} = \frac{x(P)}{x(mP)} \in \left(\frac{z(mP)}{z(P)}\right)^2 (1 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p})\,.$$

But $\frac{z(mP)}{z(P)} \in m + \mathfrak{p}^n\mathcal{O}_\mathfrak{p}$, so $t/t' \in m^2 + \mathfrak{p}^n\mathcal{O}_\mathfrak{p}$, so $\mathfrak{p}^n \mid \mathrm{num}(t/t' - m^2)$. On the other hand, $\mathfrak{p}^{2n}$ is the exact power of $\mathfrak{p}$ dividing $\mathrm{den}(t)$. Applying this argument to every $\mathfrak{p}$ proves $\mathrm{den}(t) \mid \mathrm{num}((t/t' - m^2)^2)$. □

2.5 Diophantine definition of $\mathcal{O}_F$ over $\mathcal{O}_K$

Lemma 12. *With hypotheses as in Theorem 1, there exists a subset $S \subseteq \mathcal{O}_K$ such that S is diophantine over $\mathcal{O}_K$ and $\{\, m^2 : m \in \mathbf{Z}_{\geq 1} \,\} \subseteq S \subseteq \mathcal{O}_F$.*

Proof. Let c and c' be the constants of Lemmas 4 and 5, respectively. By Lemma 8, if $\ell \in \mathbf{Z}_{\geq 1}$ is sufficiently large, then

$$c' N_{K/\mathbf{Q}}\mathrm{den}(x(\ell P_0))^{1/2} > N_{K/\mathbf{Q}}\mathrm{den}(x(P_0)^c)$$

for all $P_0 \in rE(K) - \{O\}$. Fix such an ℓ.

Let S be the set of $\mu \in \mathcal{O}_K$ such that there exist $P_0, P', P' \in rE(K) - \{O\}$ and $t_0, t, t' \in F$ such that

1. $P = \ell P_0$
2. $t_0 = x(P_0)$, $t = x(P)$, $t' = x(P')$
3. $(\mu + 1)(\mu + 2)\dots(\mu + n) \mid \mathrm{den}(t_0)$
4. $\mathrm{den}(t) \mid \mathrm{den}(t')$
5. $\mathrm{den}(t) \mid \mathrm{num}((t/t' - \mu)^2)$

It follows from Lemma 3 that S is diophantine over $\mathcal{O}_K$.

Suppose $m \in \mathbf{Z}_{\geq 1}$. We wish to show that $\mu := m^2$ belongs to S. By Lemma 10, there exists $P_0 \in rE(K) - \{O\}$ such that $(\mu+1)(\mu+2)\dots(\mu+n) \mid \mathrm{den}(x(P_0))$. Let $P = \ell P_0$ and $P' = mP$. Let $t_0 = x(P_0)$, $t = x(P)$, and $t' = x(P')$. Then conditions (1), (2), and (3) in the definition of S are satisfied, and (4) and (5) follow from Lemmas 9 and 11, respectively. Hence $m^2 \in S$.

Now suppose that $\mu \in S$. We wish to show that $\mu \in \mathcal{O}_F$. Fix P_0, P, P', t_0, t, t' satisfying (1) through (5). By (4) and Lemma 9, $P' = mP$ for some nonzero $m \in \mathbf{Z}$. By Lemma 11, $\mathrm{den}(t) \mid \mathrm{num}((t/t' - m^2)^2)$. On the other hand, (5) says that $\mathrm{den}(t) \mid \mathrm{num}((t/t' - \mu)^2)$. Therefore $\mathrm{den}(t)^{1/2} \mid \mathrm{num}(\mu - m^2) = (\mu - m^2)$. (Note that each prime of $\mathcal{O}_F$ or of $\mathcal{O}_K$ that appears in $\mathrm{den}(t)$ must occur to

an even power, since t is the x-coordinate of a point on $y^2 = x^3 + ax + b$. Hence $\mathrm{den}(t)^{1/2}$ is a well-defined ideal.) Write $\mu = \sum_{i=0}^{s-1} a_i \alpha^i$ with $a_i \in F$. By (3) and Lemma 4, $N_{K/\mathbf{Q}}(Da_i) \leq N_{K/\mathbf{Q}}(\mathrm{den}(t_0))^c$. By definition of ℓ, we have $N_{K/\mathbf{Q}}(\mathrm{den}(t_0))^c < c' N_{K/\mathbf{Q}} \mathrm{den}(t)^{1/2}$. Combining these shows that the hypotheses of Lemma 5 hold for $w = m^2$ and $I = \mathrm{den}(t)^{1/2}$ (as an ideal in $\mathcal{O}_F$). Thus $\mu \in \mathcal{O}_F$. □

Proof of Theorem 1. Let S be the set given by Lemma 12. Then $S_1 := \{ s - s' : s, s' \in S \}$ contains all odd integers at least 3, because of the identity $(m+1)^2 - m^2 = 2m + 1$. Next, $S_2 := S_1 \cup \{ 4 - s : s \in S_1 \}$ contains all odd integers, and $S_3 := S_2 \cup \{ s+1 : s \in S_2 \}$ contains $\mathbf{Z}$. Let $\beta_1, \ldots, \beta_b$ be a $\mathbf{Z}$-basis for $\mathcal{O}_F$. Then $S_4 := \{ a_1\beta_1 + \cdots + a_b\beta_b : a_1, \ldots, a_b \in S_3 \}$ contains $\mathcal{O}_F$.

But $S \subseteq \mathcal{O}_F$, so $S_i \subseteq \mathcal{O}_F$ for $i = 1, 2, 3, 4$. In particular, $S_4 = \mathcal{O}_F$. Also, S is diophantine over $\mathcal{O}_K$, so each S_i is diophantine over $\mathcal{O}_K$. In particular, $\mathcal{O}_F = S_4$ is diophantine over $\mathcal{O}_K$. □

2.6 Questions

1. Is it true that for every number field K, there exists an elliptic curve E over $\mathbf{Q}$ such that $\mathrm{rk}\, E(\mathbf{Q}) = \mathrm{rk}\, E(K) = 1$? The author would conjecture so. If so, then Hilbert's Tenth Problem over $\mathcal{O}_K$ is undecidable for every number field K.
2. Can one weaken the hypotheses of Theorem 1 and give a diophantine definition of $\mathcal{O}_F$ over $\mathcal{O}_K$ using any elliptic curve E over K with $\mathrm{rk}\, E(K) = 1$, not necessarily defined over F? Such elliptic curves may be easier to find. But our proof of Theorem 1 seems to require the fact that E is defined over F and has $\mathrm{rk}\, E(F) = 1$, since Lemma 5 fails if the ideal I of $\mathcal{O}_F$ is instead assumed to be an ideal of $\mathcal{O}_K$.
3. Can one prove an analogue of Theorem 1 in which the elliptic curve is replaced by an abelian variety?

References

[CZ00] Gunther Cornelissen and Karim Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 253–260.

[Dav53] Martin Davis, *Arithmetical problems and recursively enumerable predicates*, J. Symbolic Logic **18** (1953), 33–41.

[Den80] J. Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236.

[DL78] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391.

[DLPVG00] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel (eds.), *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, American Mathematical Society, Providence, RI, 2000, Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436.

[Eis] Kirsten Eisenträger, Ph. D. thesis, University of California, Berkeley, in preparation.

[KR92] K. H. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbf{C}(t_1, t_2)$, J. Algebra **150** (1992), no. 1, 35–44.

[Mat70] Ju. V. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282.

[Maz94] B. Mazur, *Questions of decidability and undecidability in number theory*, J. Symbolic Logic **59** (1994), no. 2, 353–371.

[MB] Laurent Moret-Bailly, paper in preparation, extending results presented in a lecture 18 June 2001 at a conference in honor of Michel Raynaud in Orsay, France.

[Phe88] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620.

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8.

[Phe00] Thanases Pheidas, *An effort to prove that the existential theory of* $\mathbf{Q}$ *is undecidable*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 237–252.

[PZ00] Thanases Pheidas and Karim Zahidi, *Undecidability of existential theories of rings and fields: a survey*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 49–105.

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Shl89] Alexandra Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939–962.

[Shl92] Alexandra Shlapentokh, *Hilbert's tenth problem for rings of algebraic functions in one variable over fields of constants of positive characteristic*, Trans. Amer. Math. Soc. **333** (1992), no. 1, 275–298.

[Shl00a] Alexandra Shlapentokh, *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic*, Pacific J. Math. **193** (2000), no. 2, 463–500.

[Shl00b] Alexandra Shlapentokh, *Hilbert's tenth problem over number fields, a survey*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Amer. Math. Soc., Providence, RI, 2000, pp. 107–137.

[Sil92] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Vid94] Carlos R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253.