HILBERT’S TENTH PROBLEM AND MAZUR’S CONJECTURES IN COMPLEMENTARY SUBRINGS OF NUMBER FIELDS

KIRSTEN EISENTRÄGER, GRAHAM EVEREST, AND ALEXANDRA SHLAPENTOKH

Abstract. We show that Hilbert’s Tenth Problem is undecidable for complementary subrings of number fields and that the $p$-adic and archimedean ring versions of Mazur’s conjectures do not hold in these rings. More specifically, given a number field $K$, a positive integer $t > 1$, and $t$ nonnegative computable real numbers $\delta_1, \ldots, \delta_t$ whose sum is one, we prove that the nonarchimedean primes of $K$ can be partitioned into $t$ disjoint recursive subsets $S_1, \ldots, S_t$ of densities $\delta_1, \ldots, \delta_t$, respectively such that Hilbert’s Tenth Problem is undecidable for each corresponding ring $O_{K,S_i}$. We also show that we can find a partition as above such that each ring $O_{K,S_i}$ possesses an infinite Diophantine set which is discrete in every topology of the field. The only assumption on $K$ we need is that there is an elliptic curve of rank one defined over $K$.

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 $x_1, \ldots, x_n \in \mathbb{Z}$. In 1969 Matiyasevich [8], using work by Davis, Putnam and Robinson (see [5]), 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 recursive commutative rings $R$. We will refer to this analogue of the original problem as Hilbert’s Tenth Problem over $R$. Perhaps the most important unsolved problem in this area is the case of $R = \mathbb{Q}$. One natural approach to showing that Hilbert’s Tenth Problem is undecidable for a ring $R$ of characteristic 0 is to show that $\mathbb{Z}$ admits a Diophantine definition over $R$, or more generally that there is a Diophantine model of the ring $\mathbb{Z}$ over $R$. We define these notions below.

Definition 1.1. Let $R$ be a commutative ring. Suppose $A \subseteq R^k$ for some $k \in \mathbb{N}$. We say that $A$ has a Diophantine definition over $R$ if there exists a polynomial

$$f(t_1, \ldots, t_k, x_1, \ldots, x_n) \in R[t_1, \ldots, t_k, x_1, \ldots, x_n]$$

such that for any $(t_1, \ldots, t_k) \in R^k$,

$$(t_1, \ldots, t_k) \in A \iff \exists x_1, \ldots, x_n \in R, f(t_1, \ldots, t_k, x_1, \ldots, x_n) = 0.$$

In this case we also say that $A$ is a Diophantine subset of $R^k$, or that $A$ is Diophantine over $R$. 

1991 Mathematics Subject Classification. 11G05, 11U05.

K.E. was partially supported by National Science Foundation grants DMS-0801123, DMS-1056703 and a Sloan Research Fellowship. A.S. was partially supported by National Science Foundation grant DMS-0650927 and a grant from the John Templeton Foundation.

Sadly, the second author passed away before the final version of the paper was completed.
Remark 1.2. Suppose that $R$ is a domain whose quotient field is not algebraically closed. Then

(a) Relaxing Definition 1.1 to allow an arbitrary finite conjunction of equations in place of the single equation on the right hand side does not enlarge the collection of Diophantine sets.

(b) Finite unions and finite intersections of Diophantine sets are Diophantine.

See [28] for details.

Definition 1.3. A Diophantine model of $\mathbb{Z}$ over a ring $R$ is a Diophantine subset $A \subseteq R^k$ for some $k$ together with a bijection $\phi: \mathbb{Z} \to A$ such that the graphs of addition and multiplication (subsets of $\mathbb{Z}^3$) correspond under $\phi$ to Diophantine subsets of $A^3 \subseteq R^{3k}$.

In 1992 Mazur formulated a conjecture that would imply that a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$ does not exist, and which also ruled out the existence of a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ [4]. One form of Mazur's conjecture was that for a variety $X$ over $\mathbb{Q}$, the closure of $X(\mathbb{Q})$ in the topological space $X(\mathbb{R})$ should have at most finitely many connected components. This conjecture also implied that no infinite set which is discrete in the archimedean topology has a Diophantine definition over $\mathbb{Q}$.

Mazur also formulated a version of his conjecture applying to both archimedean and nonarchimedean completions of arbitrary number fields [12, p. 257]:

Question 1.4. Let $V$ be any variety defined over a number field $K$. Let $S$ be a finite set of places of $K$, and consider $K_S = \prod_{v \in S} K_v$ viewed as locally compact topological ring. Let $V(K_S)$ denote the topological space of $K_S$-rational points. For every point $p \in V(K_S)$ define $W(p) \subset V$ to be the subvariety defined over $K$ that is the intersection of Zariski closures of the subsets $V(K) \cap U$, where $U$ ranges through all open neighborhoods of $p$ in $V(K_S)$. As $p$ ranges through the points of $V(K_S)$, are there only a finite number of distinct subvarieties $W(p)$?

Fix a number field $K$ and a place $p$. If Question 1.4 has a positive answer for $K$ and $S := \{p\}$, then there does not exist an infinite, $p$-adically discrete, Diophantine subset of $K$. See [16, Proof of Prop. 1.5] for the proof.

So one way to answer Question 1.4 (negatively) for $K$ would be to construct a Diophantine definition of an infinite discrete $p$-adic set over a number field $K$. Unfortunately, at the moment such a construction seems out of reach. So instead we consider analogues in which $K$ is replaced by one of its large integrally closed subrings $O_{K,S}$:

Definition 1.5. For a number field $K$, let $\mathcal{P}_K$ denote the set of finite primes of $K$, and let $O_K$ denote the ring of integers. Given a set $S$ of prime ideals, not necessarily finite, the ring $O_{K,S}$ is defined to be the subring of $K$ defined by

$$O_{K,S} = \{ x \in K : \text{ord}_p x \geq 0 \text{ for all } p \notin S \}.$$ 

Observe that if $S = \emptyset$, then $O_{K,S} = O_K$ and if $S = \mathcal{P}_K$, then $O_{K,S} = K$. If $S$ is finite, $O_{K,S}$ is called a ring of $S$-integers. In the case where the complement of $S$ is finite, the rings $O_{K,S}$ are semi-local. We will call all rings $O_{K,S}$ with infinite $S$ big rings.

To measure the “size” of a set of primes one can use natural density defined below.
Definition 1.6. Let $S \subseteq \mathcal{P}_K$. The natural density of $S$ is defined to be the limit
\[
\lim_{X \to \infty} \frac{\# \{ p \in S : Np \leq X \}}{\# \{ \text{all } p : Np \leq X \}}
\]
if it exists. If the limit above does not exist, one can talk about upper density by substituting $\lim \sup$ for $\lim$, or lower density by substituting $\lim \inf$ for $\lim$.

The study of Hilbert's Tenth Problem and of the archimedean version of Mazur's conjecture over rings of $S$-integers has produced Diophantine definitions of $\mathbb{Z}$ and discrete archimedean sets over large subrings of some number fields ([23], [24], [25], [26], [27], and [29]). In 2003 Poonen proved that there exists a recursive set $S$ of primes of natural density one such that Hilbert's Tenth Problem is undecidable for $\mathbb{Z}[S^{-1}]$. He also constructed an infinite discrete Diophantine set (in the archimedean topology) in this ring. In [16] Poonen and Shlapentokh prove that, if there exists an elliptic curve $E$ over a number field $K$ with $\text{rank}(E(K)) = 1$, then there exists a recursive set $S$ of primes of density one such that Hilbert's Tenth Problem is undecidable for $\mathcal{O}_{K,S}$. They also show that there is an infinite Diophantine subset $A$ of $\mathcal{O}_{K,S}$ such that for all places $v$ of $K$, the set $A$ is discrete when viewed as a subset of the completion $K_v$.

In [6], Eisenträger and Everest reconsidered the original result of Poonen from a different point of view, looking for a “covering” of $\mathbb{Q}$ by big rings that come from complementary sets of primes. More specifically, they proved that the rational primes can be partitioned into two disjoint sets $S_1, S_2$ such that Hilbert's Tenth Problem is undecidable over both $\mathcal{O}_{K,S_1}$ and $\mathcal{O}_{K,S_2}$. These results were improved by Perlega in [14] to show that the two sets can be of arbitrary computable densities.

In this paper we generalize the results of [16], [6] and [14] to prove the following theorems:

**Theorem 1.7.** Let $K$ be a number field, and assume there is an elliptic curve defined over $K$ with $K$-rank equal to 1. For every $t > 1$ and every collection $\delta_1, \ldots, \delta_t$ of nonnegative computable real numbers adding up to 1, the set of the nonarchimedean valuations of $K$ may be partitioned into $t$ mutually disjoint recursive subsets $S_1, \ldots, S_t$ of natural densities $\delta_1, \ldots, \delta_t$, respectively, with the property that each ring $\mathcal{O}_{K,S_i}$ contains a Diophantine subset discrete under any valuation of $K$ (archimedean or nonarchimedean).

**Theorem 1.8.** Assume there is an elliptic curve defined over $K$ with $K$-rank equal to 1. For every $t > 1$ and every collection $\delta_1, \ldots, \delta_t$ of nonnegative computable real numbers adding up to 1, the set of the nonarchimedean valuations of $K$ may be partitioned into $t$ mutually disjoint recursive subsets $S_1, \ldots, S_t$ of natural densities $\delta_1, \ldots, \delta_t$, respectively, with the property that $\mathbb{Z}$ admits a Diophantine model in each ring $\mathcal{O}_{K,S_i}$. In particular, Hilbert's Tenth Problem is undecidable for each ring $\mathcal{O}_{K,S_i}$.

Recently, Mazur and Rubin [13] showed that if the Shafarevich-Tate conjecture holds, then there always exists an elliptic curve defined over $K$ whose $K$-rank is one.

When proving Theorems 1.7 and 1.8, we will show that given any partition of the nonarchimedean primes into sets $W_1, \ldots, W_t$ of densities $\delta_1, \ldots, \delta_t$, the sets $S_i$ can be constructed by changing the $W_i$’s by sets of density zero. So our results can be seen as answering the following fundamental questions up to sets of density zero.
Questions 1.9.

1. For which number fields $K$ and which subsets $S$ of $\mathcal{P}_K$ is Hilbert’s Tenth Problem (un)decidable over $\mathcal{O}_{K,S}$?

2. For which number fields $K$ and which subsets $S$ of $\mathcal{P}_K$ is there a Diophantine model of $\mathbb{Z}$ over $\mathcal{O}_{K,S}$?

3. For which number fields $K$ and subsets $S$ of $\mathcal{P}_K$ is there an infinite subset of $\mathcal{O}_{K,S}$ which is Diophantine over $\mathcal{O}_{K,S}$ and discrete in every topology of the field $K$?

One question which is not addressed by this paper is for which number fields $K$ and which subsets $S$ of $\mathcal{P}_K$ there is a Diophantine definition of $\mathbb{Z}$ (or $\mathcal{O}_K$) over $\mathcal{O}_{K,S}$.

1.1. Overview of proof. The goal is to prove Theorems 1.7 and 1.8 by partitioning $\mathcal{P}_K$ into $t$ disjoint sets $S_1, \ldots, S_t$, so that each ring $\mathcal{O}_{K,S_r}$ admits a Diophantine model of the integers or has discrete infinite Diophantine subsets. In Sections 6 and 7 we first show how to find $t$ not necessarily disjoint sets, whose union is $\mathcal{P}_K$ such that the corresponding big rings have desirable properties. In Section 8 we show that these sets can also be chosen to be mutually disjoint and of the required density.

To construct infinite discrete Diophantine sets we will proceed as in [16] and construct a Diophantine set containing only the elements of a sequence converging (in all topologies of the number field) to a limit not in the set.

To construct a Diophantine model of $\mathbb{Z}$ inside $\mathcal{O}_{K,S_r}$, it is enough to construct a model of the structure

$$Z := (\mathbb{Z}_{\geq 1}, 1, +, B),$$

where $B$ is a unary predicate for the set $\{2^n + n^2 : n \in \mathbb{Z}_{\geq 1}\}$ (see [16, Lemma 3.16]). A Diophantine model of $Z$ over a ring $R$ is a Diophantine subset $A \subseteq R^m$ for some $m$ together with a bijection $\phi : \mathbb{Z}_{\geq 1} \rightarrow A$ such that $\phi(B)$ is Diophantine over $A$ and such that the graph of addition (a subset of $\mathbb{Z}_{\geq 1}^2$) corresponds under $\phi$ to a Diophantine subset of $A^3$.

In order to find suitable sets $S_r$ we work with an elliptic curve $E$ of rank one over $K$ and a point $P$ of infinite order that is a suitable multiple of the generator for the non-torsion part. We will construct $t$ (infinite) sequences of primes

$$\{\ell_{1,1}, \ell_{2,1}, \ldots \}, \ldots, \{\ell_{1,t}, \ell_{2,t}, \ldots \}$$

such that for each $r \in \{1, \ldots, t\}$, we have that $E(\mathcal{O}_{K,S_r}) \cap zE(K)$ for a suitable positive integer $z$, is the union of $\{\pm \ell_{1,r}P, \pm \ell_{2,r}P, \ldots \}$ and some finite set. We then show that $A_r := \{x_{\ell_{i,r}} : i \in \mathbb{Z}_{\geq 1}\}$ is a Diophantine model of $Z$ in $\mathcal{O}_{K,S_r}$ via the bijection $\phi : \mathbb{Z}_{\geq 1} \rightarrow A_r$ sending $i$ to $x_{\ell_{i,r}}$. To prove Theorem 1.7 we construct $t$ different sequences of primes and sets $S_r$ and show that $A_r$ as above is a discrete Diophantine set.

The paper is organized as follows. In Section 2 we review recursive presentations of primes of number fields, in Section 3 we give some background about primitive divisors and their properties, and then use these properties to prove that certain terms in divisibility sequences have many prime ideal divisors. Section 4 describes the technical changes in the assumptions and proofs in this paper relative to proofs and assumptions in [16]. Section 5 reviews and extends some density results from [16]. In Sections 6 and 7 we construct the rings and the sets with the required properties. Finally, Section 8 shows how to adjust the sets of primes constructed in Sections 6 and 7 to make them complementary.
2. Computable Sets of Primes in Number Fields

In this section we briefly discuss a presentation of primes in number fields and a way to define recursive sets of primes. We assume that a number field \( K \) of degree \( n \) over \( \mathbb{Q} \) is presented in terms of its integral basis over \( \mathbb{Q} \). (Such a basis always exists and can be constructed given an irreducible polynomial over \( \mathbb{Q} \) of a field generator. See for example section 7.3 of [17].) Elements of the field will be presented via \( n \)-tuples of the coordinates with respect to the basis. Given a \( K \)-prime \( p \), we will present this prime by a pair \((p, \alpha_p)\), where \( p \) is the \( \mathbb{Q} \)-prime below \( p \) and \( \alpha_p \in K \) is an algebraic integer such that \( \text{ord}_p \alpha_p = 1 \) but \( \text{ord}_q \alpha_p = 0 \) for any prime \( q \neq p \) conjugate to \( p \) over \( \mathbb{Q} \). Since the choice \( \alpha_p \) is not unique we can choose the first suitable \( \alpha_p \) under some ordering of the field. Given an integral basis for \( K \), the map \( p \mapsto (\alpha_{p_1}, \ldots, \alpha_{p_m}) \), where \( p = \prod_{i=1}^k p_i^{e_i} \) is the factorization of \( p \) in \( K \), is recursive. Further, given an element of \( K \), one can effectively determine the factorization of the divisor of this element, and given a prime compute its norm. Given a set of primes we can now say that it is computable if the corresponding set of \( n \)-tuples \( (p, \alpha_p) \) is computable. It is also not hard to see that for any set of \( K \)-primes \( \mathcal{W} \), the ring \( \mathcal{O}_{K,\mathcal{W}} \) from Definition 1.5 is computable if and only if \( \mathcal{W} \) is computable. For more details see Section 4 of [2].

3. Primitive Divisors

Let \( E \) denote an elliptic curve in Weierstrass form,

\[
E : y^2 = x^3 + a_4 x + a_6,
\]

defined over \( \mathcal{O}_K \). For background, definitions and the properties of elliptic curves used in this paper, consult [30] and [32]. Let \( K \) denote an algebraic number field of degree \( d = [K : \mathbb{Q}] \) over \( \mathbb{Q} \). Throughout the paper, \( E(K) \) denotes the group of \( K \)-rational points of \( E \) and \( \mathcal{O} \) denotes the point at infinity, the identity for the group of \( K \)-rational points. Suppose \( P \) denotes a \( K \)-rational point, \( P \in E(K) \), which is not torsion. Write \( nP = (x_n, y_n) \). The assumptions on \( E \) allow the factorization

\[
(x_n) = (x(nP)) = a_n(P)/b_n^2(P)
\]

of the principal fractional ideal \( (x(nP)) \) into relatively prime integral ideals \( a_n \) and \( b_n \). Assuming \( P \) is non-torsion guarantees that all of the terms in the sequence \( \mathfrak{b} = (\mathfrak{b}_n) \) are non-zero.

In the rational case, we may take \( \mathfrak{b}_n \) to be a positive integer. Silverman [31] proved that when \( P \) is a rational point, for all sufficiently large \( n \), we have that \( \mathfrak{b}_n \) has a primitive divisor, that is, a divisor of \( \mathfrak{b}_n \) which is coprime to \( \mathfrak{b}_m \) for all positive integers \( m < n \). In general, the expression primitive ideal divisor of a term \( \mathfrak{b}_n \) is used to describe an ideal \( \mathfrak{I} \) which divides \( \mathfrak{b}_n \) but no \( \mathfrak{b}_m \) with \( m < n \). Cheon and Hahn [3] extended Silverman’s result from [31] to algebraic number fields, showing that for all sufficiently large \( n \), it is the case that \( \mathfrak{b}_n \) has a primitive ideal divisor.

Results about primitive divisors have a long and fine tradition for certain sequences which satisfy a linear recurrence relation. An interested reader can find more results concerning the existence of primitive divisors in [1], [7], [18], [19], [20] and [33].

For a point \( P \) on \( E \) and a nonzero integer \( n \), define \( S_n(P) \) to be the set of all prime ideals of \( \mathcal{O}_K \) that divide the ideal \( \mathfrak{b}_n(P) \).
We will use the following properties of the sequence \(b_n(P)\) and the sets \(S_n(P)\):

**Lemma 3.1.** Let \(P\) be a point of infinite order on an elliptic curve \(E\) defined over a number field \(K\) as above.

1. Let \(n, m \in \mathbb{Z} - \{0\}\) and let \((m, n)\) be their gcd. Then \(S_m(P) \cap S_n(P) = S_{(m,n)}(P)\). In particular, if \(P\) is an integral point of infinite order, and \((m, n) = 1\), then \(S_m(P) \cap S_n(P) = \emptyset\).

2. The sequence \(b_n\) is a divisibility sequence, meaning that \(b_m \mid b_n\) as ideals, whenever \(m \mid n\).

**Proof.** The proof follows from the standard local theory of elliptic curves, see for example Chapters 4 and 7 in [30]: For \(p \in \mathcal{P}_K\), let \(K_p\) be the completion of \(K\) at \(p\) and let

\[
E_1(K_p) = \{O\} \cup \{R \in E(K_p) : \text{ord}_p(x(R)) \leq -2\}.
\]

From [30, Proposition VII.2.2], we have that \(E_1(K)\) with the elliptic curve addition is isomorphic to \(\hat{E}(\mathcal{M})\) under the formal group addition, where \(\hat{E}\) is the formal group associated to \(E\) and \(\mathcal{M}\) is the valuation ideal of \(K_p\). Note that while the proposition in [30] assumes that the Weierstrass equation is minimal, this assumption is not used in the proof. The first assertion of the lemma now follows from the fact that \(E_1(K_p)\) is a group.

Furthermore, using again the fact that the elliptic curve addition on \(E_1(K_p)\) corresponds to the addition in the formal group [30, Proposition VII.2.2], together with [30, Corollary IV.4.4], we have that for all \(R \in E_1(K_p) - \{O\}\)

\[
\text{ord}_p(x(nR)) \leq \text{ord}_p(x(R)) - 2\text{ord}_p(n)
\]

and the second assertion of the lemma follows at once.

To carry out our construction we need to prove that certain terms in the sequence \(b_n(P)\) have many primitive ideal divisors. This is made precise in the next theorem.

**Theorem 3.2.** Let \(p\) denote a prime and write \(q = p^t - 1\) for some fixed \(t \geq 2\). Suppose \(Q\) is a \(K\)-rational point of infinite order and \(P = qQ\). Let \(\{(b_m)\}(P)\) be the sequence of ideals coming from the multiples of \(P\) as in equation (3.2). For every large enough \(n\), which is coprime to \(p\), the term \(b_n(P)\) has at least \(t\) primitive ideal divisors. The same is true for the terms of the sequence \(b_n(pP)\).

**Proof.** Let \(n\) be an integer coprime to \(p\) and assume that \(n\) is large enough so that \(b_k(Q)\) has a primitive divisor for all \(k > n\). Let \(p_i^n\) be a primitive prime ideal divisor of \(b_{p_i^n}(Q)\), for \(i = 0, \ldots, t - 1\). Observe that for \(i \neq j\) we have that \(p_i^n \neq p_j^n\). We claim that

\[
p_p^n \in S_{p^t-1}(Q) - S_{p^t-1}(Q) = S_n(P) - S_m(P)
\]

for any positive \(m < n\). Indeed, since \(p^n\) divides \(p^t-1\) we have that \(p_i^n \in S_{p^t-1}(Q)\). Suppose also \(p_p^n \in S_{p^t-1}(Q)\), where \(m < n\). By Lemma 3.1, part (1), we can assume without loss of generality that \(m\) divides \(n\) and thus is prime to \(p\). We now also have that \(p_p^n \in S_{p^t-1}(Q)\), contradicting the assumption that \(p_p^n\) is a primitive prime ideal divisor of \(b_{p^n}(Q)\). Thus \(p_p^n, i = 0, \ldots, t - 1\) are ideal divisors of \(b_n(p^t-1)\).

Similarly, \(p_p^n \in S_{p^m}(Q) - S_{p^m}(Q)\) for any positive \(m < n\). Indeed, as above, since \(p^n\) divides \(p^t\) we have that \(p_p^n \in S_{p^n}(Q)\). Suppose also \(p_p^n \in S_{p^m}(Q)\), where \(0 < m < n\). Again, by Lemma 3.1, part (1), we can assume without loss of generality that \(m\) divides \(n\) and thus is prime to \(p\). We now also have that \(p_p^n \in S_{p^m}(Q) \cap S_{p^n}(Q) = S_{p^m}(Q)\),
contradicting the assumption that \( p_{p' n} \) is a primitive prime ideal divisor of \( b_{p' n}(Q) \). Thus \( p_{p' n}, i = 0, \ldots, t - 1 \) are primitive ideal divisors of \( b_n(p' Q) \).

\[ \square \]

4. SOME TECHNICAL MATTERS

Below we construct two collections of rings \( \mathcal{O}_{K,S_1} \): one to produce infinite discrete Diophantine sets and the other to construct a Diophantine model of the integers. The rings \( \mathcal{O}_{K,S_1} \) are constructed by generalizing the techniques from [16]. For the most part we use the same notation as in [16], but with the following modifications:

In [16], the authors define \( S_{\text{bad}} \subseteq P_K \) to be the set of primes that ramify in \( K/\mathbb{Q} \), the primes for which the reduction of the chosen Weierstrass model is singular (this includes all primes above 2), and the primes at which the coordinates of \( P \) are not integral. In the rings in [16] for which undecidability is then shown the primes in \( S_{\text{bad}} \) are always inverted. I.e. the rings are of the form \( \mathcal{O}_{K,S} \) with \( S_{\text{bad}} \subseteq S \). We have to avoid inverting the primes in \( S_{\text{bad}} \) in each ring, otherwise the sets \( S_i \) will not be mutually disjoint. That means that in our paper the fractional ideal generated by the \( x \)-coordinate of \( nP \) is of the form \( x(nP) = a_n/d_n \) (with \( a_n, d_n \) coprime integral ideals) and we do not have a separate ideal \( b_n \) that includes the contribution from the primes in \( S_{\text{bad}} \) as in [16].

In view of the above, we need to show that the undecidability results in [16] can be proved without inverting the primes in \( S_{\text{bad}} \). Below we note that (1) \( P \) can be chosen to be integral, that (2) we can avoid inverting the primes that ramify in \( K/\mathbb{Q} \) and (3) that we can avoid inverting the primes for which the reduction of the Weierstrass model of \( E \) is singular:

(1) We assume that the point \( P := zQ \) has coordinates in \( \mathcal{O}_K \). Here \( Q \) generates \( E(K)/E(K)_{\text{tors}} \) and \( z = 2^{t-1}3^{t-1} \# E(K)_{\text{tors}} \). This assumption is possible by Lemma 4.1 below. Our assumption implies that the point \( P \) does not contribute any primes to \( S_{\text{bad}} \).

(2) Not inverting the primes that ramify in \( K/\mathbb{Q} \). The fact that \( S_{\text{bad}} \) contains the primes that ramify in \( K/\mathbb{Q} \) is used in [16] to prove Lemma 3.3, which is then used to prove Proposition 3.5 in [16]. Our proof below replaces Lemma 3.3 and Proposition 3.5 from [16] with Lemma 3.1 and Theorem 3.2.

(3) Not inverting the primes of bad reduction. Our definitions of \( T_1, S_n, p_n, T_2 \) differ from those in [16]: Our set \( T_1 \) is contained in the set \( T_1 \) defined in [16], and it differs from it by at most finitely many primes (the primes in \( S_{\text{bad}} \)). Our set \( S_n \) contains all prime ideals dividing the denominator ideal of \( x(nP) \), and \( p_n = p_n^{(1)} \) denotes a primitive prime ideal divisor of the largest norm in \( S_n \). This also affects the definition of \( T_2 \). See Notation 4.1 and the sets that are defined before Lemma 6.3 and Lemma 7.3 below.

The primes of bad reduction are relevant in Lemma 3.1 and Corollary 3.2 of [16]. Since we have a different definition of \( p_n^{(1)} \) we don’t need to use these two results. The only other place in [16] where primes of bad reduction are relevant is Lemma 3.10, and we state below why this lemma still holds (see Lemmas 6.3 and 7.3 and their proofs).

**Lemma 4.1.** If \( E \) is an elliptic curve and \( P \in E(K) \), then there exists a curve \( E' \) that is isomorphic to \( E \) over \( K \) via an isomorphism \( \phi \) such that \( P' := \phi(P) \) has coordinates in \( \mathcal{O}_K \).
Proof. If $E$ is given by a Weierstrass equation $E : y^2 = x^3 + ax + b$ and $P \in E(K)$ has coordinates $(\alpha, \beta) \in K$, we can choose an element $u \in K$ such that $u\alpha, u\beta \in \mathcal{O}_K$. We can then consider the curve $E'$ whose Weierstrass equation is given by

$$E' : (y')^2 = (x')^3 + au^4(x') + u^6b,$$

which is isomorphic to $E$ under $\phi : E \to E'$, $(x, y) \mapsto (u^2x, u^3y)$. The point $P' := \phi(P)$ on $E'$ has coordinates in $\mathcal{O}_K$. 

Now we can fix some of our notation:

4.1. Notation.

- Let $K$ be a number field.
- Let $E$ be an elliptic curve of rank 1 over $K$, given by a Weierstrass equation with coefficients in the ring of integers $\mathcal{O}_K$. (In particular, we assume that $K$ is such that such an $E$ exists).
- Let $E(K)_{\text{tors}}$ be the torsion subgroup of $E(K)$.
- For any set $S$ of $K$-primes let $E(K,S)$ be the set of affine points with coordinates in $\mathcal{O}_K$.
- Let $z = 2^{t-1}3^{t-1}\#E(K)_{\text{tors}}$ with $t \geq 1$.
- $P := zQ$, where $Q$ generates $E(K)/E(K)_{\text{tors}}$. As explained above, we may assume $P = (x, y)$ with $x, y \in \mathcal{O}_K$.
- Let $P_0 = \{2, 3, 5, \ldots \}$ be the set of rational primes.
- Let $P_K$ be the set of all finite primes of $K$.
- For $p \in P_K$, let
  - $K_p$ be the completion of $K$ at $p$.
  - $R_p$ be the valuation ring of $K_p$.
  - $\mathbb{F}_p$ be the residue field of $R_p$.
  - $Np = \#\mathbb{F}_p$ be the absolute norm of $p$.
- For $n \neq 0$ write $nP = (x_n, y_n)$ where $x_n, y_n \in K$.
- Write the fractional ideal generated by $x_n$ as
  $$(x_n) = \frac{\mathfrak{a}_n}{\mathfrak{d}_n},$$

where $\mathfrak{a}_n$ and $\mathfrak{d}_n$ are coprime integral ideals.
- For $n$ as above, let $S_n = S_n(P) = \{p \in P_K : p|\mathfrak{d}_n\}$. By assumption on $P$, we have $S_1 = \emptyset$.
- For $\ell \in P_0$, define $a_\ell$ to be the smallest positive number such that $\mathfrak{d}_{\ell a_\ell}$ has at least $t$ primitive divisors. (By Theorem 3.2, applied with $p = 2$ for $\ell \neq 2$ and with $p = 3$ for $\ell = 2$, we have that $a_\ell$ exists and $a_\ell = 1$ for all but finitely many $\ell$.)
- Let $\mathcal{L} = \{\ell \in P_0 : a_\ell > 1\}$ and $L = \prod_{\ell \in \mathcal{L}} \ell^{a_\ell - 1}$.
- For $k = 1, \ldots, t$ define $p_n^{(k)}$ to be the $k$-th largest primitive prime divisor of $\mathfrak{d}_n$ (if it exists). (Order the primitive prime divisors according to their norm, and break ties for prime ideals $p_1, p_2$ of the same norm according to Section 2: compute the corresponding $\alpha_{p_1}, \alpha_{p_2}$ and see which one comes first under some ordering of the field.)
• For a prime $\ell$, define
\[
\mu_{\ell} = \sup_{X \in \mathbb{Z}_{\geq 2}} \frac{\# \{ p \in S_{\ell} : \mathbb{N}p \leq X \}}{\# \{ p \in \mathcal{P}_K : \mathbb{N}p \leq X \}}.
\]

• Let $\mathcal{M}_K$ be the set of all normalized absolute values of $K$.
• Let $\mathcal{M}_{K,\infty} \subset \mathcal{M}_K$ be the set of all archimedean absolute values of $K$.

5. ON DENSITIES OF SOME SETS OF PRIMES

The main result of this section is the proposition below.

**Proposition 5.1.** The natural density of the set $Q(E) = \{ q_{\ell}, \ell \in \mathbb{Z}_{>0} \}$, where $q_{\ell}$ is any primitive divisor of $[\ell]P$ (see Notation 4.1), is zero.

In [16] it was shown that the set $\{ p_{\ell}, \ell \in \mathbb{Z}_{>0} \}$, where $p_{\ell}$ is the largest primitive divisor of $P_{\ell}$, is equal to zero. Below we modify this proof and show that the primitive divisor does not have to be the largest in order for the density to be zero. The key result we need from [16] is stated below.

**Lemma 5.2.** For $n \in \mathbb{Z}_{>0}$ let $\omega(n)$ be the number of distinct prime factors of $n$. For any $t \geq 1$, the density of $\mathbb{Z}(E, t) = \{ p : \omega(#E(F_p)) < t \}$ is 0. (See Lemma 3.12 of [16].)

As in [16] and [15] we also need the following result and an observation.

**Theorem 5.3 (Hasse).** $\#E(F_p) \leq \mathbb{N}p + 1 + 2\sqrt{\mathbb{N}p}$.

**Remark 5.4.** If $p$ is a prime at which $E$ has a good reduction and such that $p$ is a primitive divisor of $\ell P$, then $\ell | \#E(F_p)$. Note that since there are only finitely many primes at which $E$ has a bad reduction, we can ignore these primes when calculating the density.

We now prove Proposition 5.1.

**Proof.** We choose $\varepsilon > 0$ and show that the upper natural density of $Q(E)$ is less than $\varepsilon$. By the Prime Number Theorem, for some positive constants $C_Q, C_K$ we have

\[
\# \{ p \in \mathcal{P}_Q : p \leq X \} = O(X/\log X) < \frac{C_Q X}{\log X},
\]

\[
\# \{ p \in \mathcal{P}_K : \mathbb{N}p \leq X \} = O(X/\log X) > \frac{C_K X}{\log X}.
\]

Choose $t \in \mathbb{Z}_{>1}$ so that

\[
2^{1-t} < \frac{C_K \varepsilon}{4C_Q}
\]

and choose $X \in \mathbb{R}_{>0}$ large enough so that

\[
\frac{\# \{ p \in \mathcal{Z}(E, t), \mathbb{N}p \leq X \}}{\# \{ p \in \mathcal{P}_K, \mathbb{N}p \leq X \}} < \varepsilon / 2,
\]

and

\[
\left| \frac{\log C_K + \log \varepsilon - \log 4C_Q}{\log X} \right| < 1.
\]

Let $\mathcal{Z}(E, t)$ be the complement of $\mathcal{Z}(E, t)$ in $\mathcal{P}_K$. Let $p \in \mathcal{Z}(E, t)$ and assume $p = q_{\ell}$ for some positive integer $\ell$. In this case,

\[
\ell 2^t < \# \mathcal{E}(F_p) < \mathbb{N}p + 1 + 2\sqrt{\mathbb{N}p} < 4\mathbb{N}p.
\]
and therefore
\[ \ell < 2^{4-t} Np \leq \frac{C_K Np \varepsilon}{4C_Q}. \]

Thus for every \( p \in \mathcal{O}(E) \cap \mathcal{Z}(E, t) \) there exists a unique rational prime \( \ell < \frac{C_K Np \varepsilon}{4C_Q}. \) Consider now the following ratio:
\[
\frac{\# \{ p \in \mathcal{O}(E) : Np \leq X \}}{\# \{ p \in \mathcal{P}_K : Np \leq X \}} = \frac{\# \{ p \in \mathcal{O}(E) \cap \mathcal{Z}(E, t) : Np \leq X \}}{\# \{ p \in \mathcal{P}_K : Np \leq X \}} \leq \varepsilon/2 + \frac{\varepsilon}{4(\log C_K + \log \varepsilon + \log X - \log 4C_Q)} < \varepsilon.
\]

Now we show that it is rare that \( S_\ell \) has a large fraction of the small primes.

**Lemma 5.5.** For any \( \varepsilon > 0 \), the density of \( \{ \ell : \mu_\ell > \varepsilon \} \) is 0.

**Proof.** The statement of this lemma is identical to the statement of Lemma 3.8 of [16] except for the fact that in our case \( S_\ell \) can contain primes of \( S_{\text{bad}} \). However by Lemma 3.1, only finitely many \( \ell \) can be affected by the inclusion of \( S_{\text{bad}} \) primes and therefore the density result is unaffected. \( \square \)

The next lemma is Lemma 3.6 of [16] which we restate here without a proof.

**Lemma 5.6.** Let \( \vec{\alpha} \in \mathbb{R}^n \), let \( I \) be an open neighborhood of 0 in \( \mathbb{R}^n / \mathbb{Z}^n \), and let \( d \in \mathbb{Z}_{>1} \). Then the set of primes \( \ell \equiv 1 \pmod{d} \) such that \( (\ell - 1)\vec{\alpha} \mod 1 \) is in \( I \) has positive lower density.

### 6. Infinite Diophantine Discrete Sets

In this section we construct \( t \) distinct sequences of primes from which we will construct the sets \( S_1, \ldots, S_t \). We start with a lemma which will enable us to show that the sequences we construct are computable.

**Lemma 6.1.** Let \( p_\ell^{(k)} \) and \( \mu_\ell \) be as in Notation 4.1.

1. For all \( k = 1, \ldots, t \), the mapping \( \ell \mapsto p_\ell^{(k)} \) is computable.
2. The mapping \( \ell \mapsto \mu_\ell \) is computable.

**Proof.**

1. Given \( k, \ell \in \mathbb{Z}_{>0} \) we can effectively compute the coordinates of \( x_\ell = x(\ell(P)) \) and determine the factorization of \( d_\ell \) as discussed in the Section 2. By considering the prime factorization of \( d_1, \ldots, d_{\ell-1} \) we can determine which primes occurring in \( d_\ell \) are in fact primitive divisors, compute their norms and determine \( p_\ell^{(k)} \).
sequences. More specifically we let $$V$$ and for such that all of the following hold:

Proof. Condition (5) is equivalent to the requirement that positive lower density. By Lemma 5.5, (2) fails for a set of density 0 to neighborhoods of neighborhood of 0.

Let

The sequences

Proposition 6.2. The sequences $$\{\ell_{1,r}, \ell_{2,r}, \ldots\}$$ for $$r = 1, \ldots, t$$. To do this we describe how to define $$\ell_{i,r}$$ using a set $$V_{i,r}, i \in \mathbb{Z}_{>0}, r = 1, \ldots, t$$ of previously defined elements of the sequences. More specifically we let $$V_{1,1} = \emptyset$$. For $$i > 1$$ we set

and for $$i \geq 1, 1 < r \leq t$$, we set

Let $$\ell_{i,r}$$ be the smallest prime outside $$\mathcal{L}$$ and exceeding the bound implicit in Theorem 3.2 such that all of the following hold:

1. $$\ell_{i,r} > \ell$$ for all $$\ell \in V_{i,r},$$
2. $$\mu_{\ell_{i,r}} \leq 2^{-i},$$
3. $$Np_{\ell_{i,r}}^{(r)} > 2^i$$ for all $$\ell \in V_{i,r} \cup \{\ell_{i,r}\} \cup \mathcal{L},$$
4. $$\ell_{i,r} \equiv 1 \pmod{i!},$$ and
5. $$|x_{\ell_{i,r}-1}|_v > i$$ for all $$v \in \mathcal{M}_{K,\infty}.$$ We also choose $$\ell_{1,1} > 3.$$

Proposition 6.2. The sequences $$\{\ell_{1,r}, \ell_{2,r}, \ldots\}$$ are well-defined and computable for $$r = 1, \ldots, t$$.

Proof. Condition (5) is equivalent to the requirement that $$(\ell - 1)\bar{\alpha}$$ lie in a certain open neighborhood of 0 in $$(\mathbb{R}/\mathbb{Z})^N$$, since the Lie group isomorphism maps neighborhoods of $$O$$ to neighborhoods of 0. Thus by Lemma 5.6, the set of primes satisfying (4) and (5) has positive lower density. By Lemma 5.5, (2) fails for a set of density 0. Therefore it will suffice to show that (1) and (3) are satisfied by all sufficiently large $$\ell_i$$.

For fixed $$\ell$$, the primes $$p_{\ell_{i,r}}^{(r)}$$ for varying values of $$\ell_{i,r}$$ are distinct since $$p_{\ell_{i,r}}^{(r)}$$ is the $$r$$-th largest primitive divisor of $$\partial_{\ell_{i,r}}$$. So eventually their norms are greater than $$2^i$$. The same holds for $$p_{\ell_{i,r}}^{(r)}$$ for fixed $$\ell \in \mathcal{L}$$. Thus by taking $$\ell_{i,r}$$ sufficiently large, we can make all the $$p_{\ell_{i,r}}^{(r)}$$ for $$\ell = \ell_{i,r}$$ or $$\ell \in \mathcal{L}$$ or $$\ell \in V_{i,r}$$ have norm greater than $$2^i$$. Thus the sequence is well-defined.

Each $$\ell_{i,r}$$ can be computed by searching primes in increasing order until one is found satisfying the conditions: conditions (1) – (4) can be verified effectively by Lemma 6.1, and condition (5) can be tested effectively, since $$|x_{\ell_{i,r}-1}|_v$$ is an algebraic real number. □

We now define the following subsets of $$P_K$$:

- $$T_{i,r} = \bigcup_{i \geq 1} S_{\ell_{i,r}}, r = 1, \ldots, t;$$
Lemma 6.3.

(1) For each \( r = 1, \ldots, t \), the sets \( T_{1,r} \) and \( T_{2,r} \) are disjoint. If a subset \( S_r \subset \mathcal{P}_K \) contains \( T_{1,r} \) and is disjoint from \( T_{2,r} \), then \( E_r := \hat{E}(\mathcal{O}_{K,S_r}) \cap zE(K) \) is the union of
\[
\{ \pm \ell_{i,r}P : i \geq 1 \}
\]
and some subset of the finite set \( \{ sP : s \mid \prod_{\ell \in \mathcal{L}} \ell^{a_{\ell-1}} \} \).

(2) For any \( j \in \{1, 2\} \) and \( r, s \in \{1, \ldots, t\} \) such that \( r \neq s \) the sets \( T_{j,r} \) and \( T_{j,s} \) are disjoint.

(3) For any \( k \in \{1, 2\} \) and \( r \in \{1, \ldots, t\} \) the set \( T_{k,r} \) is computable.

Proof.

(1) The proof of this assertion is the same as the proof of Lemma 3.10 of [16]. The proof is not affected by the fact that we do not invert primes in \( S_{\text{bad}} \), since in our case \( S_1 = \emptyset \) also.

(2) First we assume that \( j = 1 \). In this case
\[
T_{1,r} \cap T_{1,s} = \left( \bigcup_{i \geq 1} S_{\ell_{i,r}} \right) \cap \left( \bigcup_{i \geq 1} S_{\ell_{i,s}} \right) = \emptyset
\]
since for any \( r \neq s \) we have that \( S_{\ell_{1,r}} \cap S_{\ell_{2,s}} = S(\ell_{1,r}, \ell_{i_2,s}) = \emptyset \) as \( \{\ell_{i,r}\} \cap \{\ell_{i,s}\} = \emptyset \).

Next let \( j = 2 \) and consider \( T_{2,r} \cap T_{2,s} \). Since the set \( T_{2,r} \) consists of the \( r \)-th largest primitive prime divisors of certain terms in the divisibility sequence \( v_n \), and \( T_{2,s} \) consists of the \( s \)-th largest primitive prime divisors of terms in the divisibility sequence, the definition of being a primitive divisor immediately implies that these sets can never have any nontrivial intersection when \( r \neq s \).

(3) This assertion follows directly from the fact that each sequence
\[
\{\ell_{1,r}, \ell_{2,r}, \ldots\}, 1 \leq r \leq t
\]
is computable and from Lemma 6.1.

\[ \square \]

Proposition 6.4. The natural density of \( T_{1,r} \) and \( T_{2,r} \) (1 \( \leq r \leq t \)) is zero.

Proof. The proofs that \( T_{1,r}, T_{2,r}^b, \) and \( T_{2,r}^c \) have density 0 are identical to the proofs in Section 9 of [15]. The fact that \( T_{2,r}^a \) has density 0 follows from Proposition 5.1. \[ \square \]

Now we can construct infinite Diophantine subsets \( A_r \) of \( \mathcal{O}_{K,S_r} \) that are discrete in any topology of \( K \). We first need the following lemma.

Lemma 6.5. For each \( v \in \mathcal{M}_K \) and \( 1 \leq r \leq t \) the sequence \( \ell_{1,r}P, \ell_{2,r}P, \ldots \) converges in \( E(K_v) \) to \( P \).
Proof. This is Lemma 3.14 in [16].

We now have the following proposition.

**Proposition 6.6.** Let \( S_r \) be as in Lemma 6.3 and let \( A_r := \{ x_{\ell_1,r}, x_{\ell_2,r}, \ldots \} \). Then \( A_r \) is a Diophantine subset of \( \mathcal{O}_{K,S_r} \). For any \( v \in M_K \), the set \( A_r \) is discrete when viewed as a subset of \( K_v \).

**Proof.** By Lemma 6.5, the elements of \( A_r \) form a convergent sequence in \( K_v \) whose limit \( x_1 \) is not in \( A_r \). Hence \( A_r \) is discrete. By Lemma 6.3, part (1), \( x(\mathcal{E}_r) \) is the union of the set \( A_r \) and a finite set. Since \( \mathcal{E}_r \) is Diophantine over \( \mathcal{O}_{K,S_r} \), the set \( A_r \) is Diophantine over \( \mathcal{O}_{K,S_r} \) as well. \( \square \)

In Section 8 we will use the sets \( A_1, \ldots, A_t \) together with sets \( T_{i,1}, \ldots, T_{i,t} \) and \( T_{2,1}, \ldots, T_{2,t} \) to prove Theorem 1.7.

### 7. Constructing Diophantine Models of \( \mathbb{Z} \).

We will now modify the \( t \) sequences of primes constructed above so that in the resulting big rings Hilbert's Tenth Problem is undecidable.

Fix two primes \( p, q \in \mathcal{P}_K \) of degree 1 that are primes of good reduction for \( E_r \), and such that \( p \) and \( q \) do not ramify in \( K/\mathbb{Q} \). Choose \( p, q \) such that neither \( p \) nor \( q \) divides \( y_1 = y(P) \), and such that the underlying primes \( p, q \in \mathcal{P}_Q \) are distinct and odd. Let \( M = pq \# E(F_p) \# E(F_q) \).

We now define \( t \) sequences of primes \( \{ \ell_{i,r} \}, r = 1, \ldots, t \) by using sets \( V_{i,r}, i \in \mathbb{Z}_{>0}, r = 1, \ldots, t \) of previously defined elements of the sequences. More specifically we let \( V_{1,1} = \emptyset \). For \( i > 1 \) we set

\[
V_{i,1} = \{ \ell_{1,1}, \ldots, \ell_{1,t}, \ldots, \ell_{i-1,1}, \ldots, \ell_{i-1,t} \},
\]

and for \( i \geq 1, 1 < r \leq t \), we set

\[
V_{i,r} = \{ \ell_{1,1}, \ldots, \ell_{1,t}, \ldots, \ell_{i,1}, \ldots, \ell_{i,r-1} \}.
\]

Now let \( \ell_{i,r} \) be the smallest prime outside \( \mathcal{L} \) and exceeding the bound implicit in Theorem 3.2 such that all of the following hold:

1. \( \ell_{i,r} > \ell \) for all \( \ell \in V_{i,r} \),
2. \( \mu_{\ell_{i,r}} \leq 2^{-i} \),
3. \( N_{\ell_{i,r}}^{(r)} > 2^i \) for all \( \ell \in V_{i,r} \cup \{ \ell_{i,r} \} \cup \mathcal{L} \),
4. \( \ell_{i,r} \equiv 1 \pmod{M} \),
5. the highest power of \( p \) dividing \( (\ell_{i,r} - 1)/M \) is \( p^i \), and
6. \( q \) divides \( (\ell_{i,r} - 1)/M \) if and only if \( i \in B \).

By Proposition 3.19 in [16] and by Proposition 6.1 we have:

**Proposition 7.1.** The sequences \( \{ \ell_{1,r}, \ell_{2,r} \ldots \} \), \( r = 1, \ldots, t \), are well-defined and computable.

**Lemma 7.2.** If \( m \in \mathbb{Z}_{\geq 1} \), then

\[
\text{ord}_p(x_{mM+1} - x_1) = \text{ord}_p(x_{M+1} - x_1) + \text{ord}_p m.
\]

**Proof.** This is Lemma 3.20 in [16]. \( \square \)

We define the following subsets of \( \mathcal{P}_K \):

Proposition 7.4. The natural density of $x$ by Lemma 7.2 (with $Z$)

Theorem 7.6. Let $\mathcal{S}$ be as in Lemma 7.3 and let $A_r := \{x_{\ell_{i,r}}, x_{\ell_{2,r}}, \ldots \}$. Then $A_r$ is a Diophantine model of $\mathcal{S}$ over $O_{K,S_r}$, via the bijection $\phi: \mathbb{Z}_{\geq 1} \rightarrow A$ taking $i$ to $x_{\ell_{i,r}}$.

Proof. The set $A_r$ is Diophantine over $O_{K,S_r}$ by part (1) of Lemma 7.3.

We have

$$i \in B \iff q \divides (\ell_{i,r} - 1)/M$$

(by condition (4))

$$\iff \ord_{q}(x_{\ell_{i,r}} - x_1) > \ord_{q}(x_{M+1} - x_1)$$

by Lemma 7.2 (with $q$ in place of $p$). The latter inequality is a Diophantine condition on $x_{\ell_{i,r}}$. Thus the subset $\phi(B)$ of $A_r$ is Diophantine over $O_{K,S_r}$.

Finally, for $i \in \mathbb{Z}_{\geq 1}$, Lemma 7.2 and condition (3) imply $\ord_{p}(x_{\ell_{i,r}} - x_1) = c + i$, where the integer $c = \ord_{p}(x_{M+1} - x_1)$ is independent of $i$. Therefore, for $i, j, k \in \mathbb{Z}_{\geq 1}$, we have

$$i + j = k \iff \ord_{p}(x_{\ell_{i,r}} - x_1) + \ord_{p}(x_{\ell_{j,r}} - x_1) = \ord_{p}(x_{\ell_{k,r}} - x_1) + c.$$

It follows that the graph of $+$ corresponds under $\phi$ to a subset of $A_r^3$ that is Diophantine over $O_{K,S_r}$.

Thus $A_r$ is a Diophantine model of $Z$ over $O_{K,S_r}$. \qed
8. Complementary Rings

In this section we complete the proofs of Theorems 1.7 and 1.8. First we need a general result about the existence of sets of primes of given densities. The result we will prove is contained in Proposition 8.9 below.

8.1. Sets of primes with prescribed densities. We start with describing the real numbers we consider as possible densities of our sets.

Definition 8.1 (Computable Real Numbers). A real number $\delta$ is called computable if there exists a computable sequence of rational numbers $r_n \in \mathbb{Q}$ such that

$$\lim_{n \to \infty} r_n = \delta.$$ 

It is easy to see that if $\alpha, \beta \neq 0$ are computable real numbers, then so is $\alpha/\beta$. Next we observe that these are the only densities we should consider in the context of our problem.

Proposition 8.2. Let $K$ be a number field and let $W_K$ be a recursive set of primes of $K$ having a natural density $\delta$. In this case $\delta$ is a computable real number.

Proof. Given our definition of a computable set $A$ of primes of a number field $K$ (see Section 2), there exists a recursive procedure determining the size of the set $\{p \in A : Np \leq n\}$ uniformly in $n$, and therefore there exists a recursive function $g(n)$ computing $r_n = \frac{\#\{p \in A : Np \leq n\}}{\#\{p \in P_K : Np \leq n\}}$. If $\delta$ is the natural density of $A$, then $\lim_{n \to \infty} r_n = \delta$ and therefore $\delta$ must be a computable real number.

We will now describe an (effective) procedure which, given a computable positive real number $\delta$ and a computable set of primes $Z_K$ of a number field $K$ of natural density $\gamma \geq \delta$, constructs a computable set of primes $A_K \subseteq Z_K$ of natural density $\delta$.

Without loss of generality we may assume that $\gamma > \delta$. Otherwise we set $A_K = Z_K$. Since $Z_K$ is computable, Proposition 8.2 implies that $\gamma$ is computable. Let $\{d_i\}, \{g_i\}$ be computable sequences of rational numbers approximating $\delta$ and $\gamma$ respectively. Without loss of generality we can assume that $g_i \neq 0$ for all $i \in \mathbb{Z}_{>0}$. Then $\{r_i\} = \{d_i/g_i\}$ is a computable sequence of rational numbers approximating $\alpha := \delta/\gamma$. Without loss of generality we may also assume that all elements of the sequence $\{r_n\}$ are positive and strictly less than one.

Let $\{N_i\}$ be an increasing sequence of positive integers such that each $N_i = Np_K$ for some prime $p_K$ of $K$ in $Z_K$. Assume also that every positive integer $M \geq N_i$ occurring as a norm of a $K$-prime from $Z_K$ is an element of the sequence. Let $n = [K : \mathbb{Q}]$ and notice that $n$ is the maximum number of $K$-primes that can have the same norm.

We now define recursively two sequences of sets of primes $\{A_i\}$ and $\{Z_i\}$. We denote by $a_i$ and $z_i$ the cardinality of $|A_i|$ and $|Z_i|$, respectively (for $i \geq 1$). Recall that $\{r_i\}$ is the sequence of rational numbers (strictly less than one) approximating $\alpha = \delta/\gamma$.

1. Set $A_1 = Z_1 = \{p \in Z_K : Np = N_1\}$.
2. If $\frac{a_i}{z_i} < r_i$, then set $A_{i+1} = A_i \cup \{p \in Z_K : Np = N_{i+1}\}$. Otherwise, set $A_{i+1} = A_i$.
3. For all $i \in \mathbb{Z}_{>0}$ set

$$Z_{i+1} = \{p \in Z_K : N_1 \leq Np \leq N_{i+1}\}.$$
We have $Z_K = \bigcup_{i \in \mathbb{Z}_{>0}} Z_i$. We will now prove that the set $A_K := \bigcup_{i \in \mathbb{Z}_{>0}} A_i$ has density $\delta$. To do this we need several lemmas. It is clear from the construction that $A_K$ is a computable set of primes.

**Lemma 8.3.**

1. If $\frac{a_i}{z_i} \geq r_i$ for some index $i$, then there is a positive integer $k$ such that $\frac{a_{i+k}}{z_{i+k}} < r_i$.

2. If $\frac{a_i}{z_i} < r_i$ for some index $i$, then $\frac{a_{i+k}}{z_{i+k}} \geq r_i$ for some positive integer $k$.

**Proof.** The proofs for both assertions of the lemma will proceed by contradiction. Assume that the first assertion is false, i.e. assume that there exists an $i \in \mathbb{Z}_{>0}$ such that $\frac{a_i}{z_i} \geq r_i$ and for all $k \in \mathbb{Z}_{>0}$ we have $\frac{a_{i+k}}{z_{i+k}} \geq r_{i+k}$. By step (2) in the above construction, the last inequality implies that $A_{i+k} = A_i$ and $a_{i+k} = a_i$ for all $k \in \mathbb{Z}_{>0}$. However, $\lim_{k \to \infty} z_{i+k} = \infty$ and therefore $\lim_{k \to \infty} \frac{a_{i+k}}{z_{i+k}} = 0$, while $\lim_{k \to \infty} r_{i+k} > 0$, which is a contradiction. Hence the first assertion of the lemma is true.

Assume now that the second assertion of the lemma is false, i.e. that there exists an $i \in \mathbb{Z}_{>0}$ such that $\frac{a_i}{z_i} < r_i$ and such that

$$\forall k \in \mathbb{Z}_{>0} \quad \frac{a_{i+k}}{z_{i+k}} < r_{i+k}.$$  

(8.1)

By step (2) of the above construction, (8.1) implies that

$$\forall k \in \mathbb{Z}_{>0} \ A_{i+k} = A_{i+k-1} \cup \{p \in Z_K : Np = N_{i+1}\}.$$  

This implies that $a_{i+k} \geq z_{i+k} - c$ for all $k \in \mathbb{Z}_{>0}$ for some fixed nonnegative integer $c$. At the same time, since the $r_j$'s are less than 1, (8.1) implies that $z_{i+k} > a_{i+k}$ for all $k \in \mathbb{Z}_{>0}$. Thus

$$\lim_{k \to \infty} \frac{a_{i+k}}{z_{i+k}} = \lim_{k \to \infty} \frac{z_{i+k}}{z_{i+k}} = 1 > \alpha = \lim_{k \to \infty} r_{i+k},$$

and therefore (8.1) cannot hold. \hfill $\square$

We now define two sequences of positive integers that we will use below.

**Notation 8.4.**

- Let $j_1 = 1$ and for $i \in \mathbb{Z}_{>1}$ define $j_i$ to be the smallest positive integer greater than $j_{i-1}$ such that $\frac{a_{j_i}}{z_{j_i}} < \frac{a_{j_{i-1}}}{z_{j_{i-1}}}$ (In other words, $\frac{a_{j_i}}{z_{j_i}}$ is a “local maximum”.)

- Let $k_0 = 0$ and for $i \in \mathbb{Z}_{>0}$ define $k_i$ to be the smallest positive integer greater than $k_{i-1}$ such that $\frac{a_{k_{i+1}}}{z_{k_{i+1}}} > \frac{a_{k_i}}{z_{k_i}}$ (In other words, $\frac{a_{k_i}}{z_{k_i}}$ is a “local minimum”.)

**Remark 8.5.** By construction of the sets $A_i$, $Z_i$ we have $z_i > a_i$ for all $i > 1$. Hence if $A_i \not\subseteq A_{i+1}$, then $\frac{a_{i+1}}{z_{i+1}} = \frac{a_{i+m}}{z_{i+m}} > \frac{a_i}{z_i}$, where $m$ is the number of primes of norm $N_{i+1}$ in $Z_K$. On the other hand, if $A_i = A_{i+1}$ then $\frac{a_{i+1}}{z_{i+1}} = \frac{a_i}{z_i}$. From Lemma 8.3 we can conclude that both $j_i$ and $k_i$ are defined for all $i \in \mathbb{Z}_{>0}$.

By construction of the sets $A_i$, we have $\frac{a_{j_{i-1}}}{z_{j_{i-1}}} < r_{j_{i-1}}$ and $\frac{a_{j_i}}{z_{j_i}} \geq r_{j_i}$ for all $i > 1$. Similarly, we have $\frac{a_{k_{i-1}}}{z_{k_{i-1}}} ≥ r_{k_{i-1}}$ and $\frac{a_{k_i}}{z_{k_i}} < r_{k_i}$ for all $i > 0$.

We now show some properties of the sequences $\{k_i\}$ and $\{j_i\}$. 

Lemma 8.6.

1. For all \(i \in \mathbb{Z}_{\geq 0}\) we have \(k_i < j_{i+1} < k_{i+1}\).
2. For all \(\ell \in \mathbb{Z}_{> 0}\) there exists \(i \in \mathbb{Z}_{> 0}\) such that either
   \[
   j_i \leq \ell \leq k_i \quad \text{and} \quad \frac{a_i}{z_{j_i}} \geq \frac{a_\ell}{z_\ell} \geq \frac{a_{k_i}}{z_{k_i}}
   \]
   or
   \[
   k_i \leq \ell \leq j_{i+1} \quad \text{and} \quad \frac{a_{k_i}}{z_{k_i}} \leq \frac{a_\ell}{z_\ell} \leq \frac{a_{j_{i+1}}}{z_{j_{i+1}}}.
   \]

Proof. By Lemma 8.3 and Remark 8.5, maxima and minima alternate in the sequence \(\{a_i/r_i\}\). Further, by definition of \(A_1 = \mathbb{Z}_1\), it is clear that \(j_1 = 1\) produces a local maximum in the sequence. \(\square\)

We now show that the local maxima and minima converge to \(\alpha = \delta/\gamma = \lim_{i \to \infty} r_i\).

Lemma 8.7. \(\lim_{i \to -\infty} \frac{a_i}{z_{j_i}} = \alpha\) and \(\lim_{i \to \infty} \frac{a_{k_i}}{z_{k_i}} = \alpha\).

Proof. We show that for any \(\varepsilon > 0\) there exists a positive integer \(M\) such that for \(i > M\) we have that \(|\alpha - \frac{a_i}{z_{j_i}}| < \varepsilon\). The proof of the analogous statement with \(k_i\) substituted for \(j_i\) is similar. Fix \(\mu < \varepsilon/4\). Let \(I \in \mathbb{Z}_{> 0}\) be large enough so that for all integers \(s > I\) we have \(|r_s - \alpha| < \mu < \varepsilon/4\) and \(z_s > \frac{4n(1-\alpha)}{\varepsilon}\). (Recall that \(n = [K : \mathbb{Q}]\).) Fix a positive integer \(s > I\) and pick an \(i\) such that \(j_i > s + 1\). By Remark 8.5

\[
(8.2) \quad \frac{a_j}{z_{j_i}} = \frac{a_{j_i-1} + m}{z_{j_i-1} + m} \geq r_{j_i} > \alpha - \mu,
\]

where as above, \(m\) is the number of \(K\)-primes in \(\mathbb{Z}_K\) with \(K\)-norm equal to \(N_{j_i}\). By Remark 8.5 we also have \(\frac{a_{j_i-1}}{z_{j_i-1}} < r_{j_i-1} < \alpha + \mu\). Thus

\[
(8.3) \quad \frac{a_{j_i}}{z_{j_i}} - \alpha = \frac{a_{j_i} - a_{j_i-1}}{z_{j_i}} + \frac{a_{j_i-1}}{z_{j_i-1}} - \alpha = \frac{a_{j_i} - a_{j_i-1} - m}{z_{j_i}} + \frac{a_{j_i-1}}{z_{j_i-1}} - \alpha = \frac{a_{j_i-1}}{z_{j_i-1}} + \frac{m(z_{j_i-1} - a_{j_i-1})}{(z_{j_i-1} + m)z_{j_i-1}} - \alpha = \frac{m(1 - a_{j_i-1}/z_{j_i-1})}{z_{j_i-1}} + \frac{a_{j_i-1}}{z_{j_i-1}} - \alpha < \frac{m(1 - \alpha + \mu)}{z_{j_i-1}} + \mu \leq \frac{n(1 - \alpha + \mu)}{z_{j_i-1}} + \mu < \varepsilon.
\]

Combining (8.2) and (8.3)–(8.7) we conclude that

\[
\left| \frac{a_{j_i}}{z_{j_i}} - \alpha \right| < \varepsilon.
\]

Now we can prove that the natural density of \(A_K\) is \(\delta\). \(\square\)
Corollary 8.8. The natural density of $A_K$ is $\delta$, i.e.

$$\lim_{X \to \infty} \frac{\#\{p_K \in A_K, Np_K \leq X\}}{\#\{p_K \in \mathcal{P}_K, Np_K \leq X\}} = \delta.$$  

Proof. From Lemma 8.6 and Lemma 8.7 it follows that $\lim_{i \to \infty} \frac{a_i}{z_i} = \alpha$. Now let $X$ be a positive real number greater than $N_i$. Then

$$N_i \leq X \leq N_{i+1}$$

for some positive integer $i$. (Recall that the $N_i$’s are norms of primes of $K$ that appeared in the construction of the set $A_K$.) Since $a_i$ and $z_i$ were defined to be the cardinality of $A_i$ and $Z_i$, respectively, we have

$$\#\{p_K \in A_K, Np_K \leq X\} = a_i,$$  

$$\#\{p_K \in Z_K, Np_K \leq X\} = z_i.$$  

This implies that $\lim_{X \to \infty} \frac{\#\{p_K \in A_K, Np_K \leq X\}}{\#\{p_K \in Z_K, Np_K \leq X\}} = \lim_{i \to \infty} \frac{a_i}{z_i} = \alpha$.

The statement of the corollary now follows from the fact that

$$\lim_{X \to \infty} \frac{\#\{p_K \in A_K, Np_K \leq X\}}{\#\{p_K \in \mathcal{P}_K, Np_K \leq X\}} = \lim_{X \to \infty} \left( \frac{\#\{p_K \in A_K, Np_K \leq X\}}{\#\{p_K \in \mathcal{P}_K, Np_K \leq X\}} \cdot \frac{\#\{p_K \in Z_K, Np_K \leq X\}}{\#\{p_K \in Z_K, Np_K \leq X\}} \right) = \lim_{X \to \infty} \frac{\#\{p_K \in Z_K, Np_K \leq X\}}{\#\{p_K \in \mathcal{P}_K, Np_K \leq X\}} = \alpha \gamma = \delta$$

Finally we have the following proposition.

Proposition 8.9. If $\delta_1, \ldots, \delta_t$ is a finite set of nonnegative computable real numbers adding up to one, then there exist a partition of $\mathcal{P}_K$ into computable sets $W_1, \ldots, W_t$ of densities $\delta_1, \ldots, \delta_t$, respectively.

Proof. Without loss of generality we can assume that all the densities are positive. We proceed in $t-1$ steps. First set $Z_K = \mathcal{P}_K$ and construct a computable set $W_1$ of density $\delta_1$. Observe that $\mathcal{P}_K - W_1$ is computable of density $1 - \delta_1 \geq \delta_2$. Now set $Z_K = \mathcal{P}_K - W_1$ and construct $W_2, W_3, \text{etc.}$

Remark 8.10. The construction above shows in fact that there exists a partition of $\mathcal{P}_K$ into sets of any densities adding to 1. However, if we do not require that the densities are computable, the resulting sets of primes may be uncomputable.

Now we can prove Theorems 1.7 and 1.8.

8.2. The proofs of Theorems 1.7 and 1.8. Let $\delta_1, \ldots, \delta_t$ be nonnegative computable real numbers adding up to one. Let $W_1, \ldots, W_t$ be a partition of primes of $K$, where the natural density of each $W_i$ is $\delta_i$. Such a partition exists by Proposition 8.9. For the case of Theorem
1.7, let \( T_{1,r}, T_{2,r}, r = 1, \ldots, t \) be as defined as in Section 6 and for the case of Theorem 1.8, let \( T_{1,r}, T_{2,r}, r = 1, \ldots, t \) be as defined as in Section 7. For \( i = 1, \ldots, t \) define

\[
S_i = (W_i \cup T_{1,i} \cup T_{2,j}) - (T_{2,i} \cup \bigcup_{r \neq i} T_{1,r}),
\]

where \( j \in \{1, \ldots, t\} \) is such that \( j \equiv i - 1 \mod t \). We claim the following:

1. The natural density of \( S_i \) exists and is equal to \( \delta_i \). This is true because by Propositions 5.1 and 6.4, for any \( i, j \) the natural density of \( T_{i,j} \) is 0.

2. Each \( S_i \) contains all the primes of \( T_{1,i} \) and omits the primes of \( T_{2,i} \). To see that this assertion is true, observe that we explicitly add \( T_{1,i} \) and remove \( T_{2,i} \), and by Propositions 6.3 and 7.3, we have that \( T_{2,i} \cap T_{2,j} = \emptyset \) for \( i \neq j \). Thus, adding \( T_{2,j} \) does not introduce any primes of \( T_{2,i} \) back. Further from the same propositions removing \( \bigcup_{r \neq i} T_{1,r} \) will not remove any primes of \( T_{1,i} \).

3. \( S_1, \ldots, S_t \) are a partition of \( \mathcal{P}_K \). First we show that \( S_i \cap S_r = \emptyset \) for \( i \neq r \). Since \( W_i \) and \( W_r \) are disjoint, the common elements can arise only from the primes which were added in, i.e. an intersection can arise from

\[
(T_{1,i} \cup T_{2,j}) \cap (T_{1,r} \cup T_{2,l}),
\]

where \( j \equiv i - 1 \mod t \), and \( l \equiv r - 1 \mod t \) so that \( l \neq j \). By construction, all the primes of \( T_{1,r} \) are removed from \( S_i \) and all the primes of \( T_{1,i} \) are removed from \( S_r \). Hence the only primes from (8.8) which can possibly be in \( S_i \cap S_r \) are in \( T_{2,i} \cap T_{2,j} \).

This intersection is empty, however, by Propositions 6.3 and 7.3. Finally we show that \( \bigcup_{i=1}^{t} S_i = \mathcal{P}_K \). As above we start with the fact that \( \bigcup_{i=1}^{t} W_i = \mathcal{P}_K \) and note that we only have to follow the primes removed from \( W_i \) in the process of constructing \( S_i \):

\[
T_{2,i} \cup \bigcup_{r \neq i} T_{1,r}.
\]

We have shown in Part 1 of this proposition that for \( r = 1, \ldots, t, T_{1,r} \subset S_r \) and therefore the primes in the union \( \bigcup_{r \neq i} T_{1,r} \) are accounted for. That leaves the primes of

\[
T_{2,i} - \bigcup_{r \neq i} T_{1,r} = T_{2,i} - \bigcup_{r=1}^{t} T_{1,r},
\]

where the equality holds because \( T_{1,i} \cap T_{2,i} = \emptyset \). When \( S_i \) is constructed, this set is moved to \( S_j, j \equiv i + 1 \mod t \) and observe that since \( T_{2,i} \cap T_{2,j} = \emptyset \), the primes of \( T_{2,i} - \bigcup_{r=1}^{t} T_{1,r} \) are not removed from \( S_j \).

**Acknowledgements**

Our thanks go to the London Mathematical Society for the very enjoyable visit by the third author to the University of East Anglia. Also, to whichever barman invented the Marguerita. We also thank Bjorn Poonen who suggested the use of sets of nonnegative computable real densities rather than rational densities.
REFERENCES


DEPARTMENT OF MATHEMATICS, THE PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802, USA.

*E-mail address*: eisentra@math.psu.edu

SCHOOL OF MATHEMATICS, UNIVERSITY OF EAST ANGLIA, NORWICH NR4 7TJ, UK.

*E-mail address*: g.everest@uea.ac.uk

DEPARTMENT OF MATHEMATICS, EAST CAROLINA UNIVERSITY, GREENVILLE, NC 27858, USA.

*E-mail address*: shlapentokha@ecu.edu