THE BULLETIN OF SYMBOLIC LOGIC
Volume 17, Number 2, June 2011

DEFINING INTEGERS

ALEXANDRA SHLAPENTOKH

Abstract. This paper surveys the recent developments in the area that grew out of attempts to solve an analog of Hilbert's Tenth Problem for the field of rational numbers and the rings of integers of number fields. It is based on a plenary talk the author gave at the annual North American meeting of ASL at the University of Notre Dame in May of 2009.

You can't always get what you want
You can't always get what you want
You can't always get what you want
But if you try sometimes you might find
You get what you need
Rolling Stones

§1. Prologue.

1.1. A question and the answer. The history of the problems discussed in this exposition goes back to a question that was posed by Hilbert in 1900: is there an algorithm which, given arbitrary polynomial equation in several variables over $\mathbb{Z}$, determines whether such an equation has solutions in $\mathbb{Z}$? (At the time Hilbert posed the question, a rigorous notion of the algorithm did not yet exist. So the version above is a modern interpretation of the question.) This question, being the tenth question on a list, became known as Hilbert's Tenth Problem (referred to as "HTP" in the future), and was answered negatively in the work of M. Davis, H. Putnam, J. Robinson and Yu. Matijasevich. (See [5], [6] and [13].) In fact, as we explain below, significantly more was shown: it was proved that recursively enumerable subsets of integers and Diophantine subsets of integers were the same. We define these sets below.

DEFINITION 1.1 (Recursive and recursively enumerable subsets of $\mathbb{Z}$). A set $A \subseteq \mathbb{Z}^m$ is called *recursive, computable or decidable* if there is an algorithm (or a computer program) to determine the membership in the set.

Received March 12, 2010.
2010 *Mathematics Subject Classification.* 11U03.
The author has been partially supported by NSF grant DMS-0650927 and by a grant from John Templeton Foundation.

1079-8986/11/1702-0002/$3.20

A set $A \subseteq \mathbb{Z}^m$ is called *recursively or computably enumerable* if there is an algorithm (or a computer program) to list the set.

The following theorem is a well-known result from Recursion Theory (see for example [26, §1.9]).

THEOREM 1.2. *There exist recursively enumerable sets which are not recursive.*

We now define Diophantine sets in a somewhat more general setting.

DEFINITION 1.3 (Diophantine sets: a number-theoretic definition). Let R be a commutative ring with identity. (All the rings considered below satisfy these assumptions.) A subset $A \subset R^m$ is called Diophantine over R if there exists a polynomial $p(T_1, \dots T_m, X_1, \dots, X_k)$ with coefficients in R such that for any element $(t_1, \dots, t_m) \in R^m$ we have that

$$\exists x_1, \dots, x_k \in \mathbb{Z}\colon\ p(t_1, \dots, t_m, x_1, \dots, x_k) = 0$$
$$\Updownarrow$$
$$(t_1, \dots, t_m) \in A.$$

In this case we call $p(T_1, \dots, T_m, X_1, \dots, X_k)$ a *Diophantine definition* of A over R.

Remark 1.4. Diophantine sets can also be described as the sets *existentially definable in* R in the language of rings or as *projections of algebraic sets*.

Given the MDRP result we immediately obtain the following important corollary.

COROLLARY 1.5. *There are undecidable Diophantine subsets of* $\mathbb{Z}$.

It is easy to see that the existence of undecidable Diophantine sets implies that no algorithm as requested by Hilbert exists. Indeed, suppose $A \subset \mathbb{Z}$ is an undecidable Diophantine set with a Diophantine definition $P(T, X_1, \dots, X_k)$. Assume also that we have an algorithm to determine the existence of integer solutions for polynomials. Now, let $a \in \mathbb{Z}$ and observe that $a \in A$ if and only if $P(a, X_1, \dots, X_K) = 0$ has solutions in $\mathbb{Z}^k$. So if we can answer Hilbert's question effectively, we can determine the membership in A effectively.

It is also not hard to see that Diophantine sets are recursively enumerable. Given a polynomial $p(T, \bar{X})$ we can effectively list all $t \in \mathbb{Z}$ such that $p(t, \bar{X}) = 0$ has a solution $\bar{x} \in \mathbb{Z}^k$ in the following fashion. Using a recursive listing of $\mathbb{Z}^{k+1}$, we can plug each $(k+1)$-tuple into $p(T, \bar{X})$ to see if the value is 0. Each time we get a zero we add the first element of the $(k+1)$-tuple to the t-list.

1.2. Some easy facts or getting better acquainted. A Diophantine set does not have to be complicated: one of the simplest Diophantine sets is the set of even integers

$$\{t \in \mathbb{Z} \mid \exists w \in \mathbb{Z} \colon t = 2w\}.$$

To construct more complicated examples we need to establish some properties of Diophantine sets.

LEMMA 1.6. *Intersections and unions of Diophantine sets over $\mathbb{Z}$ are Diophantine.*

PROOF. Suppose $P_1(T, \bar{X}), P_2(T, \bar{Y})$ are Diophantine definitions of subsets A_1 and A_2 of $\mathbb{Z}$ respectively over $\mathbb{Z}$. In this case

$$P_1(T, \bar{X})P_2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cup A_2$, and

$$P_1^2(T, \bar{X}) + P_2^2(T, \bar{Y})$$

is a Diophantine definition of $A_1 \cap A_2$. ⊣

The fact that over $\mathbb{Z}$ an intersection of Diophantine sets is Diophantine is related to another important aspect of Diophantine equations over $\mathbb{Z}$: a finite system of equations is always equivalent to a single equation in the sense that both the system and the equation have the same solutions over $\mathbb{Z}$ and in the sense that given a finite system of equations, the equivalent equation can be constructed effectively. We prove this assertion in the lemma below.

LEMMA 1.7 (Replacing finitely many by one over $\mathbb{Z}$). *Any finite system of equations over $\mathbb{Z}$ can be* effectively *replaced by a single polynomial equation over $\mathbb{Z}$ with the identical $\mathbb{Z}$-solution set.*

PROOF. Consider a system of equations

$$\begin{cases} g_1(x_1, \dots, x_k) = 0 \\ g_2(x_1, \dots, x_k) = 0 \\ \qquad \dots \\ g_m(x_1, \dots, x_k) = 0 \end{cases}$$

This system has solutions in $\mathbb{Z}$ if and only if the following equation has solutions in $\mathbb{Z}$:

$$g_1(x_1, \dots, x_k)^2 + g_2(x_1, \dots, x_k)^2 + \dots + g_m(x_1, \dots, x_k)^2 = 0. \qquad ⊣$$

In fact we can replace a finite system of polynomial equations by an equivalent single polynomial equation over any integral domain R whose fraction field is not algebraically closed.

LEMMA 1.8. (Replacing finitely many by one over an arbitrary integral domain). *Let R be any ring such that its fraction field K is not algebraically closed. In this case, any finite system of equations over R can be replaced by a single polynomial equation over R with the identical R-solution set.*

PROOF. It is enough to consider the case of two equations:

$$f(x_1,\dots,x_n) = 0 \text{ and } g(x_1,\dots,x_n) = 0.$$

If $h(x) = \sum_{i=0}^{k} a_i x^i$ is a polynomial over R without any roots in K, then the polynomial

$$\sum_{i=0}^{k} a_i f^i(x_1,\dots,x_n) g^{k-i}(x_1,\dots,x_n) = 0$$

has solutions in K if and only if $f(x_1,\dots,x_n) = 0$ and $g(x_1,\dots,x_n) = 0$ have a common solution in K. ⊣

Remark 1.9. If the ring in question is recursive, i.e., there exists an injective map from the ring into $\mathbb{Z}$ such that the image of the ring is recursive and the ring operations are translated by recursive functions (functions whose graphs are recursive sets), then there exists a recursive function which can take the coefficients of the system equations as its inputs and output the coefficients of the corresponding single equation with the same solution set over the ring. For all the rings we consider in this exposition the construction of such a function, which would depend on a construction of an irreducible polynomial over the fraction field, is fairly straightforward. However, in general, the situation can be a lot more complicated.

We can use this property of finite systems to give more latitude to our Diophantine definitions

COROLLARY 1.10. *We can let the Diophantine definitions over $\mathbb{Z}$ consist of several polynomials without changing the nature of the relation.*

One surprisingly useful tool for writing Diophantine definitions has to do with an elementary property of GCD's (greatest common divisors).

PROPOSITION 1.11. *If $a, b \in \mathbb{Z}_{\neq 0}$ with $(a, b) = 1$ then there exist $x, y \in \mathbb{Z}$ such that $ax + by = 1$.*

The GCD's can be used to show that the set of non-zero integers is Diophantine and thus allow us to require that values of variables are not equal, as well as to perform "division" as will be shown later. On a more theoretical level we can say that the *positive* existential theory of $\mathbb{Z}$ is the same as the existential theory of $\mathbb{Z}$.

PROPOSITION 1.12. *The set of non-zero integers has the following Diophantine definition over $\mathbb{Z}$:*

$$\{t \in \mathbb{Z} \mid \exists x, u, v \in \mathbb{Z} \colon (2u-1)(3v-1) = tx\}.$$

PROOF. If $t = 0$, then either $2u - 1 = 0$ or $3v - 1 = 0$ has a solution in $\mathbb{Z}$, which is impossible. Suppose now $t \neq 0$. Write $t = t_2 t_3$, where t_2 is odd and $t_3 \not\equiv 0 \mod 3$. Since $(t_2, 2) = 1$ and $(t_3, 3) = 1$, by a property of GCD there exist $u, x_u, v, x_v \in \mathbb{Z}$ such that

$$2u + t_2 x_u = 1 \quad \text{and} \quad 3v + t_3 x_v = 1.$$

Thus $(2u - 1)(3v - 1) = t_2 x_u t_3 x_v = t(x_u x_v)$. ⊣

Another important Diophantine definition allows us to convert inequalities into equations.

LEMMA 1.13 (Diophantine definition of the set of non-negative integers). *From Lagrange's Theorem we get the following representation of non-negative integers*:

$$\{t \in \mathbb{Z} \mid \exists x_1, x_2, x_3, x_4 \colon t = x_1^2 + x_2^2 + x_3^2 + x_4^2\}.$$

1.3. Becoming more ambitious. The questioned posed by Hilbert about the ring of integers can of course be asked about any recursive ring R: is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in R, can determine whether this equation has solutions in R? Arguably, the most prominent open questions in the area are the decidability of an analog of Hilbert's Tenth Problem for $R = \mathbb{Q}$ and R equal to the ring of integers of an arbitrary number field. The recent developments concerning these two problems are the main subjects of this exposition.

Before we proceed further with our discussion of HTP over $\mathbb{Q}$ we would like to point out that it is not hard to see that decidability of HTP over $\mathbb{Z}$ would imply decidability of HTP for $\mathbb{Q}$. Indeed, suppose we knew how to determine whether solutions existed over $\mathbb{Z}$. If $Q(x_1, \dots, x_k)$ is a polynomial with integer coefficients, then

$$\exists x_1, \dots, x_k \in \mathbb{Q} \colon Q(x_1, \dots, x_k) = 0$$

$$\Updownarrow$$

$$\exists y_1, \dots, y_k, z_1, \dots, z_k \in \mathbb{Z} \colon Q\left(\frac{y_1}{z_1}, \dots, \frac{y_k}{z_k}\right) = 0 \wedge z_1 \dots z_k \neq 0,$$

where we remind the reader we can rewrite $z_1 \dots z_k \neq 0$ as a polynomial equation and convert the resulting finite system of equations into a single one. So if we can determine whether the resulting equation had solutions over $\mathbb{Z}$, we can determine whether the original equation had solutions over $\mathbb{Q}$. Unfortunately, the reverse implication does not work: we don't know of any easy way to derive the undecidability of HTP over $\mathbb{Q}$ from the analogous result over integers. As a matter of fact, as we will see below we don't know of any way of deriving the undecidability of HTP over $\mathbb{Q}$ (we are not even sure the problem is undecidable over $\mathbb{Q}$).

One of the earliest methods suggested for showing that HTP was undecidable over $\mathbb{Q}$ used Diophantine definitions. This idea can be summarized in the following lemma:

LEMMA 1.14. *If $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over $\mathbb{Q}$, then HTP is not decidable over $\mathbb{Q}$.*

PROOF. Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$\begin{cases} h(T_1, \ldots, T_l) = 0 \\ p(T_1, \bar{X}_1) = 0 \\ \qquad \ldots \\ p(T_l, \bar{X}_l) = 0 \end{cases} \tag{1.1}$$

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z}$ if and only if system (1.1) has solutions in $\mathbb{Q}$. Thus if HTP is decidable over $\mathbb{Q}$, it is decidable over $\mathbb{Z}$. ⊣

Unfortunately, the Diophantine definition plan quickly ran into problems.

§2. Complications.

2.1. Some unpleasant thoughts. In 1992 Barry Mazur formulated a series of conjectures which were to play an important role in the development of the subject (see [14], [15], [16]). Before we state one of these conjectures, we need a definition.

DEFINITION 2.1 (Affine algebraic sets and varieties). If $\{p_1(x_1, \ldots, x_m), \ldots, p_k(x_1, \ldots, x_m)\}$ is a finite set of polynomial equations over some field K, then the set of common zeros of these polynomials in K^m is called an algebraic set. An algebraic set which is irreducible, i.e., is not a union of non-empty algebraic sets, is called a variety.

Mazur's conjectures on the topology of rational points is stated below:

CONJECTURE 2.2 (Topology of rational points). Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

This conjecture had an unpleasant consequence.

CONJECTURE 2.3. There is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Mazur's conjecture also refers to projective varieties, but it is the affine variety case which has the most consequences for HTP over $\mathbb{Q}$. We should also note that one can replace "variety" by "algebraic set" without changing the scope of the conjecture. (See Remark 11.1.2 of [32].) As a matter of fact, if Conjecture 2.2 is true, no infinite and discrete (in the archimedean topology) set has a Diophantine definition over $\mathbb{Q}$. The affine version of Mazur's conjecture can be thought of in the following manner. Suppose you are given a system of polynomial equations:

$$\begin{cases} P_1(x_1,\dots,x_k)=0\\ P_2(x_1,\dots,x_k)=0\\ \qquad\dots\\ P_m(x_1,\dots,x_k)=0\end{cases} \tag{2.2}$$

Think of solutions to this system as points in $\mathbb{R}^k$ but consider only the points whose coordinates are rational numbers. In other words we are interested in the set

$$RP = \{(x_1,\dots,x_k)\in\mathbb{Q}^k : (x_1,\dots,x_k) \text{ is a solution to system (2.2)}\}.$$

Now take the topological closure of RP in $\mathbb{R}^k$ (i.e., the points plus the "boundary"). Mazur's conjecture asserts that the resulting set will have finitely many "connected pieces" also known as connected components. It is the finite number of these components that precludes Diophantine definability of infinite discrete subsets.

2.2. Introducing new models. Since the plan to construct a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$ ran into substantial difficulties, alternative ways were considered for showing that HTP had no solution over $\mathbb{Q}$. One of the alternative methods required construction of a Diophantine model of $\mathbb{Z}$.

DEFINITION 2.4 (Diophantine model of $\mathbb{Z}$). Let R be a recursive ring whose fraction field is not algebraically closed and let $\phi\colon \mathbb{Z} \longrightarrow R^k$ be a recursive injection mapping Diophantine sets of $\mathbb{Z}$ to Diophantine sets of R^k. Then ϕ is called a Diophantine model of $\mathbb{Z}$ over R.

Remark 2.5 (An alternative terminology from model theory). Model theorist have an alternative terminology for a map described above. They would translate the statement that R has a Diophantine model of $\mathbb{Z}$ as $\mathbb{Z}$ being existentially definably interpretable in R. (See Chapter 1, Section 3 of [12].)

It is not hard to see that sending Diophantine sets to Diophantine sets makes the map automatically recursive. The recursiveness of the map follows from the fact that the ϕ-image of the graph of addition is Diophantine and therefore is recursively enumerable (by the same argument as over $\mathbb{Z}$). Thus, we have an effective listing of the set

$$D_+ = \{(\phi(m),\phi(n),\phi(m+n)), m,n\in\mathbb{Z}\}.$$

Assume we have computed $\phi(r-1)$ for some positive integer r. Now start listing D_+ until we come across a triple whose first two entries are $\phi(r-1)$ and $\phi(1)$. The third element of the triple must be $\phi(r)$. We can simplify the requirements for the map further.

PROPOSITION 2.6. *If R is a recursive ring and $\phi\colon \mathbb{Z}\longrightarrow R^k$ is injective for some $k\in\mathbb{Z}_{>0}$, then ϕ is a Diophantine model if and only if the images of the graphs of $\mathbb{Z}$-addition and $\mathbb{Z}$-multiplication are Diophantine over R.*

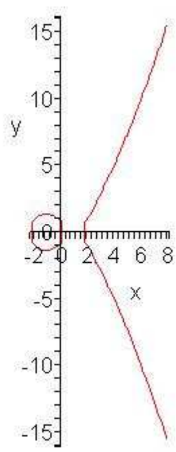

FIGURE 1.

This proposition can be proved by a straightforward induction argument which we do not reproduce here.

It quite easy to see that the following proposition holds.

PROPOSITION 2.7. *If R is a recursive ring with a Diophantine model of $\mathbb{Z}$, then HTP has no solution over R.*

PROOF. If R has a Diophantine model of $\mathbb{Z}$, then R has undecidable Diophantine sets, and the existence of undecidable Diophantine sets over R leads us to the undecidability of HTP over R in the same way as it happened over $\mathbb{Z}$. To show that R has undecidable Diophantine sets, let $A \subset \mathbb{Z}$ be an undecidable Diophantine set and suppose we want to determine whether an integer $n \in A$. Instead of answering this question directly we can ask whether $\phi(n) \in \phi(A)$. By assumption $\phi(n)$ is algorithmically computable. So if $\phi(A)$ is a computable subset of R, we have a contradiction. ⊣

It now follows that constructing a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ will solve our problem.

2.3. A steep curve. An old plan for building a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$ involved using elliptic curves. Consider an equation of the form:

$$y^2 = x^3 + ax + b, \tag{2.3}$$

where $a, b \in \mathbb{Q}$ and $\Delta = -16(4a^3 + 27b^2) \neq 0$. This equation defines an elliptic curve (a non-singular plane curve of genus 1). Figure 1 is the graph of such an elliptic curve $y^2 = x^3 - 2x + 1$ generated using Maple.

All the points $(x, y) \in \mathbb{Q}^2$ satisfying (2.3) (if any) together with O—the "point at infinity" form an abelian group, i.e., there is a way to define addition on the points of an elliptic curve with O serving as the identity. The group law on an elliptic curve can be represented geometrically (see for example [36, Chapter III, §3]). However, what is important to us is the algebraic representation of the group law. Let $P = (x_P, y_P), Q = (x_Q, y_Q), R = (x_R, y_R)$ be the points on an elliptic curve E with rational coordinates. If $P +_E Q = R$ and $P, Q, R \neq O$, then $x_R = f(x_P, y_P, x_Q, y_Q), y_R = g(x_P, y_P, x_Q, y_Q)$, where $f(z_1, z_2, z_3, z_4), g(z_1, z_2, z_3, z_4)$ are fixed (somewhat unpleasant looking) *rational functions*. Further, $-P = (x_P, -y_P)$. Mordell–Weill Theorem (see [36, Chapter III]) tells us that the abelian group formed by points of an elliptic curve over $\mathbb{Q}$ is finitely generated, meaning it has a finite rank and a finite torsion subgroup. It is also not very difficult to find elliptic curves whose rank is one. So let E be such an elliptic curve defined over $\mathbb{Q}$ such that $E(\mathbb{Q}) \cong \mathbb{Z}$ as abelian groups. (In other words $E(\mathbb{Q})$ has no torsion points. In practice torsion points are not an impediment, but they do complicate the discussion.) Let P_1 be a generator and consider a map sending an integer $n \neq 0$ to $[n]P = (x_n, y_n)$. (We should also take care of 0, but we will ignore this issue for the moment.) The group law assures us that under this map *the image of the graph of addition is Diophantine*. Unfortunately, it is not clear what happens to *the image of the graph of multiplication*. Nevertheless one might think that we have a starting point at least for our Diophantine model of $\mathbb{Z}$. Unfortunately, it turns out that situation with Diophantine models is not any better than with Diophantine definitions.

2.4. More bad news. A new piece of bad news came in the guise of a theorem of Cornelissen and Zahidi (see [3]).

THEOREM 2.8. *If Mazur's conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.*

This theorem left HTP over $\mathbb{Q}$ completely unapproachable. It is often the case that faced with intractable difficulties, mathematicians escape by changing the problem. Depending on one's point of view of the subject one could consider changing the problem in different ways: a number theorist might consider changing the object or possibly summon a big conjecture for assistance; a logician might reconsider the ban on all universal quantifiers. Perhaps one or two should be allowed back. As it turned out all these paths were explored. Below we describe these new problems starting with the ones which considered alternate objects.

§3. Big and small.

3.1. The rings between $\mathbb{Z}$ and $\mathbb{Q}$. The new objects which were introduced into the subject were the rings "in between" $\mathbb{Z}$ and $\mathbb{Q}$.

DEFINITION 3.1 (A ring in between). Let $\mathcal{S}$ be a set of primes of $\mathbb{Q}$. Let $O_{\mathbb{Q},\mathcal{S}}$ be the following subring of $\mathbb{Q}$.

$$\left\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is divisible by primes of } \mathcal{S} \text{ only}\right\}.$$

If $\mathcal{S} = \emptyset$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Z}$. If $\mathcal{S}$ contains all the primes of $\mathbb{Q}$, then $O_{\mathbb{Q},\mathcal{S}} = \mathbb{Q}$. If $\mathcal{S}$ is finite, we call the ring *small*. If $\mathcal{S}$ is infinite, we call the ring *large or big*, and if the natural density of $\mathcal{S}$ is equal to 1, we call the ring *very large or very big*.

Some of these rings have other (canonical) names: the small rings are also called rings of $\mathcal{S}$-integers, and when $\mathcal{S}$ contains all but finitely many primes, the rings are called semi-local subrings of $\mathbb{Q}$. The definition of very large rings uses the notion of natural density of a prime set stated below.

DEFINITION 3.2 (Natural density). If $\mathcal{A}$ is a set of primes, then the natural density of $\mathcal{A}$ is equal to the limit below (if it exists):

$$\lim_{X\to\infty} \frac{\#\{p \in A, p \leq X\}}{\#\{p \leq X\}}.$$

The big and small rings are not hard to construct.

EXAMPLE 3.3 (A small ring not equal to $\mathbb{Z}$).

$$\{\frac{m}{3^a 5^b} : m \in \mathbb{Z}, a, b \in \mathbb{Z}_{>0}\}.$$

EXAMPLE 3.4 (A big ring not equal to $\mathbb{Q}$).

$$\{\frac{m}{\prod p_i^{n_i}} : p_i \equiv 1 \mod 4, n_i \in \mathbb{Z}_{>0}\}.$$

Given a big or a small ring R we can now ask the following questions which were raised above with respect to $\mathbb{Q}$:

- Is HTP solvable over R?
- Do integers have a Diophantine definition over R?
- Is there a Diophantine model of integers over R?

While the answers to these questions are interesting on their own right, the hope (possibly unjustified) is that understanding the big rings will eventually lead us to $\mathbb{Q}$.

3.2. Diophantine properties of big and small rings. Before trying to answer the questions above, one should observe that the big and small rings share many Diophantine properties with the integers:

PROPOSITION 3.5. (1) *The set of non-zero elements of a big or a small ring is Diophantine over the ring.*
(2) *"One = finitely many" over big and small rings.*
(3) *The set of non-negative elements of a big or a small ring R is Diophantine over R: a small modification of the Lagrange argument is required to accommodate possible denominators*

$$\{t \in R \mid \exists x_1, x_2, x_3, x_4, x_5 \colon x_5^2 t = x_1^2 + x_2^2 + x_3^2 + x_4^2 \wedge x_5 \neq 0\}.$$

It turned out that we already knew everything we needed to know about small rings from the work of Julia Robinson (see [25]). In particular from her work on the first-order definability of integers over $\mathbb{Q}$ one can deduce the following theorem and corollary.

THEOREM 3.6 (Julia Robinson). *$\mathbb{Z}$ has a Diophantine definition over any small subring of $\mathbb{Q}$.*

COROLLARY 3.7. *HTP is unsolvable over all small subrings of $\mathbb{Q}$.*

Over large rings the questions turned out to be far more difficult.

§4. A different model.

4.1. Existential model of $\mathbb{Z}$ over a very large subring. In 2003 Poonen in [19] proved the first result on Diophantine undecidability (unsolvability of HTP) over a big subring of $\mathbb{Q}$.

THEOREM 4.1. *There exist recursive sets of primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of primes containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, the following hold:*

- *$\mathbb{Z}$ has a Diophantine model over $O_{\mathbb{Q},\mathcal{S}}$.*
- *Hilbert's Tenth Problem is undecidable over $O_{\mathbb{Q},\mathcal{S}}$.*

Poonen used elliptic curves to prove his result but the model he constructed was very different from the one envisioned by the old elliptic curve plan we described earlier. Poonen modeled integers *by approximation*. The construction of the model does start with an elliptic curve of rank one

$$E\colon y^2 = x^3 + ax + b \tag{4.4}$$

selected so that for a set of primes $\mathcal{S}$, except possibly for finitely many points, the only multiples of a generator P that have their affine coordinates in the ring $O_{\mathbb{Q},\mathcal{S}}$ are in the sequence $[\pm\ell_i]P = (x_{\ell_i}, \pm y_{\ell_i})$ with $|y_{\ell_j} - j| < 10^{-j}$. We remind the reader that we know how to define positive numbers using a variation on Lagrange's theme (Proposition 3.5) and how to get rid of a finite set of undesirable values such as points of finite order (just say "$\neq$" as in Proposition 3.5 again). We claim that $\phi\colon j \longrightarrow y_{\ell_j}$ is a Diophantine model of $\mathbb{Z}_{>0}$. In other words we claim that ϕ is an injection and the following sets are Diophantine:

$$D_+ = \{(y_{\ell_i}, y_{\ell_j}, y_{\ell_k}) \in D^3\colon k = i + j, k, i, j \in \mathbb{Z}_{>0}\}$$

and

$$D_2 = \{(y_{\ell_i}, y_{\ell_k}) \in D^2\colon k = i^2, i \in \mathbb{Z}_{>0}\}.$$

(Note that if D_+ and D_2 are Diophantine, then $D_\times = \{(y_{\ell_i}, y_{\ell_j}, y_{\ell_k}) \in D^3\colon k = ij, k, i, j \in \mathbb{Z}_{>0}\}$ is also Diophantine since $xy = \frac{1}{2}((x+y)^2 - x^2 - y^2)$.) It is easy to show that

$$k = i + j \Leftrightarrow |y_{\ell_i} + y_{\ell_j} - y_{\ell_k}| < 1/3.$$

and with the help of Lagrange this makes D_+ Diophantine. Similarly we have that

$$k = i^2 \Leftrightarrow |y_{\ell_i}^2 - y_{\ell_k}| < 2/5,$$

implying that D_2 is Diophantine.

To restrict the number of solutions to the elliptic curve equation, Poonen's construction relied to a large extent on the fact that the denominators of the coordinates of points on an elliptic curve which are multiples of a single point form a divisibility sequence: an integer sequence $\{a_n\}$ is called a divisibility sequence if $n \mid m$ implies $a_n \mid a_m$ (see Chapter 4 and Chapter 10 of [11] for a discussion of such sequences and see the discussion of the formal group of an elliptic curve in Chapter 4 of [36] for an explanation of why the denominators form a divisibility sequence). We now take a closer look at these denominators.

4.2. The denominators of points on an elliptic curve. Let E be an elliptic curve as in (4.4), fix a point of infinite order $P_1 = (x_1, y_1)$ on the curve and let $P_n = (x_n, y_n) = [n]P_1$ be the n-th multiple of P_1 for a non-zero integer n. In the notation above, using properties of elliptic curves one can show with various degrees of difficulty that the following statements are true:

- The same primes divide the (reduced) denominators of x_n and y_n, and therefore we can speak about primes dividing the "denominator" of P_n. (This follows from looking at the elliptic curve equation we use.)
- For all n sufficiently large in absolute value, it is the case that P_n has a *primitive divisor*, i.e., a prime dividing the "denominator" of P_n but not the "denominator" of any P_m with $|m| < |n|$. Denote the largest primitive divisor of P_n by p_n. We call p_n an *an indicator prime*. (This can be deduced from the rate of growth of denominators relative to the rate of growth of the exponents of the primes dividing the denominators.)
- $(\mathrm{denom}(x_n), \mathrm{denom}(x_m)) = \mathrm{denom}(x_{(m,n)})$ for sufficiently large $|m|$ and $|n|$ and therefore $\mathrm{denom}(x_m)$ divides $\mathrm{denom}(x_n)$ if and only if m divides n (again for sufficiently large $|m|$ and $|n|$). (This property uses the existence of primitive divisors as well as the fact that the denominators form a divisibility sequence.)
- Poonen showed that the set $\{p_\ell : \ell \text{ is a prime numer}\}$ has natural density equal to 0. (This density result was proved using some results of Serre and was probably the most technically challenging part of Poonen's paper.)

Now it is not hard to see that if p_ℓ is not allowed in the denominators of the elements of our big ring, then the coordinates of the point $[\ell]P_1 = (x_\ell, y_\ell)$ will not be solutions to the elliptic curve curve equation in our ring. Further, we will also exclude *all the multiples* of this point but will not affect the points whose indices are prime to ℓ. This is the principal mechanism for controlling which solutions to the elliptic curve equation appear in our ring.

In a 2009 paper (see [10]) Eisenträger and Everest extended Poonen's method to prove a theorem concerning sets of complementary primes. If $\mathcal{P}$ is the set of all primes of $\mathbb{Q}$, then two subsets $\mathcal{T}, \mathcal{S} \subset \mathcal{P}$ are exactly complementary if $\mathcal{S} \cup \mathcal{T} = \mathcal{P}$ and $\mathcal{S} \cap \mathcal{T} = \emptyset$. We state this theorem below.

THEOREM 4.2. *There are exactly complementary recursive sets* $\mathcal{S}, \mathcal{T} \subset \mathcal{P}$ *such that Hilbert's Tenth Problem is undecidable for both rings* $O_{\mathbb{Q},\mathcal{S}}$ *and* $O_{\mathbb{Q},\mathcal{T}}$.

§5. **Old dreams die hard.** So what about the old plan for modeling $\mathbb{Z}$ using indices of elliptic curve points? As it turns out the old plan can be resurrected but not exactly as intended. We remind the reader that the stumbling block for that plan was showing that the set $\{(x_n, y_n), (x_m, y_m), (x_{nm}, y_{nm})\}$ was Diophantine over $\mathbb{Q}$, where (x_n, y_n) are the affine coordinates of an n-th multiple of a generator of an elliptic curve of rank one over $\mathbb{Q}$. (See Section 2.3.) We manage to make this set Diophantine but only over some very big rings. To do this we modify Poonen's idea by not inverting *any* indicator primes p_ℓ. In this case no point of the elliptic curve has coordinates in our ring and we have to represent a point by a quadruple of numerators and denominators. While this is more awkward, we can derive some benefits.

5.1. Defining multiplication of indices. The main result pertaining to index multiplication is stated below.

THEOREM 5.1. *Let E be an elliptic curve defined and of rank one over $\mathbb{Q}$. Let P be a generator of $E(\mathbb{Q})$ modulo the torsion subgroup, and fix an affine (Weierstrass) equation for E of the form $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$. If (x_n, y_n) are the coordinates of $[n]P$ with $n \neq 0$ derived from this (Weierstrass) equation, then there exists a set of primes $\mathcal{W}$ of natural density one, and a positive integer m_0 such that the following set $\Pi \subset O^{12}_{\mathbb{Q},\mathcal{W}}$ is Diophantine over $O_{\mathbb{Q},\mathcal{W}}$.*

$$(U_1, U_2, U_3, X_1, X_2, X_3, V_1, V_2, V_3, Y_1, Y_2, Y_3) \in \Pi \Leftrightarrow$$
$$\exists \textit{ unique } k_1, k_2, k_3 \in \mathbb{Z}_{\neq 0} \textit{ such that}$$
$$\left(\frac{U_i}{V_i}, \frac{X_i}{Y_i}\right) = (x_{m_0 k_i}, y_{m_0 k_i}), \textit{ for } i = 1, 2, 3, \textit{ and } k_3 = k_1 k_2.$$

(See [35].)

We outline the proof under some simplifying assumptions. Let E as before be an elliptic curve of rank one defined over $\mathbb{Q}$ and let $E(\mathbb{Q})$ be the set of all the points of the curve with rational coordinates together with O—the point at infinity. For a generator P of $E(\mathbb{Q})$, for $n \in \mathbb{Z}_{\neq 0}$, we let $[n]P = (x_n, y_n) = (\frac{U_n}{V_n}, \frac{X_n}{Y_n}) \in \mathbb{Q}^2$, where $V_n > 0$, $Y_n > 0$, $(U_n, V_n) = 1$, $(X_n, Y_n) = 1$, $U_n, V_n, X_n, Y_n \in \mathbb{Z}$. (We are still using a (Weierstrass) equation of our elliptic curve of the form $y^2 = x^3 + ax + b$.) We assume that every non-trivial multiple of the generator P has an odd primitive divisor, i.e., for every $n \in \mathbb{Z}_{\neq 0,\pm 1}$ there exists a prime $p \neq 2$ such that $p \mid V_n$ but $p \nmid V_m$ for any m with $|m| < |n|$. We also assume that coordinates of P are integers. A point P_n will now be represented by a quadruple (A_n, B_n, C_n, D_n) of elements in our ring and this representation will not be unique because while it is possible to require that a numerator and the denominator are relatively prime in our big ring, big rings in general have infinitely many units and this will stand in a way of a unique representation of a point. In our big ring we do not invert the set

$$\mathcal{V} = \{\text{The largest odd primitive prime factor } p_{\ell^i} \text{ of } V_{\ell^i}\},$$

where ℓ runs through all the prime numbers and $i \in \mathbb{Z}_{>0}$. Not inverting these primes will ensure that $\text{denom}(x_m)$ divides $\text{denom}(x_n)$ if and only if m divides n. We invert *all the other primes*. In the resulting big ring we now have that

$$(V_m, V_n) = 1, (m, V_n), (n, V_m) = 1, V_m V_n \mid V_k \wedge V_k \mid V_m V_n \Longrightarrow |k| = |mn|.$$

More work is required to get rid of the absolute values and to remove the relative primeness condition, but that task can be accomplished with standard methods. Given that each point of the elliptic curve has infinitely many quadruples representing it we cannot construct a Diophantine model of $\mathbb{Z}$ (or show that $\mathbb{Z}$ is existentially definably interpretable in $O_{\mathbb{Q},\mathcal{W}}$) as above. What we can do is construct a class Diophantine model of $\mathbb{Z}$ defined below. (The corresponding model-theoretic notion is existential interpretability. Again see Chapter 1, Section 3 of [12].)

DEFINITION 5.2 (Class diophantine model). Let R be a countable recursive ring, let $D \subset R^k$, $k \in \mathbb{Z}_{>0}$ be a Diophantine subset, and let $\approx$ be a (Diophantine) equivalence relation on D, i.e., assume that the set $\{(\bar{x}, \bar{y}) \colon \bar{x}, \bar{y} \in D, \bar{x} \approx \bar{y}\}$ is a Diophantine subset of R^{2k}. Let $D = \bigcup_{i \in \mathbb{Z}} D_i$, where D_i is an equivalence class of $\approx$, and let $\phi \colon \mathbb{Z} \longrightarrow \{D_i, i \in \mathbb{Z}\}$ be defined by $\phi(i) = D_i$. Finally assume that the sets

$$\mathit{Plus} = \{(\bar{x}, \bar{y}, \bar{z}) \colon \bar{x} \in D_i, \bar{y} \in D_j, \bar{z} \in D_{i+j}\}$$

and

$$\mathit{Times} = \{(\bar{x}, \bar{y}, \bar{z}) \colon \bar{x} \in D_i, \bar{y} \in D_j, \bar{z} \in D_{ij}\}$$

are Diophantine over R. In this case we say that R has a *class* Diophantine model of $\mathbb{Z}$.

It is not hard to show that the rings with class Diophantine models of $\mathbb{Z}$ have undecidable Diophantine sets, just as the rings with Diophantine models of $\mathbb{Z}$. As as result of our ability to give a Diophantine definition of multiplication of indices we can construct a class Diophantine model of $\mathbb{Z}$

over a class of big subrings of $\mathbb{Q}$ not covered by the results of Poonen or Eisenträger and Everest.

COROLLARY 5.3. *In the notation above, for $n \neq 0$ let*

$$\phi(n) = [(U_{m_0n}, X_{m_0n}, V_{m_0n}, Y_{m_0n})],$$

the equivalence class of $(U_{m_0n}, X_{m_0n}, V_{m_0n}, Y_{m_0n})$ under the equivalence relation described below, where

$$U_{m_0n}, X_{m_0n}, V_{m_0n}, Y_{m_0n} \in O_{\mathbb{Q},\mathcal{S}},$$
$$V_{m_0n}Y_{m_0n} \neq 0,$$

and

$$(x_{m_0n}, y_{m_0n}) = \left(\frac{U_{m_0n}}{V_{m_0n}}, \frac{X_{m_0n}}{Y_{m_0n}}\right).$$

Let $\phi(0) = \{(0,0,0,0)\}$. Then ϕ is a class Diophantine model of $\mathbb{Z}$. (Here if $V\hat{V}\hat{Y}Y \neq 0$ we set $(U, X, V, Y) \approx (\hat{U}, \hat{X}, \hat{V}, \hat{Y})$ if and only if $\frac{\hat{U}}{\hat{V}} = \frac{U}{V}$ and $\frac{\hat{X}}{\hat{Y}} = \frac{X}{Y}$.)

We have now pretty much covered the state of existential affairs and it is time to return to the issue of lifting the ban on a few universal quantifiers. One could interpret this as a sign of surrender in the face of the overwhelming enemy (i.e., HTP for $\mathbb{Q}$), but we prefer a more optimistic interpretation: a gradual gathering of forces.

§6. Matters of the first order or back to the future. The result defining integers over $\mathbb{Q}$ using the "full force" of the first-order language is pretty old and belongs to Julia Robinson.

THEOREM 6.1 (Julia Robinson). *$\mathbb{Z}$ is first-order definable over $\mathbb{Q}$. (See [25].)*

Julia Robinson used quadratic forms and Hasse–Minkwoski Theorem to prove her theorem and in the process produced an existential definition over $\mathbb{Q}$ of the set

$$\text{Int}_q = \{x \in \mathbb{Q}\colon x = \frac{a}{b}, a, b \in \mathbb{Z}, b \not\equiv 0 \mod q\}$$

for any given prime q. It is this existential definition and the fact that we can "simulate" the denominators because we can define the set of non-zero elements of any small ring, that allowed us to conclude that $\mathbb{Z}$ was existentially definable over small rings.

In a 2007 paper Cornelissen and Zahidi analyzed Julia Robinson's formula and showed that it can be converted to a formula of the form $(\forall\exists\forall\exists)(F = 0)$ where the $\forall$-quantifiers run over a total of 8 variables, and where F is a polynomial. They also were the first ones to consider optimizing Julia Robinson's result using elliptic divisibility sequences:

THEOREM 6.2 (Cornelissen and Zahidi). *Assuming a (heuristically plausible) conjecture concerning denominators of points on elliptic curves over* $\mathbb{Q}$, *there exists a first-order model of* $\mathbb{Z}$ *over* $\mathbb{Q}$ *using just one universal quantifier.* (*See* [4].)

And so a conjecture makes its appearance to help push a result along, though not yet a famous conjecture.

In a 2007 paper (see [2]), using elliptic curves along the lines of Poonen's method and results of Julia Robinson, Cornelissen and the author showed that one could define $\mathbb{Z}$ over a large subring of $\mathbb{Q}$ using two universal quantifiers. Continuing further down this road, in 2008 Poonen in [22] produced an unconditional improvement of the first-order definition of integers over $\mathbb{Q}$ and over some big rings.

THEOREM 6.3.
- $\mathbb{Z}$ *is definable over* $\mathbb{Q}$ *using just two universal quantifiers in a* $\forall\exists$*-formula.*
- *For any* $\varepsilon > 0$, *there exists a set of rational primes* $\mathcal{W}_{\mathbb{Q}}$ *of natural density greater than* $1 - \varepsilon$ *such that* $\mathbb{Z}$ *is definable using just one quantifier in a* $\forall\exists$*-formula over* $O_{\mathbb{Q},\mathcal{W}_{\mathbb{Q}}}$.

Poonen used quadratic forms, quaternions and the Hasse Norm Principle. His definition of $\mathbb{Z}$ over $\mathbb{Q}$ is simple enough to be reproduced here: the set $\mathbb{Z}$ equals the set of $t \in \mathbb{Q}$ for which the following formula is true over $\mathbb{Q}$:

$$
\begin{aligned}
&(\forall a, b)(\exists a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, n):\\
&\quad (a + a_1^2 + a_2^2 + a_3^2 + a_4^2)(b + b_1^2 + b_2^2 + b_3^2 + b_4^2)\\
&\quad \cdot [(x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 - 1)^2 + (y_1^2 - ay_2^2 - by_3^2 + aby_4^2 - 1)^2\\
&\qquad\qquad + n^2 + (n-1)^2 \dots (n - 2309)^2 + (2x_1 + 2y_1 + n - t)^2] = 0
\end{aligned}
$$

Using existential definition of multiplication on indices one can also show the following.

THEOREM 6.4. *There exists a set* $\mathcal{W}$ *of primes of* $\mathbb{Q}$ *of natural density one such that* $\mathbb{Z}$ *is first-order definable over* $O_{\mathbb{Q},\mathcal{W}}$ *using just one universal quantifier in a* $\forall\exists$*-formula.* (*See* [35].)

Further the following result was announced by J. Koenigsmann in February 2009.

THEOREM 6.5. $\mathbb{Z}$ *is first-order definable over* $\mathbb{Q}$ *using just one* $\forall$*-quantifier in a* $\forall\exists$ *- formula.*

To summarize the discussion so far we can conceive of the following big definability project partly discussed already in Section 3.1.

QUESTION 6.6. For which big subrings of $\mathbb{Q}$ is the following true?

- $\mathbb{Z}$ is existentially definable.
- $\mathbb{Z}$ has an existential model.
- $\mathbb{Z}$ is definable using one universal quantifier.

Remark 6.7. If we start counting the number of quantifiers we use, definability results over the field will no longer automatically imply the analogous definability results for the subrings. Thus Koenigsman's result for $\mathbb{Q}$ does not automatically answer the question about the big subrings in general.

We now briefly consider the progress made on the other arguably most interesting problem in the area: the Diophantine (un)decidability of the rings of integers of number fields.

§7. Meanwhile in a galaxy not far away. We start with a review of some terms.

- A number field is a finite extension of $\mathbb{Q}$.
- A totally real number field is a number field all of whose embeddings into its algebraic closure are real.
- A ring of integers O_K of a number field K is the set of all elements of the number field satisfying monic irreducible polynomials over $\mathbb{Z}$ or alternatively the integral closure of $\mathbb{Z}$ in the number field.
- A prime of a number field K is a prime ideal of O_K. If $x \neq 0$ and $x \in O_K$, then for any prime $\mathfrak{p}$ of K there exists a non-negative integer m such that $x \in \mathfrak{p}^m$ but $x \notin \mathfrak{p}^{m+1}$. We call m the order of x at $\mathfrak{p}$ and write $m = \text{ord}_{\mathfrak{p}} x$. If $y \in K$ and $y \neq 0$, we write $y = \frac{x_1}{x_2}$, where $x_1, x_2 \in O_K$ with $x_1 x_2 \neq 0$, and define $\text{ord}_{\mathfrak{p}} y = \text{ord}_{\mathfrak{p}} x_1 - \text{ord}_{\mathfrak{p}} x_2$. This definition is not dependent on the choice of x_1 and x_2 which are of course not unique. We define $\text{ord}_{\mathfrak{p}} 0 = \infty$ for any prime $\mathfrak{p}$ of K.
- Any prime ideal $\mathfrak{p}$ of O_K is maximal and the residue classes of O_K modulo $\mathfrak{p}$ form a field. This field is always finite and its size (a power of a rational prime number) is call the norm of $\mathfrak{p}$ denoted by $\boldsymbol{N}\mathfrak{p}$.
- If $\mathcal{W}$ is a set of primes of K, its natural density is defined to be the following limit if it exists:
$$\lim_{X \to \infty} \frac{\#\{\mathfrak{p} \in \mathcal{W}, \boldsymbol{N}\mathfrak{p} \leq X\}}{\#\{\boldsymbol{N}\mathfrak{p} \leq X\}}.$$
- Let K be a number field and let $\mathcal{W}$ be a set of primes of K. Let $O_{K,\mathcal{W}}$ be the following subring of K.
$$\{x \in K : \text{ord}_{\mathfrak{p}} x \geq 0 \; \forall \mathfrak{p} \notin \mathcal{W}\}.$$
If $\mathcal{W} = \emptyset$, then $O_{K,\mathcal{W}} = O_K$—the ring of integers of K. If $\mathcal{W}$ contains all the primes of K, then $O_{K,\mathcal{W}} = K$. If $\mathcal{W}$ is finite, we call the ring *small* (or the ring of $\mathcal{W}$-integers). If $\mathcal{W}$ is infinite, we call the ring *large*, and if the natural density of $\mathcal{W}$ is one, we call the ring "very large". These rings are the counterparts of the "in between" subrings of $\mathbb{Q}$.

The state of knowledge concerning the rings of integers is summarized in the theorem below.

THEOREM 7.1. *$\mathbb{Z}$ is Diophantine and HTP is unsolvable over the rings of integers of the following fields*:

- *"Most" extensions of degree* 4 *of* $\mathbb{Q}$, *totally real number fields and their extensions of degree* 2. (*See* [7], [8].) *Note that these fields include all abelian extensions.*
- *Number fields with exactly one pair of non-real embeddings* (*See* [18] *and* [27].)
- *Any number field K such that there exists an elliptic curve E of positive rank defined over $\mathbb{Q}$ with* $[E(K)\colon E(\mathbb{Q})] < \infty$. (*See* [20], [33], [23].)
- *Any number field K such that there exists an elliptic curve of rank* 1 *over K and an abelian variety over $\mathbb{Q}$ keeping its rank over K.* (*See* [1].)

We also have several results concerning big rings in number fields. Note that in the big rings below we actually give a Diophantine definition of $\mathbb{Z}$.

THEOREM 7.2. *Let K be a number field satisfying one of the following conditions*:

- *K is a totally real field.*
- *K is an extension of degree* 2 *of a totally real field.*
- *There exists an elliptic curve E defined over $\mathbb{Q}$ such that* $[E(K)\colon E(\mathbb{Q})] < \infty$.

Let $\varepsilon > 0$ be given. Then there exists a set $\mathcal{S}$ of non-archimedean primes of K such that

- *The natural density of $\mathcal{S}$ is greater* $1 - \dfrac{1}{[K:\mathbb{Q}]} - \varepsilon$.
- *$\mathbb{Z}$ is Diophantine over $O_{K,\mathcal{S}}$.*
- *HTP is unsolvable over $O_{K,\mathcal{S}}$.*

(*See* [28], [29], [31], [33], [34].)

Over very large subrings, as was the case over $\mathbb{Q}$, we have Diophantine models of $\mathbb{Z}$ only. The first theorem is a number field version of Poonen's method for $\mathbb{Q}$. However the situation is more complicated over a number field and instead of constructing a model of $\mathbb{Z}$ by "approximation", what is constructed here is a model of a subset of the rational integers over which one can construct a model of $\mathbb{Z}$. In short, one constructs a "model of a model".

THEOREM 7.3. *Let K be a number field with a rank one elliptic curve. Then there exist recursive sets of K-primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of primes of K containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, $\mathbb{Z}$ has an existential model and Hilbert's Tenth Problem is unsolvable over $O_{K,\mathcal{S}}$.* (*See* [24].)

There is also a version of index multiplication over number fields. Here the strategy remains the same as over $\mathbb{Q}$.

THEOREM 7.4. *Let K be a number field. Let E be an elliptic curve defined and of rank one over K. Let P be a generator of $E(K)$ modulo the torsion subgroup,* *and fix an affine Weierstrass equation for E of the form $y^2 = x^3 + ax + b$, with $a, b \in O_K$. Let (x_n, y_n) be the coordinates of $[n]P$ with $n \neq 0$ derived from this Weierstrass equation. Then there exists a recursive set of K-primes $\mathcal{W}_K$ of natural density one, and a positive integer m_0 such that the following set $\Pi \subset O^{12}_{K,\mathcal{W}_K}$ is Diophantine over $O_{K,\mathcal{W}_K}$:*

$$(U_1, U_2, U_3, X_1, X_2, X_3, V_1, V_2, V_3, Y_1, Y_2, Y_3) \in \Pi \Leftrightarrow$$
$$\exists \text{ unique } k_1, k_2, k_3 \in \mathbb{Z}_{\neq 0} \text{ such that}$$
$$\left(\frac{U_i}{V_i}, \frac{X_i}{Y_i}\right) = (x_{m_0 k_i}, y_{m_0 k_i}), \text{ for } i = 1, 2, 3, \text{ and } k_3 = k_1 k_2,$$

$\mathbb{Z}$ has a class Diophantine model, and HTP is unsolvable over this ring.

See [35].

Theorems 7.1–7.4 have an elliptic curve assumption in their statements. These assumptions come in two flavors: an existence of a rank one elliptic curve over a field in question and an assumption concerning an elliptic curve of positive rank, not changing its rank in a finite extension. The rank one assumption is pretty straightforward but the "positive stable rank" assumption can be modified. It is not hard to show that it is enough to have a "positive stable rank" phenomenon for every cyclic extension of prime degree to obtain a Diophantine definition of $\mathbb{Z}$ over the ring of integers of any number field. The reduction takes place in several steps.

(1) Let K be a number field and let O_K be the ring of integers of K. Further, let M be the Galois closure of K over $\mathbb{Q}$ and let O_M be the ring of integers of M. Under these assumptions if $\mathbb{Z}$ has a Diophantine definition over O_M, then $\mathbb{Z}$ has a Diophantine definition over O_K. (Thus we can consider Galois extensions of $\mathbb{Q}$ only.)

(2) Let $M/\mathbb{Q}$ be a Galois extension of number fields with O_M the rings of integers of M respectively. Let $E_1, \dots, E_n$ be all the cyclic subextensions of M with $O_{E_1}, \dots, O_{E_n}$ the rings of integers of $E_1, \dots, E_n$ respectively. Observe that $\bigcap_{i=1}^n E_i = \mathbb{Q}$ and $\bigcap_{i=1}^n O_{E_i} = \mathbb{Z}$ and therefore if each O_{E_i} has a Diophantine definition over O_M, then $\mathbb{Z}$ has a Diophantine definition over O_M. (Thus, it is enough to show that in every cyclic extension the ring of integers below has a Diophantine definition over the ring of integers above.)

(3) If $E \subseteq H \subseteq M$ is a finite extension of number fields, O_H has a Diophantine definition over O_M, and O_E has a Diophantine definition over O_H, then O_E has a Diophantine definition over O_M. (Thus, it is enough to consider cyclic extensions of prime degree only.)

In the case of big rings the same kind of reductions also work, but an extra effort is required to make sure the sets of primes allowed in the denominators have the right density. For a general discussion of reductions of this sort see [30] and Chapter 2 of [32].

Unfortunately as of now we do not have unconditional results asserting the existence of required elliptic curves, but with a "little help" from this time a famous conjecture we do have the following recent result by Mazur and Rubin.

THEOREM 7.5. *Suppose L/K is a cyclic extension of prime degree of number fields. If the Shafarevich–Tate Conjecture is true for K, then there is an elliptic curve E over K with $rank(E(L)) = rank(E(K)) = 1$. (See* [17].)

As discussed above, this theorem has quite a few consequences.

COROLLARY 7.6. *If the Shafarevich–Tate Conjecture is true for all number fields, then the following statements are true.*

- *$\mathbb{Z}$ has a Diophantine definition over the ring of integers of any number field K.*
- *For any number field K and any $\varepsilon > 0$, there exists a set $\mathcal{S}$ of non-archimedean primes of K such that the natural density of $\mathcal{S}$ is greater $1 - \dfrac{1}{[K:\mathbb{Q}]} - \varepsilon$ and $\mathbb{Z}$ is Diophantine over $O_{K,\mathcal{S}}$.*
- *For any number field K, there exists a set of primes $\mathcal{S}$ of natural density 1 such that $\mathbb{Z}$ has a Diophantine model over $O_{K,\mathcal{S}}$.*

§**8. Final remarks.** This article touched only on a small part of the subject which grew out of Hilbert's Tenth Problem. In particular, we did not discuss a great number of results on the analogs of HTP over different kinds of functions fields and infinite algebraic extensions, and also rings where the problem becomes decidable. We refer the interested reader to the following surveys and collections for more information: [9], [21] and [32].

REFERENCES

[1] GUNTHER CORNELISSEN, THANASES PHEIDAS, and KARIM ZAHIDI, *Division-ample sets and diophantine problem for rings of integers*, ***Journal de Théorie des Nombres Bordeaux***, vol. 17 (2005), pp. 727–735.

[2] GUNTHER CORNELISSEN and ALEXANDRA SHLAPENTOKH, *Defining the integers in large rings of number fields using one universal quantifier*, ***Zapiski Nauchnykh Seminarov POMI***, vol. 358 (2008), pp. 199–223.

[3] GUNTHER CORNELISSEN and KARIM ZAHIDI, *Topology of diophantine sets: Remarks on Mazur's conjectures*, ***Hilbert's tenth problem: Relations with arithmetic and algebraic geometry*** (Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors), Contemporary Mathematics, vol. 270, American Mathematical Society, 2000, pp. 253–260.

[4] ———, *Elliptic divisibility sequences and undecidable problems about rational points*, ***Journal für die Reine und Angewandte Mathematik***, vol. 613 (2007), pp. 1–33.

[5] MARTIN DAVIS, *Hilbert's tenth problem is unsolvable*, ***American Mathematical Monthly***, vol. 80 (1973), pp. 233–269.

[6] MARTIN DAVIS, YURI MATIYASEVICH, and JULIA ROBINSON, *Hilbert's tenth problem, diophantine equations: Positive aspects of a negative solution*, ***Proceedings of the symposium on pure mathematics***, vol. 28, American Mathematical Society, 1976, pp. 323– 378.

[7] Jan Denef, *Hilbert's tenth problem for quadratic rings*, ***Proceedings of the American Mathematical Society***, vol. 48 (1975), pp. 214–220.

[8] Jan Denef and Leonard Lipshitz, *Diophantine sets over some rings of algebraic integers*, ***Journal of London Mathematical Society***, vol. 18 (1978), no. 2, pp. 385–391.

[9] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel (editors), ***Hilbert's tenth problem: Relations with arithmetic and algebraic geometry***, Contemporary Mathematics, vol. 270, American Mathematical Society, Providence, RI, 2000.

[10] Kirsten Eisenträger and Graham Everest, *Descent on elliptic curves and Hilbert's tenth problem*, ***Proceedings of the American Mathematical Society***, vol. 137 (2009), no. 6, pp. 1951–1959.

[11] Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward, ***Recurrence sequences***, Mathematical Surveys and Monographs, vol. 104, American Mathematical Society, Providence, RI, 2003.

[12] David Marker, ***Model theory***, Graduate Texts in Mathematics, vol. 217, Springer-Verlag, New York, 2002, an introduction.

[13] Yuri V. Matiyasevich, ***Hilbert's tenth problem***, Foundations of Computing Series, MIT Press, Cambridge, MA, 1993, translated from the 1993 Russian original by the author.

[14] Barry Mazur, *The topology of rational points*, ***Experimental Mathematics***, vol. 1 (1992), no. 1, pp. 35–45.

[15] ———, *Questions of decidability and undecidability in number theory*, ***The Journal of Symbolic Logic***, vol. 59 (1994), no. 2, pp. 353–371.

[16] ———, *Open problems regarding rational points on curves and varieties*, ***Galois representations in arithmetic algebraic geometry*** (A. J. Scholl and R. L. Taylor, editors), Cambridge University Press, 1998.

[17] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, ***Inventiones Mathematicae***, vol. 181 (2010), pp. 541–575.

[18] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, ***Proceedings of American Mathematical Society***, vol. 104 (1988), no. 2, pp. 611–620.

[19] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, ***Algorithmic number theory*** (C. Fieker and D. Kohel, editors), Lecture Notes in Computer Science, vol. 2369, Springer Verlag, 2002, pp. 33–42.

[20] ———, *Hilbert's tenth problem and Mazur's conjecture for large subrings of* $\mathbb{Q}$, ***Journal of the American Mathematical Society***, vol. 16 (2003), no. 4, pp. 981–990.

[21] ———, *Undecidability in number theory*, ***Notices in the American Mathematical Society***, vol. 55 (2008), no. 3, pp. 344–350.

[22] ———, *Characterizing integers among rational numbers with a universal-existential formula*, ***American Journal of Mathematics***, vol. 131 (2009), no. 3, pp. 675–682.

[23] ———, *Elliptic curves whose rank does not grow and Hilbert's tenth problem over the rings of integers*, private communication.

[24] Bjorn Poonen and Alexandra Shlapentokh, *Diophantine definability of infinite discrete non-archimedean sets and diophantine models for large subrings of number fields*, ***Journal für die Reine und Angewandte Mathematik***, vol. 2005 (2005), pp. 27–48.

[25] Julia Robinson, *Definability and decision problems in arithmetic*, ***The Journal of Symbolic Logic***, vol. 14 (1949), pp. 98–114.

[26] Hartley Rogers, ***Theory of recursive functions and effective computability***, McGraw-Hill, New York, 1967.

[27] Alexandra Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, ***Communications on Pure and Applied Mathematics***, vol. XLII (1989), pp. 939–962.

[28] ———, *Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator*, ***Inventiones Mathematicae***, vol. 129 (1997), pp. 489–507.

[29] ———, *Defining integrality at prime sets of high density in number fields*, ***Duke Mathematical Journal***, vol. 101 (2000), no. 1, pp. 117–134.

[30] ———, *Hilbert's tenth problem over number fields, a survey*, ***Hilbert's tenth problem: Relations with arithmetic and algebraic geometry*** (Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors), Contemporary Mathematics, vol. 270, American Mathematical Society, 2000, pp. 107–137.

[31] ———, *On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree* 2, ***Journal of Number Theory***, vol. 95 (2002), pp. 227–252.

[32] ———, ***Hilbert's tenth problem: Diophantine classes and extensions to global fields***, Cambridge University Press, 2006.

[33] ———, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, ***Transactions of the American Mathematical Society***, vol. 360 (2008), no. 7, pp. 3541–3555.

[34] ———, *Rings of algebraic numbers in infinite extensions of* $\mathbb{Q}$ *and elliptic curves retaining their rank*, ***Archive for Mathematical Logic***, vol. 48 (2009), no. 1, pp. 77–114.

[35] ———, *Using indices of points on an elliptic curve to construct a diophantine model of* $\mathbb{Z}$ *and define* $\mathbb{Z}$ *using one universal quantifier in very large subrings of number fields, including* $\mathbb{Q}$, `arXiv:0901.4168v1 [math.NT]`.

[36] JOSEPH SILVERMAN, ***The arithmetic of elliptic curves***, Springer Verlag, New York, New York, 1986.

DEPARTMENT OF MATHEMATICS
EAST CAROLINA UNIVERSITY
GREENVILLE, NC 27858, USA
E-mail: shlapentokha@ecu.edu
URL: www.personal.ecu.edu/shlapentokha