Notes on Hilbert's Tenth Problem over $\mathbb{Q}$

Marco Streng

20th June 2007

Contents

1 Diophantine subsets of $\mathbb{Q}^n$

Definition. Let R be an integral ring. We call a subset $D \subset R^n$ *Diophantine* if there exists a finite set of polynomials $\{P_1, \dots, P_r\}$ in $n+m$ variables such that for any $x \in R^n$,

$$x \in D \Leftrightarrow \exists y \in R^m : P(x, y) = 0.$$

We call a predicate, relation, function or property *Diophantine* if the set of elements that satisfy the predicate or property, the set of tuples that satisfy the relation or the graph of the function is Diophantine.

Lemma 1.1. *If R is a subring of $\mathbb{R}$, then for every Diophantine set, we can take $r = 1$, i.e. only one polynomial.*

Proof. Take $P = P_1^2 + P_2^2 + \cdots + P_r^2$. □

Lemma 1.2. *Suppose $S, T \subset R^n$ are Diophantine over R, then $S \cap T$ and $S \cup T$ are also Diophantine over R.*

Proof. Let S and T be given by sets of polynomials $\mathcal{P}$ and $\mathcal{Q}$, where the sets of variables "$y_{\mathcal{P}}$" and "$y_{\mathcal{Q}}$" are taken to be disdisjoint.

We can use the union of $\mathcal{P}$ and $\mathcal{Q}$ to give a Diophantine definition of $S \cap T$. For $S \cup T$, take $\{pq : p \in \mathcal{P}, q \in \mathcal{Q}\}$. □

Lemma 1.3. *If R is a field, then the relation $\neq$ is Diophantine.*

Proof. In a field R, we have $x \neq y$ if and only if there exists z such that $(x - y)z = 1$. □

Lemma 1.4. *If R is a subring of $\mathbb{Q}$, then $>, <, \geq, \leq$ and $\neq$ are Diophantine relations i.e. for any such relation, the set of pairs $(a, b) \in R^2$ satisfying such a relation is a Diophantine set.*

Proof. Any positive rational number x can be written as $x = m/n$ for positive integers m, n. By Lagrange's four squares theorem, both $(m - 1)$ and $(n - 1)$ are sums of four squares of integers, so $(e^2 + f^2 + g^2 + h^2 + 1)x = (a^2 + b^2 + c^2 + d^2 + 1)$ for $a, b, \dots, h \in \mathbb{Z} \subset R$. On the other hand, any rational number x that satisfies this equation with $a, b, \dots, h \in R \subset \mathbb{Q}$ must be positive.

Now for any pair $x, y \in R$, we have $x > y$ exactly if there is a positive $z \in R$ with $x = z + y$. Also, $x \geq y$ exactly if either $x > y$ or $x = y$. Finally $x \neq y$ exactly if either $x > y$ or $y > x$. □

Example 1.5. Give $\mathbb{Q}^n = \mathbb{A}^n(\mathbb{Q})$ the Zariski topology. Any open subset X of a closed subset of $\mathbb{Q}^n$ is Diophantine.

Proof. The set X is the zero set of a finite set of polynomials f minus the zero set of a finite set of polynomials g. Now "$f(x) = 0$ and $g(x) \neq 0$" is a Diophantine property by 1.4 and 1.2. □

Definition. *Hilbert's Tenth Problem* over R (HTP(R)) is the following problem. Is there an algorithm which, on input a polynomial $P \in R[X_1, \ldots, X_n]$ in an arbitrary number n of variables, decides whether the equation $P = 0$ has a solution in R^n?

The original tenth problem of Hilbert was to give such an algorithm for $R = \mathbb{Z}$. The DPRM Theorem implies that no such algorithm exists:

DPRM Theorem (Davis, Putnam, Robinson and Matiyasevich). *A subset of $\mathbb{Z}^n$ is Diophantine if and only if it is listable.*

Proof. See for example [Dav73], [DMR74] or [Poo03]. □

Corollary 1.6. *Hilbert's Tenth Problem over $\mathbb{Z}$ has a negative answer.*

Proof. Recall that a set $S \in \mathbb{Z}^n$ is called *listable* (or *recursively enumerable*) if there exists a Turing machine which outputs each element of the set S, but no element of its complement. The set S is called *recursive* if there exists a Turing machine which on a given $y \in \mathbb{Z}^n$ decides whether $x \in \mathbb{Z}^n$.

We start with the following important fact from recursion theory: There is a listable set $S \subset \mathbb{Z}$ that is not recursive. (This follows from the fact that the Halting Problem is undecidable, see also [Poo03].)

By the DPRM Theorem, S is Diophantine, so (by Lemma 1.1) there exists a polynomial $P(X, Y_1, \ldots, Y_n) \in \mathbb{Z}[X, Y_1, \ldots, Y_n]$ such that S consists of those $x \in \mathbb{Z}$ for which there exists $y \in \mathbb{Z}^n$ such that $P(x, y) = 0$. If Hilbert's Tenth Problem has a positive solution, then there is an algorithm which decides, given $x \in \mathbb{Z}$, whether $P(x, y) = 0$ has a solution $y \in \mathbb{Z}^n$. This contradicts the fact that S is not recursive. □

2 Using the negative solution over $\mathbb{Z}$

One way to try to prove that Hilbert's Tenth Problem over $\mathbb{Q}$ has a negative solution, is by using the negative solution for $\mathbb{Z}$. For example, if we could prove that $\mathbb{Z}$ is Diophantine over $\mathbb{Q}$, then for any Diophantine equation D over $\mathbb{Z}$ we can look at a family of Diophantine equations over $\mathbb{Q}$ consisting of D and for every variable x of D an equation that has a solution if and only if $x \in \mathbb{Z}$. Then a positive answer to HTP over $\mathbb{Q}$ gives us a positive answer over $\mathbb{Z}$, which does not exist.

In this section, we will start by introducing Diophantine models, which simulate $\mathbb{Z}$ in a Diophantine sort of way over $\mathbb{Q}$. The existence of such an object would imply that HTP over $\mathbb{Q}$ has a negative solution. Then we will see that such models are in contradiction with a conjecture by Mazur about the real topology on varieties. After that, we move on to objects that are more general than models, but still imply that HTP has a negative answer over $\mathbb{Q}$.

2.1 Diophantine models

Definition. A *Diophantine model* of the ring $\mathbb{Z}$ over $\mathbb{Q}$ is a Diophantine set $S \subset \mathbb{Q}^n$ together with a bijection $\phi : \mathbb{Z} \to S$ such that both the graphs of addition and multiplication in $\mathbb{Z}$ correspond to Diophantine subsets of $S^3 \subset \mathbb{Q}^{3n}$.

Lemma 2.1. *If S is a Diophantine model of $\mathbb{Z}$ in $\mathbb{Q}$, and T is a Diophantine subset of $\mathbb{Z}^m$, then $\phi^m(T)$ is a Diophantine subset of $S^m \subset \mathbb{Q}^{nm}$.*

Proof. As T is Diophantine, there is a set $Y \subset \mathbb{Z}^{l+m}$ and a polynomial f in $l + m$ variables such that Y is the zero set of f and T is the projection of Y to $\mathbb{Q}^m$. We may add a variable for every $+$ and $\cdot$ in f and end up with a bigger l and a new Y which is defined by a family of equations of the forms $x + y = z$ and $xy = z$. Then $\phi(Y)$ is a Diophantine subset of S^{l+m}, so $\phi(T)$ is also Diophantine. □

Proposition 2.2. *If there exists a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$, then HTP($\mathbb{Q}$) has a negative answer.*

Proof. Given a Diophantine equation D over $\mathbb{Z}^m$, let T be the set of solutions of D. The procedure in the above proof shows that $\phi(T)$ is Diophantine over $\mathbb{Q}$ and even more: we can construct a Diophantine equation E for $\phi(T)$ from D and the model S. Now a positive solution to HTP($\mathbb{Q}$) allows us to determine whether E has a solution, but that is equivalent to determining whether $\phi(T)$ (and hence T) is non-empty. This is in contradiction with the negative solution to HTP($\mathbb{Z}$). $\square$

Example 2.3. One can construct an elliptic curve E over $\mathbb{Q}$ such that $E(\mathbb{Q}) \cong \mathbb{Z}$. It has been suggested that such a curve may be a good candidate for a Diophantine model, since addition is given by the chord-and-tangent method, which is already Diophantine. Unfortunately, it is not known whether multiplication in $\mathbb{Z}$ corresponds to a Diophantine function on $E(\mathbb{Q})$.

Actually, because of the point at infinity, $E(\mathbb{Q})$ is not a subset of $\mathbb{Q}^n$, hence we cannot speak about Diophantine sets in our definition. This is not a problem, because we could take the affine part of the curve and add a point outside the curve to it, then call that the point at infinity and make some easy exceptions on the definitions of $+$ and $\cdot$ in our model. This is something which can be done in general: If our definition of Diophantine model is generalized using algebraic varieties or algebraic sets, then they can be written as a union of (not neccessarily open) affine algebraic sets. These affine algebraic sets can then be embedded disjointly into a higher dimensional $\mathbb{A}^n$, so can always turn such a model into a Diophantine model that uses only $\mathbb{Q}^n$.

Lemma 2.4. *If (S, ϕ) is a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$, then both ϕ and its inverse on S are Turing computable.*

Proof. A Turing machine could search for $a_0 \in S$ such that (a_0, a_0, a_0) is in the set S_+, corresponding to the graph of addition in $\mathbb{Z}$. Then $\phi(0)$ must be a_0. Then it could search for $a_1 \in S$, different from a_0, such that (a_1, a_1, a_1) is in the set $S_\bullet$, corresponding to the graph of multiplication. This gives $\phi(1) = a_1$. After that, the machine could look for $\phi(-1) = a_{-1}$ such that $(a_{-1}, a_1, a_0) \in S_+$. Then it can calculate $\phi(n)$ for every n recursively as follows: For $n \in \mathbb{Z}$ find $\phi(n \pm 1)$ by searching for $a \in S$ with $(\phi(n), a_{\pm 1}, a) \in S_+$.

Now for a given $b \in B$, a Turing machine could look at $\phi(0)$, $\phi(1)$, $\phi(-1)$, $\phi(2)$, $\phi(-2), \ldots$, until it finds $\phi(a) = b$. So the inverse of ϕ is also computable. $\square$

2.2 Mazur's Conjecture

Mazur's Conjecture ([Maz92, Conjecture 3]). If X is a variety over $\mathbb{Q}$, then the real topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has finitely many connected components.

That is, $X(\mathbb{R})$ inherits a topology from the topology of $\mathbb{R}$ and $X(\mathbb{Q})$ is a subset of $X(\mathbb{R})$, so we could look at the closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$. Now $X(\mathbb{R})$ consists of finitely many components, but $\overline{X(\mathbb{Q})}$ is not always equal to $X(\mathbb{R})$. The conjecture states however, that $\overline{X(\mathbb{Q})}$ also consists of only finitely many components. This conjecture is the weakest of a series of conjectures posed by Barry Mazur in the 1990's. It is known to hold for example when X is a curve or an abelian variety (see [Poo03]).

Now, we will look at this conjecture in connection with Diophantine models. First, we note that Mazur's conjecture implies the same statement for Diophantine sets:

Proposition 2.5. *Mazur's conjecture implies that the real topological closure $\overline{S}$ of any Diophantine subset $S \subset \mathbb{Q}^n$, consists of finitely many connected components.*

Proof. If S is Diophantine, then there is an algebraic set $Y \subset \mathbb{Q}^{m+n}$ such that S is the image of a continuous map f from Y to $\mathbb{Q}^n$. The set Y is the union of the sets of rational points on finitely many varieties, so by Mazur's conjecture, $\overline{Y}$ consists of finitely many connected components.

From now on, the argument is purely topological. By a limit argument, we see that $\overline{Y}$ gets mapped inside $\overline{f(Y)}$, so $\overline{S} = \overline{f(Y)} = \overline{f(\overline{Y})}$. A continuous map maps connected sets to connected sets, so $f(\overline{Y})$ is a finite union of connected components, because $\overline{Y}$ is. The closure of a finite union is the union of the closures, so $\overline{S} = \overline{f(\overline{Y})}$ consists of finitely many connected components. □

From this proposition, we immediately get the following result, which was the reason Mazur proposed this conjecture.

Corollary 2.6 (Mazur). *Mazur's conjecture implies that no infinite Diophantine subset of $\mathbb{Q}^n$ is discrete in the real topology. In particular, if Mazur's conjecture is true, then $\mathbb{Z}$ is not Diophantine in $\mathbb{Q}$.*

But even more is true:

Theorem 2.7 (Cornelissen-Zahidi [CZ00]). *Mazur's conjecture implies that there is no Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.*

Proof. Assume Mazur's conjecture and suppose that there is a Diophantine model (S, ϕ) of $\mathbb{Z}$ over $\mathbb{Q}$. By Corollary 2.6, there is a non-isolated point $s \in S$.

We construct a sequence of integers $(m_i)_{i=1}^{\infty}$ as follows. If $\phi(0) = s$, then $m_1 = 1$, otherwise $m_1 = 0$. Order $\mathbb{Z}$ as $0, 1, -1, 2, -2, 3, \ldots$. Then for any positive integer i, let m_{i+1} be first integer after m_i (in the above ordering) such that

$$0 < |\phi(m_{i+1}) - s| \leq |\phi(m_i) - s|/2,$$

where $|\cdot|$ is the Euclidean norm. Because ϕ is computable (Lemma 2.4), we can calculate m_{i+1} with a Turing machine by inspecting the integers after m_i. This shows that the set $M = \{m_i : i = 1, 2, 3, \ldots\}$ is listable, so by the DPRM Theorem, it is Diophantine. But then $\phi(M)$ is also Diophantine (Lemma 2.1), which contradicts Corollary 2.6, because all the points in $\phi(M)$ are isolated. □

Notice that the above does not say that the model itself is a counterexample to Mazur's conjecture. We need the entire DPRM Theorem to construct the counterexample.

2.3 Diophantine Interpretation

In this section we will look at Diophantine interpretations, which are more general than Diophantine models, but still imply that HTP($\mathbb{Q}$) has a negative answer. The main open question is whether Diophantine interpretations contradict Mazur's conjecture, like Diophantine models do.

Definition. A *Diophantine interpretation*[1] is a Diophantine set $S \subset \mathbb{Q}^n$ together with a surjection $\psi : S \to \mathbb{Z}$ such that the inverse images S_+ resp. $S_\bullet$ of the graphs of addition and multiplication in $\mathbb{Z}$ are Diophantine subsets of S^3.

We can apply the same proofs as for Lemma 2.1 and proposition 2.2 if we replace the images under ϕ by the inverse images under ψ. So we get

[1] This is non-standard terminology, taken from [Poo03].

Lemma 2.8. *If S is a Diophantine interpretation of $\mathbb{Z}$ over $\mathbb{Q}$, and T is a Diophantine subset of $\mathbb{Z}^m$, then $\psi^{-1}(T)$ is a Diophantine subset of S^m.*

Proposition 2.9. *If there exists a Diophantine interpretation of $\mathbb{Z}$ over $\mathbb{Q}$, then HTP($\mathbb{Q}$) has a negative answer.*

Now, we have seen that Diophantine interpretations are just as useful for HTP($\mathbb{Q}$) as Diophantine models. Next, we will see that they are just as computable.

Remark 2.10. We can define the equivalence relation $\sim$ on an interpretation S by $b \sim b' \Leftrightarrow \psi(b) = \psi(b')$. This relation is Diophantine, because if we pick b_0 such that $\psi(b_0) = 0$, then $\psi(b) = \psi(b')$ if and only if $(b, b_0, b') \in S_+$.

Lemma 2.11. *If (S, ψ) is a Diophantine interpretation of $\mathbb{Z}$ over $\mathbb{Q}$, then the surjection ψ has a Turing computable section ϕ, that is, $\psi \circ \phi = \mathrm{id}_{\mathbb{Z}}$. Also, this implies that ψ is Turing computable.*

Proof. First, a section ϕ is calculated in the same way as in the proof of Lemma 2.4. Then for given $b \in S$, a Turing machine could search all pairs (a, b') with $a \in \mathbb{Z}$ and $b' \in S$ for a pair such that $\phi(a) = b'$ and $b \sim b'$. Such a pair exists and $\sim$ is Diophantine by the above remark, so it will be found. Then $\psi(b) = \psi(b') = a$. □

Now that we have seen some things that are the same, the question is: what is new? Suppose that (S, ψ) is a Diophantine interpretation of $\mathbb{Z}$ over $\mathbb{Q}$. If there is a Diophantine subset $T \subset \mathbb{Q}^n$ such that T intersects every fibre of ψ exactly once, then $T \cap S$ is a Diophantine model. So in order to get something really new from our generalization, we have to prevent this from happening.

Also, the natural question arises: do Diophantine interpretations allow us to escape Mazur's conjecture? In other words,

Open Question 2.12. Does Mazur's conjecture imply that there is no Diophantine interpretation of $\mathbb{Z}$ over $\mathbb{Q}$?

We have already seen that the existence of a Diophantine set T such that $\#(T \cap \psi^{-1}a) = 1$ for every $a \in \mathbb{Z}$ implies that there is a Diophantine model and Mazur's conjecture is false. Even more is true: If we only have $\#(T \cap \psi^{-1}a) \leq 1$ for every $a \in \mathbb{Z}$ and $T \cap S$ is infinite, then we can adapt the proof of Theorem 2.7 to see that Mazur's conjecture is false:

Proposition 2.13. *If there is a Diophantine interpretation (S, ψ) and a Diophantine set T such that $T \cap S$ is infinite and $\#(T \cap \psi^{-1}(a)) \leq 1$ for every $a \in \mathbb{Z}$. Then Mazur's conjecture is false.*

Proof. Suppose that we have such $S, T \subset \mathbb{Q}^n$ and suppose that Mazur's conjecture is true. Then $S \cap T$ is an infinite Diophantine set, so by Corollary 2.6, there is a non-isolated point $s \in S$.

We construct a sequence n_i in $S \cap T$ as follows. Let n_0 be any point different from s. Then, to find n_{i+1}, we inspect all points b in $S \cap T$ until $0 < |b - s| \leq |n_i - s|/2$. Then we set $n_{i+1} = b$. This construction can be done by a Turing machine and ψ is computable by Lemma 2.11. Therefore, the set $M = \{\psi(n_i) : i = 0, 1, 2 \ldots\} \subset \mathbb{Z}$ is listable, hence Diophantine by the DPRM Theorem. This implies (Lemma 2.8) that $T \cap \psi^{-1}(M) = \{n_i : i = 0, 1, 2, \ldots\}$ is Diophantine. But it is also infinite and discrete, so this contradicts Corollary 2.6. □

Corollary 2.14. *Suppose that there is a Diophantine interpretation (S, ψ). If there exist a Diophantine set $T \subset \mathbb{Q}^n$ and a listable set $L \subset \mathbb{Z}$ such that $T \cap \psi^{-1}(L)$ is infinite and $\#(T \cap \psi^{-1}(a)) \leq 1$ for every $a \in L$, then Mazur's conjecture is false.*

Proof. By the DPRM Theorem, L is Diophantine. Therefore, so is $T \cap \psi^{-1}(L)$, so we replace T by $T \cap \psi^{-1}(L)$. Then $T \cap \psi^{-1}(a)$ is empty for all $a \notin L$ and we can apply the proposition. □

So in order to escape Mazur's conjecture, we at least need to make sure that there is no Diophantine set T as above.

References

[CZ00] Gunther Cornelissen and Karim Zahidi. Topology of diophantine sets: Remarks on Mazur's conjectures. In *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, volume 270 of *Contemporary Mathematics*, pages 253–260. American Mathematical Society, 2000.

[Dav73] Martin Davis. Hilbert's tenth problem is unsolvable. pages 233–269, 1973.

[DMR74] M. Davis, Y. Matijasevich, and J. Robinson. Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution. In *Mathematical developments arising from Hilbert problems*, number XXVIII in Proc. Sympos. Pure Math., pages 323–378, 1974.

[Maz92] Barry Mazur. The topology of rational points. *Experimental Mathematics*, 1(1):35–45, 1992.

[Maz95] Barry Mazur. Speculations about the topology of rational points: an update. *Astérisque*, 228:165–182, 1995. Columbia University Number Theory Seminar (New York, 1992).

[Maz98] Barry Mazur. Open problems regarding rational points on curves and varieties. In *Galois representations in arithmetic algebraic geometry*, volume 254 of *London Mathematical Society Lecture Note Series*, pages 239–265. Cambridge Univ. Press, 1998.

[Poo03] Bjorn Poonen. Hilbert's tenth problem over rings of number-theoretic interest. 2003. At the Arizona Winter School on "Number theory and logic" 2003. http://math.berkeley.edu/ poonen/papers/aws2003.pdf.

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.