THE NUMBER OF SOLUTIONS OF A DIOPHANTINE EQUATION OVER A RECURSIVE RING

CHRISTOPH BAXA

(Communicated by Julia Knight)

ABSTRACT. Let R be a recursive ring whose quotient field is not algebraically closed with the property that Hilbert’s Tenth Problem over R is undecidable, and let A be a non-empty proper subset of $\{0, 1, 2, \dots\} \cup \{\aleph_0\}$. We prove that it is not decidable whether the number of solutions of a diophantine equation with coefficients in R is in A .

Hilbert’s Tenth Problem asked for an algorithm which would decide whether an arbitrary diophantine equation is solvable. It was solved by Ju. V. Matijasevič [6], who built on earlier work by M. Davis, H. Putnam and J. Robinson [4] and showed that it is undecidable. An elementary introduction to the problem and its solution and ramifications can be found, e.g., in the textbook [7]. In the decades following this breakthrough a large number of consequences and extensions of Hilbert’s Tenth Problem have been studied and proved.

We fix the following notation for the remainder of this paper: if R is an enumerable ring and $p \in R[X_1, \dots, X_n]$, let

$$\#(p) = |\{(a_1, \dots, a_n) \in R^n \mid p(a_1, \dots, a_n) = 0\}|.$$

Furthermore, set $C = \{0, 1, 2, \dots\} \cup \{\aleph_0\}$.

M. Davis [3] proved the following surprising result in the case $R = \mathbb{Z}$.

Theorem. *Let A be a non-empty proper subset of C . Then there is no algorithm for testing whether $\#(p) \in A$ where p denotes a polynomial with integer coefficients.*

A simplification of Davis’ proof can be found in C. Smoryński’s textbook [10] (see also [9]).

Hilbert’s Tenth Problem has also been extended to a large number of rings, most notably rings of integers in number fields. The most prominent problem in this direction is Hilbert’s Tenth Problem over $\mathbb{Q}$, which remains open in spite of dramatic recent progress made by B. Poonen [1]. His survey paper [2] is an excellent introduction to this field. Much more information and further references can be found in the conference proceedings [5] and in A. Shlapentokh’s monograph [8].

In order to be able to transfer notions from recursion theory to a ring it has to be recursive, which intuitively says that its elements can be represented by a computer and that its addition, subtraction and multiplication can be carried out by a computer.

Received by the editors December 1, 2011 and, in revised form, February 12, 2012.
 2010 *Mathematics Subject Classification.* Primary 11U05; Secondary 03B25, 11D45.
Key words and phrases. Hilbert’s Tenth Problem, recursive ring.

Definition. A countable integral domain R will be called a recursive ring if there is an injection $J : R \rightarrow \mathbb{N}$ such that $J(R)$ is recursive and the functions translating addition, subtraction and multiplication are recursive. (For example, there is a computable function $J_+ : \mathbb{N}^2 \rightarrow \mathbb{N}$ such that $J_+(J(x), J(y)) = J(x + y)$ for all $x, y \in R$.)

The map J is called a recursive presentation of R . A set $A \subseteq R$ is called recursive (recursively enumerable) under the presentation J if $J(A)$ is recursive (recursively enumerable).

A function $f : A(\subseteq R^n) \rightarrow R$ is called recursive under a presentation J if its translation is recursive (i.e., there is a recursive function $J_f : \mathbb{N}^n \rightarrow \mathbb{N}$ such that $J_f(J(x_1), \dots, J(x_n)) = J(f(x_1, \dots, x_n))$ for all $(x_1, \dots, x_n) \in A$).

It is known that every polynomial function $R^n \rightarrow R$ is recursive. If R is a finitely generated ring, then being recursive does not depend on the presentation [8, Appendix A].

It is the purpose of this note to extend Davis' theorem to suitable recursive rings R for which Hilbert's Tenth Problem is undecidable; i.e., there is no algorithm which can decide whether an equation $p(X_1, \dots, X_n) = 0$ with $n \in \mathbb{N}$ and $p \in R[X_1, \dots, X_n]$ has a solution.

Theorem 1. *Let R be a recursive ring whose quotient field is not algebraically closed with the property that Hilbert's Tenth Problem over R is undecidable and let $\emptyset \subsetneq A \subsetneq C$. Then there is no algorithm for testing whether $\#(p) \in A$ for an arbitrary polynomial p with coefficients in R .*

Lemma 2. *Let R be an integral domain whose quotient field K is not algebraically closed and let $p_1, \dots, p_m \in R[X_1, \dots, X_n]$. Then there is a polynomial*

$$H_m(p_1, \dots, p_m) \in R[X_1, \dots, X_n]$$

such that the system of equations

$$p_1(X_1, \dots, X_n) = \dots = p_m(X_1, \dots, X_n) = 0$$

has a solution in R^n if and only if $H_m(p_1, \dots, p_m)(X_1, \dots, X_n) = 0$ has a solution in R^n .

The proof of this lemma can be found, e.g., as Lemma 1.2.3 in [8]. We sketch the proof for the reader's convenience.

Proof. Let $m = 2$ and let $h(X) = a_k X^k + \dots + a_1 X + a_0 \in R[X]$ (with $k \neq 0$ and $a_k \neq 0$) denote a polynomial without roots in K . Then $a_0 \neq 0$ and $g(X) = a_0 X^k + \dots + a_{k-1} X + a_k$ has no roots in K either. Set

$$H_2(p_1, p_2)(X_1, \dots, X_n) = \sum_{i=0}^k a_i p_1^{k-i}(X_1, \dots, X_n) p_2^i(X_1, \dots, X_n).$$

Let $(b_1, \dots, b_n) \in R^n$. If $p_1(b_1, \dots, b_n) = p_2(b_1, \dots, b_n) = 0$, then

$$H_2(p_1, p_2)(b_1, \dots, b_n) = 0.$$

Conversely, let $H_2(p_1, p_2)(b_1, \dots, b_n) = 0$. If $p_1(b_1, \dots, b_n) \neq 0$, then

$$h\left(\frac{p_2(b_1, \dots, b_n)}{p_1(b_1, \dots, b_n)}\right) = 0,$$

and if $p_2(b_1, \dots, b_n) \neq 0$, then

$$g\left(\frac{p_1(b_1, \dots, b_n)}{p_2(b_1, \dots, b_n)}\right) = 0,$$

both of which are impossible. For $m > 2$ let

$$H_m(p_1, \dots, p_m) = H_2(H_{m-1}(p_1, \dots, p_{m-1}), p_m).$$

Finally, let $H_1(p) = p$. □

Lemma 3. *Let R be a recursive ring whose quotient field is not algebraically closed and let $k \in \{0, 1, 2, \dots\}$. Then there is a recursive operation T^k on the set $\bigcup_{n=0}^{\infty} R[X_1, \dots, X_n]$ such that $\#(T^k(p)) = \#(p) + k$ for all $p \in \bigcup_{n=0}^{\infty} R[X_1, \dots, X_n]$.*

Proof. If $k = 0$, let $T^k(p) = p$. If $k \geq 1$, let

$$(T^k(p))(X_1, \dots, X_n, Y) = H_2(p(X_1, \dots, X_n), Y) \cdot \prod_{i=1}^k H_{n+1}(X_1, \dots, X_n, Y - a_i),$$

where Y is a new variable and $a_1, a_2, a_3, \dots$ is a recursive enumeration of an infinite subset of $R \setminus \{0\}$. Then $(b_1, \dots, b_n, c) \in R^{n+1}$ is a solution of

$$(T^k(p))(X_1, \dots, X_n, Y) = 0$$

if and only if either $p(b_1, \dots, b_n) = c = 0$ or $b_1 = \dots = b_n = 0$ and $c \in \{a_1, \dots, a_k\}$. □

Remark. If the characteristic of R is zero, we can use $a_i = 1 + \dots + 1$ (with i summands). One can also use the following variant: let

$$(\tilde{T}^1(p))(X_1, \dots, X_n, Y) = H_2(p(X_1, \dots, X_n), Y) \cdot H_{n+1}(X_1, \dots, X_n, Y - 1)$$

and $\tilde{T}^k(p) = \tilde{T}^1(\tilde{T}^{k-1}(p))$ for $k \geq 2$.

Lemma 4. *Let R be a recursive ring whose quotient field is not algebraically closed. Then there is a recursive operation T^∞ on $\bigcup_{n=0}^{\infty} R[X_1, \dots, X_n]$ such that*

$$\#(T^\infty(p)) = \begin{cases} 0, & \text{if } \#(p) = 0, \\ \aleph_0, & \text{if } \#(p) > 0, \end{cases}$$

for all $p \in \bigcup_{n=0}^{\infty} R[X_1, \dots, X_n]$.

Proof. Let $(T^\infty(p))(X_1, \dots, X_n, Y) = p(X_1, \dots, X_n) \cdot h(Y)$, where Y is a new variable and $h \in R[Y]$ is a non-constant polynomial without roots in the quotient field of R . If $p(X_1, \dots, X_n) = 0$ is unsolvable, then so is $p(X_1, \dots, X_n)h(Y) = 0$. If $(b_1, \dots, b_n) \in R^n$ satisfies $p(b_1, \dots, b_n) = 0$, then $p(b_1, \dots, b_n)h(c) = 0$ for all $c \in R$. □

Proof of Theorem 1. We first assume that $\aleph_0 \in A$. As $A \neq C$ there is a $k \in \{0, 1, 2, \dots\}$ such that $k \notin A$. Then $\#(p) = 0$ if and only if $\#(T^k(T^\infty(p))) \notin A$. This means that Hilbert's Tenth Problem over R would be decidable if we could decide whether the number of solutions of a diophantine equation is in A . If $\aleph_0 \notin A$, then $\aleph_0 \in C \setminus A$. If we could decide whether $\#(p) \in A$ for every polynomial p , we could also decide whether $\#(p) \in C \setminus A$, which is impossible by the first case. □

REFERENCES

- [1] Bjorn Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$* , J. Amer. Math. Soc. **16** (2003), no. 4, 981–990 (electronic), DOI 10.1090/S0894-0347-03-00433-8. MR1992832 (2004f:11145)
- [2] Bjorn Poonen, *Undecidability in number theory*, Notices Amer. Math. Soc. **55** (2008), no. 3, 344–350. MR2382821 (2008m:11238)
- [3] Martin Davis, *On the number of solutions of Diophantine equations*, Proc. Amer. Math. Soc. **35** (1972), 552–554. MR0304347 (46 #3482)
- [4] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436. MR0133227 (24 #A3061)
- [5] *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, Contemporary Mathematics, vol. 270, American Mathematical Society, Providence, RI, 2000. Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999; Edited by Jan Denef, Leonard Lipshitz, Thanases Pheidas and Jan Van Geel. MR1802007 (2001g:00018)
- [6] Ju. V. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR **191** (1970), 279–282 (Russian). MR0258744 (41 #3390)
- [7] Yuri V. Matiyasevich, *Hilbert's tenth problem*, translated from the 1993 Russian original by the author; with a foreword by Martin Davis. Foundations of Computing Series, MIT Press, Cambridge, MA, 1993. MR1244324 (94m:03002b)
- [8] Alexandra Shlapentokh, *Hilbert's tenth problem. Diophantine classes and extensions to global fields*, New Mathematical Monographs, vol. 7, Cambridge University Press, Cambridge, 2007. MR2297245 (2009e:11235)
- [9] C. Smoryński, *A note on the number of zeros of polynomials and exponential polynomials*, J. Symbolic Logic **42** (1977), no. 1, 99–106. MR0485277 (58 #5124)
- [10] C. Smoryński, *Logical Number Theory I*, Springer-Verlag, Berlin, 1991. MR1106853 (92g:03001)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF VIENNA, NORDBERGSTRASSE 15, A-1090 WIEN, AUSTRIA

E-mail address: christoph.baxa@univie.ac.at