PROBLEMS RELATED TO "EXTENSIONS OF HILBERT'S TENTH PROBLEM"

MODERATED BY B. POONEN AND T. SCANLON, NOTES BY J. DEMEYER

Question 1 (D'Aquino)**.** *Fermat's little theorem states that*

$$x^p \equiv x \mod p$$

Proof 1: $\mathbb{F}_p^*$ *is cyclic using the fact that*

$$\#\{x \mid P(x) = 0\} \leq \deg(P)$$

Proof 2: List $R = \{1, 2, \ldots, p-1\}$*. Show that for* $a \in R$*, multiplication by* a *is a permuation. Then*

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} (ai) \mod p$$

From this follows that

$$(p-1)! \equiv a^{p-1}(p-1)! \mod p$$

Give a "simple" definition of $n! \bmod p$ *(this is OK for exponentiation).*

Proof 3: Use

$$(x+y)^p = x^p + y^p \mod p$$

Find other proofs.

Question 2 (D'Aquino)**.** *Is DPRM a theorem of* $I\Delta_0$*? This is Peano arithmetic with the induction axiom for every first order formula* $\varphi(x)$ *with bounded quantifiers*

$$I(\varphi) : \Big[\varphi(0) \ \wedge \ (\forall x)\big(\varphi(x) \to \varphi(x+1)\big)\Big] \to (\forall x)\big(\varphi(x)\big)$$

A positive answer would imply that NP is equal to co-NP.

Given a Σ_1 *formula* $\psi(\vec{x})$*, does there exist a polynomial* $P(\vec{x}, \vec{y})$ *such that*

$$I\Delta_0 \vdash (\forall \vec{x})\Big(\psi(\vec{x}) \leftrightarrow (\exists \vec{y})\big(P(\vec{x}, \vec{y}) = 0\big)\Big)$$

Consider the language $L = \{+, \cdot, 0, 1, \#, \leq\}$*, where*

$$\#(x, y) := x^{\lfloor \log(y) \rfloor}$$

Question 3 (Demeyer)**.** *Consider the ring* $\mathbb{F}_q[W, Z]$*. Does there exist a Diophantine predicate* $\alpha(f, \vec{g})$ *with* $f \in \mathbb{F}_q[W, Z]$ *and* $\vec{g} \in \mathbb{F}_q[Z]^n$ *such that*

(1) *For all* $f \in \mathbb{F}_q[W, Z]$*, there exists a* $\vec{g} \in \mathbb{F}_q[Z]^n$ *such that* $\alpha(f, \vec{g})$ *holds.*
(2) *For all* $\vec{g} \in \mathbb{F}_q[Z]^n$*, the set* $\{f \in \mathbb{F}_q[W, Z] \mid \alpha(f, \vec{g}) \text{ holds}\}$ *is finite.*

This will imply that r.e. = Diophantine for $\mathbb{F}_q[W, Z]$*.*

It is possible to give such a Diophantine predicate if "$\alpha(\cdots)$ *holds" is replaced with "*$\alpha(\cdots)$ *does not hold".*

Question 4 (Demeyer)**.** *Fix a prime p. Is there a Diophantine model of $\mathbb{F}_q[Z]$ over $\mathbb{F}_p[Z]$, when q is a power of p, uniformly in q?*

In other words, do there exist polynomials $f(t, \vec{x}, \vec{x'})$, $g(t, \vec{y}, \vec{y'})$ and $h(t, \vec{z}, \vec{z'})$ such that:

- *For every power q of p, $S_q := \{\vec{x} \mid f(Z^q, \vec{x}, \vec{x'}) = 0\}$ is in bijection with $\mathbb{F}_q[Z]$.*
- *$\{\vec{y} \mid g(Z^q, \vec{y}, \vec{y'}) = 0\} \subseteq S_q^3$ corresponds to the graph of addition on $\mathbb{F}_q[Z]$.*
- *$\{\vec{z} \mid h(Z^q, \vec{z}, \vec{z'}) = 0\} \subseteq S_q^3$ corresponds to the graph of multiplication on $\mathbb{F}_q[Z]$.*

Or with "Z^q" replaced by some other reasonable function $\{$powers of $p\} \to \mathbb{F}_p[Z]$.

This might imply that r.e. = Diophantine for $\mathbb{F}_p[Z]$.

Question 5 (Pheidas)**.** *An* additive polynomial *in $\mathbb{F}_p[Z]$ is a polynomial of the form*

$$F(Z) = \alpha_0 Z + \alpha_1 Z^p + \alpha_2 Z^{p^2} + \cdots + \alpha_n Z^{p^n} \qquad (\alpha_i \in \mathbb{F}_p)$$

These are the polynomials that satisfy $f(A + B) = f(A) + f(B)$ for all $A, B \in \mathbb{F}_p[Z]$. Can we Diophantinely define the additive polynomials?

*(Demeyer) The following suggestion by Pheidas does **not** work:*

$$\begin{aligned}
&(\exists A, B, C, L, M, N \in \mathbb{F}_p[Z])(\exists \alpha, \beta, \gamma, \lambda, \mu, \nu \in \mathbb{F}_p)\\
&\qquad F = (A^p - A) + \alpha Z\\
&\qquad \wedge\ F^2 = (B^p - B) + \beta Z + (C^p - C)Z + \gamma Z^2\\
&\qquad \wedge\ F^3 = (L^p - L) + \lambda Z + (M^p - M)Z + \mu Z^2 + (N^p - N)Z^2 + \nu Z^3\\
&\qquad \vdots
\end{aligned}$$

Continue this up to some power F^n. All additive polynomials satisfy this predicate, but also the following non-additive polynomial satisfies, no matter how many equations you add:

$$\sum_{i=0}^{p-1} \left(Z^{2p} - Z^{p+1}\right)^{p^i}$$

Fact 6 (Cornelissen)**.** *Here is an example of a non-commutative undecidable theory. Let L be any field of characteristic $p > 0$. Let A_L denote the ring of additive polynomials with coefficients from L (a ring for addition and composition). Then $f \circ Z^p = Z^p \circ f$ is a Diophantine definition of $A_{\mathbb{F}_p} \cong \mathbb{F}_p[Z]$ in A_L.*

The same works in the quotient skew field Q_L of A_L. Hence the Diophantine theory of A_L and Q_L in a ring language augmented by a symbol for Z is undecidable (since the theories of $\mathbb{F}_q[Z]$ and $\mathbb{F}_q(Z)$ are by Denef and Pheidas). If one can therefore give a Diophantine definition of A_L or Q_L in $L[Z]$ or $L(Z)$, the theory of the latter would be undecidable.

Question 5 of Pheidas tries to define the set *A_L. For cognescenti: this works more generally if "$f \circ Z^p = Z^p \circ f$" is replaced by $f \circ \rho_T = \rho_T \circ f$ for ρ a Drinfeld $\mathbb{F}_q[T]$-module over L.*

Question 7 (Davis)**.** *Let $\mathbb{H}$ be the quaternions over $\mathbb{Q}$, and*

$$\mathcal{O} = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$$

(1) *Is there an algorithm to decide whether a noncommutative polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in $\mathbb{Q}$ has a solution in $\mathbb{H}$?*
(2) *Is there an algorithm to decide whether a noncommutative polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in $\mathbb{Q}$ has a solution in $\mathcal{O}$?*

(3) *Is there an algorithm to decide whether a noncommutative polynomial equation $f(x_1, \dots, x_n) = 0$ with coefficients in $\mathbb{H}$ has a solution in $\mathbb{H}$?*
(4) *Is there an algorithm to decide whether a noncommutative polynomial equation $f(x_1, \dots, x_n) = 0$ with coefficients in $\mathbb{H}$ has a solution in $\mathcal{O}$?*

Is $\mathbb{Z}$ existentially definable in $\mathcal{O}$? This probably works:

$$x \in \mathbb{Z} \iff (\exists I, J, K)(I^2 = -1 \ \wedge \ J^2 = -1 \ \wedge \ IJ = -JI \ \wedge \ xI = Ix \ \wedge \ xJ = Jx)$$

Very likely done by D. Tunc. This solves the problems 2 and 4.

In an analogous way, $\mathbb{Q}$ should be Diophantine in $\mathbb{H}$. So, 1 and 3 are equivalent with Hilbert's Tenth Problem over $\mathbb{Q}$.

Same questions for the matrix rings $M_n(\mathbb{Z})$ and $M_n(\mathbb{Q})$.

Question 8 (Pheidas)**.** *Is the following problem decidable:*

Given $P(\vec{x}) \in \mathbb{Z}[\vec{x}]$, do there exist $n_1, \dots, n_m \in \mathbb{N}$ such that $P(2^{n_1}, \dots, 2^{n_m}) = 0$?

The answer is YES: this is related to the Mordell–Lang conjecture for tori.

Question 9 (Pheidas)**.** *Can we redo the proof of Hilbert's Tenth Problem over $\mathbb{Z}$, using elliptic curves instead of Pell equations?*

Hopefully, this would lead to a lower number of variables and/or lower degree.

Can this give a finite-fold Diophantine definition of all r.e. sets?

Question 10 (Davis)**.** *Find a native proof of DPRM in $\mathbb{Z}$, instead of referring to $\mathbb{N}$.*

Prove DPRM for some class of rings abstractly, with no reference to $\mathbb{N}$.

Question 11 (Davis)**.** *A subset $S \subseteq \mathbb{N}$ is called* simple *if and only if:*

(1) *S is r.e.*
(2) *$\mathbb{N} \setminus S$ is infinite.*
(3) *If $T \subseteq \mathbb{N} \setminus S$ is r.e., then T is finite.*

Take a simple set $S \subseteq \mathcal{O}_K$ and an embedding $f : \mathcal{O}_K \hookrightarrow R$, for some ring R. Let

$$S = \{x \in \mathcal{O}_K \mid (\exists \vec{y} \in \mathcal{O}_K^n)(P(x, \vec{y}) = 0)\}$$

and consider

$$S' = \{x \in \mathcal{O}_K \mid (\exists \vec{y} \in R^n)(P(x, \vec{y}) = 0)\}$$

Clearly, $f(S) \subseteq S'$. Either S' is simple (hence not recursive) or its complement is finite. In particular, if $P(x, \vec{y}) \in \mathbb{Z}[x, \vec{y}]$ is such that

$$\{x \in \mathbb{Z} \mid (\exists \vec{y} \in \mathbb{Z}^n)(P(x, \vec{y}) = 0)\}$$

is simple and

$$\mathbb{Z} \setminus \{x \in \mathbb{Z} \mid (\exists \vec{y} \in \mathbb{Q}^n)(P(x, \vec{y}) = 0)\}$$

is infinite, then Hilbert's Tenth Problem for $\mathbb{Q}$ has a negative answer.

Reference: Davis, Putnam, "Diophantine sets over polynomial rings".

Question 12 (Cornelissen)**.** *If $\mathbb{Z}$ admits a Diophantine interpretation in $\mathbb{Q}$ (that is, using an equivalence relation), does it follow that Mazur's conjecture is wrong?*

See Cornelissen–Zahidi, Contemp. Math. ***270*** *253–260.*

Question 13 (Cornelissen). *Solve in integers A, B, X, Y:*

$$(A^2 + B^2)(A^2 + 11B^2) = 9 \cdot 25 \cdot (X^2 - 5Y^2)^2$$

This is related to defining the integers in the rational numbers by a Σ_3^+-formula, see Cornelissen–Zahidi, `ArXiv:math.NT/0412473`*.*

Question 14 (Cornelissen). *Jeroen Demeyer has observed that the existence of a polynomial bijection $\mathbb{N}^2 \to \mathbb{N}$ implies that any first order formula over $\mathbb{N}$ in positive prenex form is equivalent to one in which every block of consecutive universal quantifiers is replaced by just one (and the number of existential quantifiers goes up). Such a polynomial bijection can be found in Davis, Math. Monthly **80**, 236–237.*

*Does something similar work for $\mathbb{Q}$, in other words, can we find a Diophantine injection $\mathbb{Q}^2 \hookrightarrow \mathbb{Q}$? There are some observations related to this in C.R.A.S. Paris **328**, 3–8 (1999); for example, this would follow from the generalized abc-conjecture.*

Question 15 (Rojas). *What is the smallest n such that Hilbert's Tenth Problem over $\mathbb{Z}$ restricted to one polynomial in n variables is undecidable?*

Minimal n is known to be $2 \leq n \leq 22$ by Matijasevič, and probably $2 \leq n \leq 11$ by some Chinese. There is some evidence that $n = 3$.

Question 16 (Rojas). *Consider sequences in $\mathbb{Z}[x]$ of the form*

$$1, x, g_1, g_2, \ldots$$

where each g_i is a sum, difference or product of 2 earlier terms in the sequence. Let

$$\tau(f) := \min\{n \mid \text{there exists such a sequence with } g_n = f\}$$

Conjecture: there exists a constant c such that the number of integer zeros of f is at most $\big(1 + \tau(f)\big)^c$, where f is not identically zero.

Question 17 (Rojas). *Let $c_j \in \mathbb{Z}$ and consider polynomials of the form*

$$P(x_1, \ldots, x_n) = \prod_{j=1}^{n+1} c_j \vec{x}^{\vec{a_j}}$$

where $\vec{a_1}, \ldots, \vec{a_{n+1}} \in \mathbb{N}^n$ are affinely independent.

Can we decide in polynomial time (for fixed p) whether there exists a $\vec{x} \in \mathbb{Q}_p^n$ such that $P(\vec{x}) = 0$?

Answer: NO, because the $0/1$ knapsack problem can be encoded as a subproblem of this (Poonen). Over $\mathbb{R}$ this is in NP, and probably in P (modulo some technicalities).

Can we decide whether there exists a $\vec{x} \in \mathbb{Q}^n$ such that $P(\vec{x}) = 0$?

This includes the unsolved problem of deciding whether a genus 1 curve of the form $ax^3 + by^3 = 1$ has a rational point, so it is probably very hard.

Question 18 (Rojas). *Is there a computable bound (in function of f) on the size of the largest integer solution to $f(x, y) = 0$, when there are finitely many solutions?*

This is already done for genus 1 curves.

There exists an algorithm to decide finiteness of the set of solutions.

For rational points, there are papers by Minhyong Kim from Arizona:

*"Relating decision and search algorithms for rational points on curves of higher genus", Arch. Math. Logic **42** (2003), no. 6, 563–568*

"On relative computability for curves", `ArXiv:math.NT/0502224`

Question 19 (Jarden). *Is there an algorithm to decide whether $f(x, y) = 0$ has infinitely many $\mathbb{Q}$-rational solutions?*

This seems to be very hard for genus 1 curves. It has been done in other cases.

Possible if Ш is finite for all elliptic curves over $\mathbb{Q}$.

Question 20 (Shlapentokh). *Let E be an elliptic curve over $\mathbb{Q}$ of rank 2. Does there exist an existentially definable rank 1 subgroup?*

Question 21 (Shlapentokh). *Let E be an elliptic curve over $\mathbb{Q}$ of rank 2. Can we find a subset S of (infinitely many) primes such that the subgroup generated by $E(\mathbb{Z}[S^{-1}])$ has rank one?*

If S is finite, the Siegel–Mahler theorem states that $E(\mathbb{Z}[S^{-1}])$ is finite.

Suppose S is infinite, but of density 0. Is $E(\mathbb{Z}[S^{-1}])$ still "small"?

Question 22 (Zahidi). *Look at the Denef curve*

$$\mathcal{E} : f(t)Y^2 = f(X)$$

where f is a cubic. If we choose the curve in a good way, then $\mathcal{E}(k(t))$ has rank 1.

Define

$$\mathcal{E}_u : f(u)Y^2 = f(X)$$

Try to give conditions on $u \in k(t)$ such that $\mathcal{E}_u(k(t))$ also has rank 1.

Question 23 (Pheidas). *Consider the elliptic curve*

$$E : Y^2 = X^3 + aX + b$$

The following statement is Diophantine: "$\mathrm{End}(E)/(2\,\mathrm{End}(E))$ has more than 2 elements". Because $\mathrm{End}(E)$ is a free finitely generated $\mathbb{Z}$-module, this is equivalent with "$\mathrm{End}(E) \neq \mathbb{Z}$".

So, we can existentially define the following set in $\mathbb{C}(Z)$:

$$\{j \in \mathbb{C} \mid j \text{ is the } j\text{-invariant of a CM elliptic curve}\}$$

Can we do anything with this set?

Question 24 (Pheidas). *If $x \in \mathbb{C}(Z)$, then*

$$\mathrm{ord}_{Z=0}\left(\frac{1+Zx^2}{1-Zx^2}\right) = \mathrm{ord}_{Z=\infty}\left(\frac{1+Zx^2}{1-Zx^2}\right) = 0$$

Can every $f \in \mathbb{C}(Z)$ with $\mathrm{ord}_{Z=0}(f) = \mathrm{ord}_{Z=\infty}(f)$ even be written as (obviously, the number 1000 can be changed to any other integer)

$$f = u^2 \prod_{i=1}^{1000} \frac{1+Zx_i^2}{1-Zx_i^2}$$

Weaker version: is this true at least for $f \in \mathbb{Q}(Z)$, with $u, x_i \in \mathbb{C}(Z)$?

This would imply that the existential theory of $\mathbb{C}(Z)$ is undecidable.

Question 25 (Pheidas). *Is $\{f \in \mathbb{C}(Z) \mid \mathrm{ord}_{Z=0}(f) \geq 0\}$ (existentially) definable in $\mathbb{C}(Z)$, where there is a symbol for Z in the language?*

Question 26 (Moret-Bailly)**.** *Is there a nontrivial valuation ring*

$$R \subset Frac\frac{\mathbb{R}[x,y]}{(x^2+y^2+1)}$$

which is definable?

Same question for "semi-local ring" (finite intersection of valuation rings) instead of "valuation ring"? This is equivalent with the problem for valuation rings.

Question 27 (Shlapentokh)**.** *Can one find an algebraically closed field K and a nontrivial valuation ring $R \subset K(Z)$ (or a finite extension), which is definable in $K(Z)$?*

Question 28 (Shlapentokh)**.** *Is there an algebraic extension K of $\mathbb{Q}$ and a nontrivial valuation ring $R \subset K$, such that the residue field of R is algebraically closed and R is definable over K?*

Answer: YES. Inside $\mathbb{Q}_p^{alg} = \overline{\mathbb{Q}} \cap \mathbb{Q}_p \subseteq \overline{\mathbb{Q}_p}$, the ring $\mathbb{Z}_p^{alg}$ is definable.

Fact 29 (Pheidas)**.** $\mathbb{C}[[Z]]$ *is definable in* $\mathbb{C}((Z))$*:*

$$x \in \mathbb{C}[[Z]] \iff (\exists y)(1 + Zx^2 = y^2)$$

Proven using Hensel's lemma.

Question 30 (Shlapentokh)**.** *Let K be a number field and $\mathcal{O}_K$ its ring of integers. Fix an embedding $K \hookrightarrow \mathbb{C}$, with $K \not\subseteq \mathbb{R}$. Is $\{\alpha \in \mathcal{O}_K \mid |\alpha| \leq 1\}$ Diophantine in $\mathcal{O}_K$?*

If this is true for all K, then Hilbert's Tenth Problem is undecidable for all $\mathcal{O}_K$.

Question 31 (Cornelissen)**.** *Let K be a number field and $\mathcal{O}_K$ its ring of integers. A set $A \subseteq \mathcal{O}_K$ is said to be* division-ample *if*

- *It is Diophantine over $\mathcal{O}_K$.*
- *Any $x \in \mathcal{O}_K$ divides some $a \in A$.*
- *There exists a positive integer l such that for any $a \in A$, there exists $\tilde{a} \in \mathbb{Z}$ with $\tilde{a}|a$ and $N(a) \leq |\tilde{a}|^l$.*

Observe that if $A \subseteq \mathbb{Z}$, then one can dispose of the last condition by choosing $\tilde{a} = a$ and $l = [K : \mathbb{Q}]$.

Question: give an example of such A where for any finite $S \subseteq \mathcal{O}_K$, A is not a subset of $\mathcal{O}_K^* \cdot (\mathbb{Z} \cup S)$.

Cornelissen–Pheidas–Zahidi have shown that HTP($\mathcal{O}_K$) has a negative answer if such A exists and there exists an elliptic curve of rank one over K.

Question 32 (Poonen)**.** *Is is true that for all number fields K, there exists a variety X (scheme of finite type) over $\mathbb{Z}$ such that*

1. *$X(\mathbb{Z})$ is infinite.*
2. *$X(\mathcal{O}_K) = X(\mathbb{Z})$.*

Question 33 (Videla)**.** *Let $K \subseteq \mathbb{Q}^{tot.\ real} \subseteq \overline{\mathbb{Q}}$. Define*

$$A_K := \{s \in \mathbb{R}_{>0} \mid \text{There exist infinitely many } \alpha \in \mathcal{O}_K \text{ such that } \alpha \text{ and its conjugates are all in } [0,s]\}$$

Question of Julia Robinson: Is the infimum of A_K an element of A_K? If so, the first order theory of $\mathcal{O}_K$ is undecidable.

For $K = \mathbb{Q}^{tot.\ real}$, $\inf(A_K) = 4 \in A_K$.

Question 34 (Zahidi). *Let* $\mathbb{R}^{alg} := \overline{\mathbb{Q}} \cap \mathbb{R}$. *It is known that* $\mathbb{R}^{alg} \equiv \mathbb{R}$ *(elementary equivalence), but that* $\mathbb{R}^{alg}(t) \not\equiv \mathbb{R}(t)$. *On the other hand, the existential theories of* $\mathbb{R}^{alg}(t)$ *and* $\mathbb{R}(t)$ *are the same. What is the minimal quantifier complexity for which* $\mathbb{R}^{alg}(t)$ *and* $\mathbb{R}(t)$ *have different theories?*

Another question is the minimal number of variables one needs.

Question 35 (Pheidas). *Let* X *be a variety over* $\mathbb{Q}$. *Call* X hyperbolic *iff there is no nonconstant holomorphic map* $\mathbb{C} \to X(\mathbb{C})$. *Is there an algorithm which can decide whether a variety* $X/\mathbb{Q}$ *over hyperbolic?*

Question 36 (Jarden). *Given* $f_1, \ldots, f_n \in \mathbb{C}[x_1, \ldots, x_m]$ *which are homogeneous of degree* d. *Assume that the only common zero of the* f_i *is* $(0, \ldots, 0)$. *Prove that*

$$V(f_1(\vec{x}) = b_1, \ldots, f_n(\vec{x}) = b_n)$$

is finite, for all $b_1, \ldots, b_n \in \mathbb{C}$.

Solution: If it were infinite, then the variety in $\mathbb{P}^m$ *defined by the homogenizations of the equations would be positive-dimensional, and then it would have to intersect the hyperplane at infinity, which would mean that the* f_i *have a common zero.*