L-functions, proximity functions, and Diophantine sets

Hector Pasten

The goal of this note (and my talk) is to discuss descriptions of the Diophantine sets of global fields and their rings of integers. By [4] and [10], a set in $\mathbb{Z}$ is Diophantine if and only if it is listable in the sense of recursion theory; I'll refer to this result as the DPRM theorem. This gives a complete description of the Diophantine sets of $\mathbb{Z}$, implying that Hilbert's tenth problem is unsolvable.

Rings of integers. The analogue of DPRM for rings of S-integers in a global function field (S a non-empty finite set of places) follows from [5] and [23].

The analogue of the DPRM for the rings of integers O_K of a number field K is known for: CM fields and certain degree 4 extensions [7, 6]; K with exactly one complex place [16, 21, 24]; K contained in one of the previous fields [20].

Towards the general case, the series of papers [18, 2, 22] culminated in the following elliptic curve criterion by Poonen and Shlapentokh: *Suppose that for every cyclic extension of prime degree L/F of number fields there is an elliptic curve E defined over F such that* $\mathrm{rk}(E(L)) = \mathrm{rk}(E(F)) > 0$. *Then for every number field K, the Diophantine sets and the listable sets of O_K are the same.*

Mazur and Rubin [13] verified the elliptic curve criterion conditionally on a conjecture on Shafarevich-Tate groups. Alternatively, using non-vanishing theorems for L-functions [8, 14], Ram Murty and I proved [15] that the criterion is satisfied under the rank part of Birch and Swinnerton-Dyer conjecture:

Theorem 1 (Murty-Pasten). *Suppose that (certain) elliptic curves over number fields E/F satisfy that the L-function $L(s, E)$ is automorphic and:*

- *(Parity conjecture)* $\mathrm{ord}_{s=1} L(s, E) \equiv \mathrm{rk}(E(F)) \mod 2$
- *(Analytic rank 0 BSD) If χ is a Hecke character of F corresponding to a finite extension L/F and if $L(1, E/F, \chi) \neq 0$, then $E(L)^{\chi}_{\mathbb{C}} = 0$.*

Then the Poonen-Shlapentokh elliptic curve criterion is satisfied, and for every number field K, the analogue of DPRM for O_K holds.

Global fields. Hilbert's tenth problem for $\mathbb{F}_q(z)$ is undecidable [17, 25], while it is open for $\mathbb{Q}$. Nevertheless, the question of whether in a global field K Diophantine sets and listable sets are the same, remains open in all cases.

The analogue of DPRM holds for $\mathbb{Q}$ if and only if $\mathbb{Z}$ is Diophantine in $\mathbb{Q}$. In the direction of the latter, Koenigsmann proved [9] that $\mathbb{Z}$ admits a $\forall\exists\exists...\exists$-positive definition in $\mathbb{Q}$, so that it only remains to eliminate one universal quantifier.

However, Mazur conjectured that if $X/\mathbb{Q}$ is a projective variety then the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has only finitely many connected components [11, 1]. This would imply that $\mathbb{Z}$ is not Diophantine in $\mathbb{Q}$. There is a lesser known version of Mazur's topological conjecture over number fields (including non-Archimedean places) with analogous non-Diophantineness implications [12, 19]:

Conjecture 2 (Mazur). *Let K be a number field, $v \in M_K$, and X/K a projective variety. For $x \in X(K_v)$, let $Z_x \subseteq X$ be the limit of the Zariski closure of $X(K) \cap U$ in X, as U varies over v-neighborhoods of x. Then $\{Z_x : x \in X(K_v)\}$ is finite.*

Mazur's conjecture is specific to the number field case and the analogue for global function fields is *false*, as the following example shows:

Example 3 (cf. [17, 3])**.** *Let $p > 2$ be prime. The sets $A = \{z^{p^n} : n \geq 0\}$ and $B = \{\lambda + z + z^p ... + z^{p^n} : n \geq 0$ and $\lambda \in \mathbb{F}_p\}$ are Diophantine in $K = \mathbb{F}_p(z)$. (They are images of K-rational points of certain curve X defined over K.)*

Proximity functions and heights. Let K be a global field. Let X/K be a projective variety with $\mathrm{CD}^+(X/K)$ its set of effective Cartier divisors. Fix a choice of Weil functions $\lambda_{D,v} : X(\bar{K}) - D \to \mathbb{R}$ for $D \in \mathrm{CD}^+(X/K)$ and $v \in M_K$.

Let $S \subseteq M_K$ be a finite set of places and let $D \in \mathrm{CD}^+(X/K)$. The *proximity function* to D relative to S is $m_{X,S}(D, -) := \sum_{v \in S} \lambda_{D,v}(-)$, and the *height* relative to D is $h_{X,D}(-) := \sum_{v \in M_K} \lambda_{D,v}(-)$. Both are functions $X(\bar{K}) - D \to \mathbb{R}$. One has the *trivial inequality* $m_{X,S}(D, x) \leq h_{X,D}(x) + O(1)$ for $x \in X(\bar{K}) - D$, and the central problem in Diophantine approximation is to establish non-trivial inequalities between the proximity function and the height of rational points. Let me formulate a conjecture trying to formalize the hope that the proximity function contributes non-trivially to the height. Details will appear elsewhere.

Conjecture 4. *Let K be a global field and let $S \neq \emptyset$ be a finite set of places of K. Let X, Y be projective varieties over K. Let $D \in \mathrm{CD}^+(X/K)$ and let $f : X \to Y$ be a K-morphism. Suppose that for all $E \in \mathrm{CD}^+(Y/K)$, the height h_{X,f^*E} is unbounded on $X(K) - (D + f^*E)$. Then there exists $E_0 \in \mathrm{CD}^+(Y/K)$ such that $m_{X,S}(f^*E_0, -)$ is unbounded on $X(K) - (D + f^*E_0)$.*

Here is a summary of some results:

Theorem 5. *The case $Y = \mathbb{P}^1$ implies the general case in Conjecture 4, and in the number field setting Conjecture 2 implies Conjecture 4. In addition, Conjecture 4 holds unconditionally if X is a curve or an abelian variety.*

The relevance of Conjecture 4 in our setting is justified by the following.

Theorem 6. *Assume Conjecture 4. Then:*

(i) *$\mathbb{Z}$ is not Diophantine in $\mathbb{Q}$.*
(ii) *$\mathbb{F}_p[z]$ is not Diophantine in $\mathbb{F}_p(z)$.*
(iii) *$\{z^n : n \geq 1\}$ is not Diophantine in $\mathbb{F}_p(z)$.*

Observe that Example 3 is consistent with Conjecture 4: The curve X has maps $f, g : X \to \mathbb{P}^1$ defined over $K = \mathbb{F}_p(z)$ such that $f(X(K)) = A$ and $g(X(K)) = B$. Take $S = \{v_z\}$ the z-adic place. Let Y_0, Y_1 be the homogeneous coordinates in $\mathbb{P}^1$. For f we take the divisor $E_0 = \{Y_1 = 0\}$ and for g we take $E_0 = \{Y_1^p - Y_1 + z = 0\}$.

References

[1] J.-L. Colliot-Thélène, A. N. Skorobogatov, P. Swinnerton-Dyer, *Double fibres and double covers: paucity of rational points*, Acta Arith. 79 (1997), no. 2, 113-135.

[2] G. Cornelissen, T. Pheidas, K. Zahidi, *Division-ample sets and the Diophantine problem for rings of integers*. J. Théor. Nombres Bordeaux 17 (2005), no. 3, 727-735.

[3] G. Cornelissen, K. Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures.* Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 253-260, Contemp. Math., 270, Amer. Math. Soc., Providence, RI, 2000.

[4] M. Davis, H. Putnam, J. Robinson, *The decision problem for exponential diophantine equations.* Ann. of Math. (2) 74 1961 425-436.

[5] J. Demeyer, *Recursively enumerable sets of polynomials over a finite field are Diophantine.* Invent. Math. 170 (2007), no. 3, 655-670.

[6] J. Denef, *Diophantine sets over algebraic integer rings. II.* Trans. Amer. Math. Soc. 257 (1980), no. 1, 227-236.

[7] J. Denef, L. Lipshitz, *Diophantine sets over some rings of algebraic integers.* J. London Math. Soc. (2) 18 (1978), no. 3, 385-391.

[8] S. Friedberg, J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on* $GL(2)$. Ann. of Math. (2) 142 (1995), no. 2, 385-423.

[9] J. Koenigsmann, *Defining* $\mathbb{Z}$ *in* $\mathbb{Q}$. Ann. of Math. (2) 183 (2016), no. 1, 73-93.

[10] J. Matijasevich, *The Diophantineness of enumerable sets.* (Russian) Dokl. Akad. Nauk SSSR 191 1970 279-282.

[11] B. Mazur, *The topology of rational points*, Exper. Math. 1 (1992), no. 1, 35-45.

[12] B. Mazur, *Open problems regarding rational points on curves and varieties*, Galois representations in arithmetic algebraic geometry (Durham 1996), London Math. Soc. Lect. Note Ser. 254 (1998), 239-265.

[13] B. Mazur, K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem.* Invent. Math. 181 (2010), no. 3, 541-575.

[14] K. Murty, R. Murty, *Non-vanishing of L-functions and applications.* (English summary) Progress in Mathematics, 157. Birkhäuser Verlag, Basel, 1997. xii+196 pp. ISBN: 3-7643-5801-7

[15] R. Murty, H. Pasten, *Elliptic curves, L-functions, and Hilbert's tenth problem.* Submitted (2016).

[16] T. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers.* Proc. Amer. Math. Soc. 104 (1988), no. 2, 611-620.

[17] T. Pheidas *Hilbert's tenth problem for fields of rational functions over finite fields.* Invent. Math. 103 (1991), no. 1, 1-8.

[18] B. Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers.* Algorithmic number theory (Sydney, 2002), 33-42, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[19] B. Poonen, A. Shlapentokh, *Diophantine definability of infinite discrete nonarchimedean sets and Diophantine models over large subrings of number fields.* J. Reine Angew. Math. 588 (2005), 27-47.

[20] H. Shapiro, A. Shlapentokh, *Diophantine relationships between algebraic number fields.* Comm. Pure Appl. Math. 42 (1989), no. 8, 1113-1122.

[21] A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields.* Comm. Pure Appl. Math. 42 (1989), no. 7, 939-962.

[22] A. Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers.* Trans. Amer. Math. Soc. 360 (2008), no. 7, 3541-3555.

[23] A. Shlapentokh, *Diophantine relations between rings of S-integers of fields of algebraic functions in one variable over constant fields of positive characteristic.* J. Symbolic Logic 58 (1993), no. 1, 158-192.

[24] C. Videla *On Hilbert's Tenth Problem*, Atas da Xa Escola de Algebra, Vitoria, ES, Brasil Colecao Atas 16 p. 95-108, Sociedade Brasileira de Matematica (1989).

[25] C. Videla *Hilbert's tenth problem for rational function fields in characteristic 2.* Proc. Amer. Math. Soc. 120 (1994), no. 1, 249-253.