Elliptic curves and Hilbert's 10th problem for number fields

Florian Ito Sprung

April 22, 2024

Abstract

We establish an analogue of Hilbert's 10th Problem, which is a conjecture of Denef and Lipshitz, for the ring of integers of some number fields of small degree, including those of the form $\mathbb{Q}(\sqrt[5]{n})$ with $n \leqslant 37$. We then describe how to use the arithmetic of elliptic curves to find families of degree 6 number fields satisfying this conjecture. We also make some conjectures related to these techniques.

1 Hilbert's 10th Problem and the Denef–Lipshitz Conjecture

The tenth problem in Hilbert's list of 23 problems posed at the International Congress of Mathematicians in 1900 asks whether there is an algorithm to determine if a polynomial $f(\vec{x}) \in \mathbb{Z}[x_1, x_2, \cdots, x_n]$ has a solution $f(\vec{x}) = 0$ for some $\vec{x} \in \mathbb{Z}^n$. [1]

Hilbert's 10th problem was solved in 1970 by Matiyasevič in the negative, i.e. there is no general algorithm that can decide this [10]. The interested reader may now read the appendix for a sketch of the ideas underlying the proof.

A natural question is to ask what happens when we replace every instance of $\mathbb{Z}$ above by a ring R.

Hilbert's 10th Problem for R.

Is there an algorithm that can determine whether for a polynomial $f(\vec{x}) \in R[x_1, \cdots, x_n]$ there is a solution $\vec{x} \in R^n$ to the equation $f(\vec{x}) = 0$?

Answer	R
No	$\mathbb{Z}$ (original problem)
Yes	$\mathbb{C}$ or a finite field
??	$\mathbb{Q}$
No?	$\mathcal{O}_F$ = the ring of integers of a number field F

As indicated in the above table, the answer differs with the choice of R. For $R = \mathbb{C}$ or a finite field, it is yes, while for $R = \mathbb{Q}$, it seems unclear what to conjecture. For $R = \mathcal{O}_F$ the ring of integers of a number field F, Denef and Lipshitz made the following conjecture in 1973:

Conjecture 1.1 (Denef–Lipshitz Conjecture [4])**.** *Let F be a number field. Then for $R = \mathcal{O}_F$, Hilbert's Problem for R has a negative solution, i.e. there is no algorithm that can decide whether a polynomial $f(\vec{x}) \in R[x_1, \cdots, x_n]$ admits a solution $f(\vec{x}) = 0$ with $\vec{x} \in R^n$.*

[1] This is not exactly the original formulation, which considered multiple polynomials, didn't use the word 'algorithm,' and was worded with the expectation that such an algorithm would exist!

It is customary to refer to the above conjecture as the Denef–Lipshitz Conjecture for F, although the name "Denef–Lipshitz Conjecture for $\mathcal{O}_F$" would be more correct. For example, the Denef–Lipshitz Conjecture for $\mathbb{Q}$ is Matiyasevič's theorem.

The Denef–Lipshitz Conjecture (DLC) is known for the following number fields F:

- any totally real number field F, or a quadratic extension thereof, see [4, 5],
- a number field admitting one complex place, [14, 18, 19]. An important example of such a field is $F = \mathbb{Q}(\sqrt[3]{n})$,
- any number field F that is not totally real and so that $[F : \mathbb{Q}] = 4$ and there is a (proper, nontrivial) intermediate field between F and $\mathbb{Q}$ [5],
- F is a subfield of one of the extensions mentioned above; see [17]. In particular, it follows from the Kronecker–Weber Theorem that the DLC is unsolvable when $F/\mathbb{Q}$ is abelian.
- If the conjecture holds for a number field F, then it holds for certain infinite families of degree ℓ^n-extensions L of F. More precisely, once F has been chosen, then for all but finitely many primes ℓ and all $n \geqslant 1$, the conjecture holds for infinitely many cyclic ℓ^n-extensions L of F; see [11, 12][2]. See also [16] for a recent result on cyclotomic $\mathbb{Z}_l$-extensions.
- F belongs to an explicit family of number fields of the form $\mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$;[7]. We will study this family further.
- In [2], G. Cornelissen, T. Pheidas and K. Zahidi studied the case where F is a number field satisfying two specific arithmetic conditions.
- In the recent preprint of B. Mazur, K. Rubin and A. Shlapentokh [13], related questions for a large family of Galois extensions of $\mathbb{Q}$ have been studied.

Here are some scenarios for which the DLC is unknown at present:

- number fields F for which $[F : \mathbb{Q}] = 4$ and there is no intermediate field.

  An example (for which we solve the DLC in the next section) is $F = \mathbb{Q}(r)$ with r a solution to $x^4 + 8x + 12 = 0$. Note that there is no intermediate field because the Galois group A_4 of the Galois closure of F has no subgroups of index two[3].
- number fields F of the form $F = \mathbb{Q}(\sqrt[5]{n})$ or $F = \mathbb{Q}(\sqrt[6]{n})$,
- number fields of the form $F = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q})$ for arbitrary primes p and q.

2 The relationship with elliptic curves

A combination of two theorems by Poonen and Shlapentokh connects the conjecture of Denef and Lipshitz to the arithmetic of elliptic curves. The theorem states the following:

[2] We thank Karl Rubin for patiently clarifying this point. The main ingredient for deriving this from [12, Theorem 1.2] is that the simple abelian variety can be chosen to be a non-CM elliptic curve.

[3] See Example 4.15 and Remark 4.16 in Keith Conrad's write-up 'Galois groups as permutation groups' at https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisaspermgp.pdf that discusses this field in detail.

Theorem 2.1 (Poonen [15] and Shlapentokh [18]). *Let F be a number field. If there is an elliptic curve E defined over $\mathbb{Q}$ so that*

$$\mathrm{rank} E(F) = \mathrm{rank} E(\mathbb{Q}) > 0,$$

then the Denef–Lipshitz conjecture holds for F.

More generally, given a finite extension $F' \supset F$ of a number field F for which the Denef–Lipshitz conjecture holds, the presence of an elliptic curve $E/\mathbb{Q}$ for which

$$\mathrm{rank} E(F') = \mathrm{rank} E(F) > 0$$

implies the Denef–Lipshitz Conjecture for F'.

This theorem suggests the following strategy for proving the DLC:
Given a number field F, find an elliptic curve $E/\mathbb{Q}$ so that

$$\mathrm{rank} E(F) = \mathrm{rank} E(\mathbb{Q}) > 0.$$

Proposition 2.2 (García-Fritz and Pasten). *The Denef–Lipshitz conjecture holds for the integer ring of the number field $\mathbb{Q}(\sqrt[5]{2})$.*

Indeed, [7, Section 3.1] employs the elliptic curve of Cremona label 58a1 to prove this.
We follow this strategy further and prove the DLC for a few new number fields.

Proposition 2.3. *The Denef–Lipshitz conjecture holds for the integer rings of the number fields*

1. $\mathbb{Q}(\sqrt[5]{n})$ *with* $n \leqslant 37$*, and also with* $n = 39, 41, 43 - 47, 49, 51 - 55, 57 - 59, 61, 62, 64, 66 - 71, 74 - 79, 81, 82, 84, 87, 89, 91 - 95, 97 - 100$*,*
2. $\mathbb{Q}(\sqrt[6]{2})$*, and*
3. $\mathbb{Q}(r)$*, r a root of* $x^4 + 8x + 12$.

Proof. Let E be the curve with Cremona label 145a1. An equation for this curves is given by $y^2 = x^3 - 43x + 102$. We let $F = \mathbb{Q}(\sqrt[5]{3})$. For these choices, we run the following SAGE code:

```
E = EllipticCurve("145a1")
K.<t> = NumberField(x^5 - 3)
EK = E.base_extend(K)
r = EK.rank()
print('The Mordell-Weil rank in ', K, 'is', r)
```

This confirms that

$$\mathrm{rank} E(F) = \mathrm{rank} E(\mathbb{Q}) = 1$$

for this particular choice.

Running the same program with the appropriate modifications for any number field $F = \mathbb{Q}(\sqrt[5]{n})$ and elliptic curve E as shown in the table establishes the proposition.

E	some possible F's
145a1: $y^2 = x^3 - 43x + 102$	any $F = \mathbb{Q}(\sqrt[5]{n})$ for $n \in \{3, 6, 7, 12, 15, 17, 20, 21, 23, 26, 28, 30, 31, 35, 39, 45, 51, 52, 53, 54, 59, 68, 74, 76, 94, 97, 98\}$
91a1: $y^2 + y = x^3 + x$	$F = \mathbb{Q}(\sqrt[5]{2})$
184b1: $y^2 = x^3 - x^2 - 4x + 5$	$F = \mathbb{Q}(\sqrt[5]{5})$
102a1: $y^2 = x^3 - 3267x + 45630$	$\mathbb{Q}(\sqrt[5]{10}), \mathbb{Q}(\sqrt[5]{22}), \mathbb{Q}(\sqrt[5]{58}), \mathbb{Q}(\sqrt[5]{62}), \mathbb{Q}(\sqrt[5]{82}), \mathbb{Q}(\sqrt[5]{92})$
136a1: $y^2 = x^3 + x^2 - 4x$	$\mathbb{Q}(\sqrt[5]{14}), \mathbb{Q}(\sqrt[5]{58})$ (also found via 102a1) , $\mathbb{Q}(\sqrt[5]{70}), \mathbb{Q}(\sqrt[5]{78})$
57a1: $y^2 = x^3 - 3024x + 70416$	$\mathbb{Q}(\sqrt[5]{18})$
224a1: $y^2 = x^3 + x^2 + 2x$	$\mathbb{Q}(\sqrt[5]{13}), \mathbb{Q}(\sqrt[5]{43})$
224a2: $y^2 = x^3 + x^2 - 8x - 8$	$\mathbb{Q}(\sqrt[5]{n})$ with $n = 11, 29, 33, 57, 79, 89, 93, 95, 99$
238a2: $y^2 = x^3 - 77787x + 979830$	$\mathbb{Q}(\sqrt[5]{66})$
312b1: $y^2 = x^3 - 4320x - 50112$	$\mathbb{Q}(\sqrt[5]{75}), \mathbb{Q}(\sqrt[5]{87})$
312f1: $y^2 = x^3 + 6048x + 578880$	$\mathbb{Q}(\sqrt[5]{91})$
504e1: $y^2 = x^3 - 6x + 5$	$\mathbb{Q}(\sqrt[5]{19}), \mathbb{Q}(\sqrt[5]{37}), \mathbb{Q}(\sqrt[5]{47})$
336e1: $y^2 = x^3 + 20304x + 245376$	$\mathbb{Q}(\sqrt[5]{44}), \mathbb{Q}(\sqrt[5]{61})$
342e1: $y^2 = x^3 - 4131x + 10206$	$\mathbb{Q}(\sqrt[5]{34}), \mathbb{Q}(\sqrt[5]{46})$
534a2: $y^2 = x^3 + 33669x + 4495446$	$\mathbb{Q}(\sqrt[5]{77})$
545a3: $y^2 = x^3 - 1184787x - 396834066$	$\mathbb{Q}(\sqrt[5]{69}), \mathbb{Q}(\sqrt[5]{71})$
384d1: $y^2 = x^3 - 4320x + 89856$	$\mathbb{Q}(\sqrt[5]{67})$
256a1: $y^2 = x^3 - 4320x + 96768$	$\mathbb{Q}(\sqrt[5]{84})$
400a1: $y^2 = x^3 - 50x - 125$	$\mathbb{Q}(\sqrt[5]{55}), \mathbb{Q}(\sqrt[5]{87})$
426b1: $y^2 = x^3 - 371331x + 88614270$	$\mathbb{Q}(\sqrt[5]{41})$

We note that all the fields of the form $\mathbb{Q}(\sqrt[5]{n})$ in the statement of the proposition appear in the table, e.g. $\mathbb{Q}(\sqrt[5]{24}) = \mathbb{Q}(\sqrt[5]{18})$.

As for the non-quintic fields in the proposition, we use the following:

E	F
58a1: $y^2 = x^3 - 19x + 46$	$\mathbb{Q}(\sqrt[6]{2})$
88a1: $y^2 = x^3 - 4x + 4$	$\mathbb{Q}(r)$, r a root of $x^4 + 8x + 12$

□

The moral of the proposition is that a judiciously chosen elliptic curve, such as that with Cremona label 145a1 (which by the way also reproves the DLC for $\mathbb{Q}(\sqrt[5]{2})$ and $\mathbb{Q}(\sqrt[5]{18})$ via Theorem 2.1!) can furnish us with many instances of the DLC. Unfortunately, there is no known method for finding an appropriate E given an F – one can find E in the above example by simply looking through elliptic curves of small conductor. What is desired is a more systematic approach. The following is a proposition using quadratic twists, and appeared first in a paper by García–Fritz and Pasten [7, Proposition 3.3]:

Proposition 2.4. *Suppose the DLC holds for a number field F. If there is an elliptic curve E so that*

1. $\mathrm{rank} E(F) = 0$, *and*
2. $\mathrm{rank} E(\mathbb{Q}(\sqrt{d})) > 0$,

then DLC holds for $F(\sqrt{d})$.

Proof. The idea is to apply the theorem of Poonen and Shlapentokh to the dth quadratic twist $E^{(d)}$ of the elliptic curve E.

The two conditions in the proposition imply that $F(\sqrt{d}) \neq F$. But the second condition implies that $0 < \text{rank}E(F(\sqrt{d}))$. Now,

$$\text{rank}E(F(\sqrt{d})) = \text{rank}E^{(d)}(F(\sqrt{d})) = \text{rank}E(F) + \text{rank}E^{(d)}(F).$$

By the first condition, we have that $\text{rank}E(F) + \text{rank}E^{(d)}(F) = \text{rank}E^{(d)}(F)$, so putting it all together yields

$$\text{rank}E^{(d)}(F(\sqrt{d})) = \text{rank}E^{(d)}(F) > 0.$$

□

3 Results

Proposition 2.4 is amenable to families of elliptic curves satisfying the conclusions of the theorem of Poonen and Shlapentokh. García–Fritz and Pasten made use of it to addressed families of DLC as follows:

Theorem 3.1 (García–Fritz and Pasten [7])**.** *There are explicit sets $\mathcal{P}$ and $\mathcal{Q}$ of primes so that DLC holds for*

$$F = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q}) \text{ for every } p \in \mathcal{P}, q \in \mathcal{Q}.$$

Further, the densities of the sets $\mathcal{P}$ and $\mathcal{Q}$ are given by $\delta(\mathcal{P}) = \frac{5}{16}$ and $\delta(\mathcal{Q}) = \frac{1}{12}$.

Here, the density δ is defined by the Čebotarev density theorem as follows. The sets $\mathcal{P}$ and $\mathcal{Q}$ turn out to be both *Čebotarev sets*, i.e. sets $\mathcal{S}$ of primes so that there is a Galois extension $K/\mathbb{Q}$ and a conjugacy-stable set $\mathcal{C} \subseteq \text{Gal}(K/\mathbb{Q})$ so that $\mathcal{S}$ agrees with the set $\{p : \text{Frob}_p \in \mathcal{S}\}$ up to finitely many exceptions. Because of the Čebotarev density theorem, the following limit exists and is equal to $\frac{\#\mathcal{C}}{[K:\mathbb{Q}]}$:

$$\lim_{x\to\infty} \frac{\#\mathcal{S} \cap [1, x]}{\pi(x)},$$

where $\pi(x)$ is the prime counting function. We denote this limit by $\delta(\mathcal{S})$, and call it simply the *density* of $\mathcal{S}$. Note that by construction, this density is always a rational number.

A consequence of the Denef–Lipshitz Conjecture would be the following:

Conjecture 3.2. *There are sets primes $\mathcal{P}$ and $\mathcal{Q}$, each of density 1, so that the Denef–Lipshitz Conjecture holds for number fields of the form*

$$F = \mathbb{Q}(\sqrt[3]{p}, \sqrt{-q}) \text{ for every } p \in \mathcal{P}, q \in \mathcal{Q}.$$

In joint work with D. Kundu and A. Lei, we made some progress towards this conjecture by enlarging the sets of primes to ones with higher densities:

Theorem 3.3 (Kundu, Lei, and the author [9])**.** *There are sets $\mathcal{P}' \supset \mathcal{P}$ and $\mathcal{Q}' \supset \mathcal{Q}$ so that the conclusions of Theorem 3.1 hold with $\mathcal{P}$ replaced by $\mathcal{P}'$ and $\mathcal{Q}$ replaced by $\mathcal{Q}'$, and so that*

$$\delta(\mathcal{P}') = \frac{9}{16}, \quad \delta(\mathcal{Q}') = \frac{7}{48}$$

One may try to optimize the density of one set of primes at the expense of the other. In this direction, we obtained the following result:

Theorem 3.4 (Kundu, Lei, and the author [9]). *There are explicit sets of primes $\mathcal{P}''$ and $\mathcal{Q}''$ so that the Denef–Lipshitz conjecture holds for number fields of the form*

$$F = \mathbb{Q}(\sqrt[3]{p}, \sqrt{7 \times q}) \text{ for every } p \in \mathcal{P}'', q \in \mathcal{Q}''.$$

These sets have densities

$$\delta(\mathcal{P}') = \frac{103}{128}, \quad \delta(\mathcal{Q}') = \frac{1}{36}$$

4 Discussion of the proof and open questions

To make the points in the key proposition, Proposition 2.4, work, we need to find an elliptic curve E so that

1. $\text{rank}E(\mathbb{Q}(\sqrt[3]{p})) = 0$, and
2. $\text{rank}E\left(\mathbb{Q}(\sqrt{d})\right) > 0$, for appropriately chosen d (i.e. $d = -q$ resp. $d = 7q$).

We then count how many times this can be done. It turns out that elliptic curves that satisfy conditions (1) and (2) often enough are the curves given in Weierstraß form and Cremona label by

$$y^2 + y = x^3 - x^2 - 268x + 1781 \quad (E557b1),$$

and

$$y^2 = x^3 - x^2 - 11x - 11 \qquad (E704d1).$$

4.1 Ingredients for the proof

Let E be any of the two elliptic curves just discussed. We want to show that condition (1) from Proposition 2.4 holds often, i.e. we want to find families of:

$$\text{cubic fields } F = \mathbb{Q}(\sqrt[3]{p}) \text{ satisfying } \text{rank}E(F) = 0, \text{ and} \tag{1}$$

$$\text{quadratic fields } K = \mathbb{Q}(\sqrt{d}) \text{ satisfying } \text{rank}E(K) = 1 \tag{2}$$

We use results going back to the work of Brau [1] to find the cubic family for 1, and results of Kriz and Li to find the quadratic family in 2. Proposition 2.4 can then be applied to prove DLC for the composita $\mathbb{Q}(\sqrt[3]{p}, \sqrt{d})$.

For 1, the result based on that of Brau roughly says the following. Denote by ζ_3 a primitive third root of unity.

Lemma 4.1. *([9, Theorem 3.5], building on [1, Proposition 5.2])*
If a list of conditions concerning the behavior of the prime 3 relative to E is satisfied, of which the most important one is that $\text{rank}E(\mathbb{Q}(\zeta_3)) = 0$*, then*

$$\text{rank}E(\mathbb{Q}(\sqrt[3]{p}, \zeta_3)) = \text{rank}E(\mathbb{Q}(\sqrt[3]{p})) = 0$$

for every $p \in \mathcal{P}(E)$, where

$$\mathcal{P}(E) = \{\textit{good reduction primes } p : a_{\mathfrak{p}}(E) \not\equiv 2 \pmod 3, \forall \mathfrak{p} | p \textit{ in } \mathbb{Q}(\zeta_3)\}.$$

The densities $\frac{9}{16}$ in Theorem 3.3 and $\frac{103}{128}$ in Theorem 3.4 come about as follows. Estimating the density of the primes in $\mathcal{P}(E)$ with the indicated $\pmod 3$ condition is the same as estimating the corresponding Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{Q}(E[3])/\mathbb{Q})$. The improvement from the estimate $\frac{5}{16}$ in Theorem 3.1 to $\frac{9}{16}$ in Theorem 3.3 reflects several relaxations on the conditions concerning the prime 3 – in [7], the analogue of the above lemma was slightly weaker, relying on some Iwasawa-theoretic tools. To obtain the much higher density of $\frac{103}{128}$ in Theorem 3.4, we count primes that satisfy the conditions of the lemma for any of the *two* elliptic curves mentioned before: We have $\mathrm{rank} E(\mathbb{Q}(\sqrt[3]{p})) = 0$ for any

$$p \in \mathcal{P}(E557b1) \cup \mathcal{P}(E704d1).$$

For 2, the result of Kriz and Li says the following

Lemma 4.2. *Let $E/\mathbb{Q}$ be an elliptic curve so that $\mathrm{rank} E(\mathbb{Q}) = 0$ (and E has trivial 2-torsion). Let K be an imaginary quadratic field. Put*

$$\mathcal{Q}(K) := \{\textit{primes } q \neq 2 \textit{ of good reduction and split in } K \textit{ so that } a_q \equiv 1 \pmod 2.\}$$

Then under an appropriate condition on a Heegner point (and another condition on the Tamagawa number at 2), we have

- *$\Delta_E < 0$ implies that $\mathrm{rank} E^{(d \times d_K)}(\mathbb{Q}) = 1$, and*
- *$\Delta_E > 0$ and $d < 0$ imply that $\mathrm{rank} E^{(d)}(\mathbb{Q}) = 1$,*

for every d supported on $\mathcal{Q}(K)$, and where Δ_E denotes the discriminant of E.

The densities for $\delta(\mathcal{Q})$ come about when counting the corresponding Frobenius elements $\mathrm{Frob}_q \in \mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q})$ with the desired trace condition. In Theorem 3.1, the density $\frac{1}{12}$ was obtained when applying the above lemma to $K = \mathbb{Q}(\sqrt{-7})$. The density $\frac{7}{48}$ in Theorem 3.3 came about when considering multiple auxiliary imaginary quadratic fields, $\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-79})$, and $\mathbb{Q}(\sqrt{-127})$, resulting in the primes q being allowed to be in the larger set

$$\mathcal{Q}(\mathbb{Q}(\sqrt{-7})) \cup \mathcal{Q}(\mathbb{Q}(\sqrt{-79})) \cup \mathcal{Q}(\mathbb{Q}(\sqrt{-127})).$$

The reason for the much lower density $\frac{1}{36}$ in Theorem 3.4 is that we need the Mordell–Weil ranks of the two elliptic curves to increase under base change simultaneously. Translating this into the conditions of the lemma, this is asking for *simultaneous* conditions for the traces of Frobenius in both elliptic curves, thus cutting down the density.

4.2 An open question

We compare the densities in Theorems 3.1,3.3 and 3.4. We call the set of primes used in constructing the number fields that satisfy DLC simply $\mathcal{P}$ and $\mathcal{Q}$ uniformly.

We summarize the densities from Theorems 3.1, 3.3, 3.4 in the table below:

	Thm 3.1	Thm 3.3	Thm 3.4	"Thm n"	$\lim_{n\to\infty}$ Thm n
$\delta(\mathcal{P})$	$\frac{5}{16}$	$\frac{9}{16}$	$\frac{103}{128}$	$\frac{3^n+4^n}{2^{3n+1}}$	1
$\delta(\mathcal{Q})$	$\frac{1}{12}$	$\frac{7}{48}$	$\frac{1}{36}$	$\frac{1}{4} \times \frac{1}{3^n}$	0

We were able to improve Theorem 3.1 by considering multiple auxiliary quadratic fields. The different densities in Theorem 3.3 and Theorem 3.4 came about because we considered two elliptic curves.

If we extended the methods and found n elliptic curves instead, one should be able to use the methods of Theorem 3.4 to find a "Theorem n," where the densities should transform as shown – in the limit, one could thus prove part of Conjecture 3.2.

Remark 4.3. *The density 0 in the last entry is not too helpful. It seems reasonable to expect that the densities $\delta(\mathcal{Q})$ could be bounded from below, so that in the limit, they should have positive density. We would like to make the following conjecture:*

Conjecture 4.4. *Denote by $\mathcal{Q}$ the set of primes that satisfy the conclusion of Proposition 2.4 simultaneously for n appropriate elliptic curves. Then there is a constant $\delta' > 0$ so that $\delta(\mathcal{Q}) > \delta'$.*

In particular, $\delta' > \frac{1}{4} \times \frac{1}{3^n}$ for sufficiently large n, so that the lower right entry in the table should be improved to δ'.

Acknowledgments. We would like to thank the organizers for a wonderful conference.

5 Appendix

We sketch the ideas behind Matiyasevič's proof, which completes a strategy originally due to M. Davis. A particularly simple scenario that Hilbert had in mind is the family of polynomials in two variables given by

$$x^2 + y^2 - n.$$

A well-known theorem by Fermat furnishes us with Hilbert's desired algorithm when n is prime. In this case, a possible algorithm may be simply:

"Output YES if $n = 2$ or $n = 4k + 1$ for an integer k;

Output NO if $n = 4k + 3$."

Fermat began to give a criterion for composite n as well, see e.g. [8, Exercise 5.3], and one may formulate appropriate algorithms in those cases as well. Using this algorithm, we find that the set of n for which the output would be YES is $\{0, 1, 2, 4, 5, 8, \cdots\}$. (For arbitrary quadratic equations in two variables, an algorithm is due to Gauß, quadratic reciprocity.)

From the wording of Hilbert's problem, it seems that Hilbert was hoping for a general algorithm that would vastly generalize these results of Fermat and Gauß.

However, Matiyasevič proved that such an algorithm does not exist. How does one prove such a theorem? Three ideas played a key role, Diophantine sets, two types of sets coming from algorithms (computable and listable sets), and conjecturing that listable sets are Diophantine.

5.1 Diophantine Sets

Recall that Hilbert's 10th Problem asks for a solution (of a certain type) of a polynomial. The first idea is to turn the problem around, i.e. given a set of integers, are they a solution set for a polynomial?

A concrete example is the set

$$\{0, 1, 2, 4, 5, 8, \cdots\} = \{n \text{ such that } x^2 + y^2 = n \text{ has a solution with } x, y \in \mathbb{Z}\}$$

from above. This is an example of a Diophantine set. The polynomial equation $x^2 + y^2 - n$ is the associated Diophantine equation.

Definition 5.1. *A set S of integers is **Diophantine** if there is a polynomial P with coefficients in $\mathbb{Z}$ (the associated **Diophantine equation**) so that*

$$n \in S \iff P(n, x_1, x_2, \cdots, x_m) = 0 \textit{ has an integral solution } (x_1, \cdots, x_m).$$

5.2 Computable and listable sets

Roughly speaking, computable sets S of integers are the best to process for a computer, while listable sets are "second best."

A set S of integers is **computable** if there is an algorithm that decides which integers are in S and which are not.

By contrast, a set S of integers is **listable** if there is a Turing machine program, or more informally a (mechanical) method inferior to algorithms, that furnishes us the following:

$$n \in S \iff \text{Output is YES.}$$

Note, however, that the program may run arbitrarily long to arrive at the conclusion that $n \in S$.

$$n \notin S \implies \text{Output is NO, or program keeps running forever.}$$

The problem is that while the program is running, we don't know whether $n \in S$.

The set of integers $\{0, 1, 2, 4, 5, 8, \cdots\}$ above is listable. Indeed, we may fix some enumeration of all 3-tuples of integers. Given any such tuple (x, y, z), compute $x^2 + y^2 - n$. If this is $= 0$, put n on the list (n may appear multiple times.)

A similar argument shows that any Diophantine set is listable. It turns out that the set $\{0, 1, 2, 4, 5, 8, \cdots\}$ is in fact computable, but this is not always true: **There is a listable set K that is not computable.**

5.3 Davis's Dream: Listable sets are Diophantine

In the 1930's, Martin Davis began to suspect that any listable set L was Diophantine, i.e. had a Diophantine equation P_L for which it became a Diophantine set. (In our recurring example $L = \{0, 1, 2, 4, 5, 8, \cdots\}$, we would have $P_L = x^2 + y^2 - n$.)

If this were true, there would be a Diophantine equation P_K for the set K from the last sentence of the previous section, so that

$$P_K = 0 \text{ has a solution } (x_1, \cdots, x_m) \in \mathbb{Z}^m \text{ (for given } n \in \mathbb{Z}) \iff n \in K.$$

A consequence would be that given n, there is no algorithm for telling if P_K has a solution in $x_1, \cdots, x_m$ (and n).

The reason for this is that if there were such an algorithm, we could use it to decide if $n \in K$, i.e. K would be computable – but it is not!

5.4 Realization of Davis's dream

Davis couldn't realize their dream. However, Julia Robertson in the 1950's developed techniques shedding light on Diophantine sets which increased in an exponential fashion. In 1960, Robertson collaborated with Hilary Putnam and Martin Davis to show if just one Diophantine equation could be found whose solution increased exponentially, this would imply Davis's dream. An example of a set of numbers that grow exponentially is the set of Virahanka numbers:

$$1, 1, 2 = 1 + 1, 3 = 1 + 2, 5 = 2 + 3, 8 = 3 + 5, 13 = 5 + 8, 21 = 8 + 13, \cdots$$

(Virahanka numbers are also known as Fibonacci numbers.) Matiyasevič found a Diophantine equation whose solutions were (appropriately related to) Virahanka numbers, so that ultimately the following theorem was proved:

Theorem 5.2 (Davis–Putnam–Robinson–Matiyasevič)**.** *Every listable set of integers is Diophantine.*

Corollary 5.3. *Hilbert's* 10*th Problem has a negative solution.*

For further reading which this appendix merely summarizes, see [6] and [3].

References

[1] Julio Brau. Selmer groups of elliptic curves in degree p extensions, 2014. preprint, ArXiv:1401.3304.

[2] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi. Division-ample sets and the Diophantine problem for rings of integers. *J. Théor. Nombres Bordeaux*, 17(3):727–735, 2005.

[3] Martin Davis, Yuri Matijasevič, and Julia Robinson. Hilbert's tenth problem: Diophantine equations: positive aspects of a negative solution. In *Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Northern Illinois Univ., De Kalb, Ill., 1974)*, volume Vol. XXVIII of *Proc. Sympos. Pure Math.*, pages 323–378. (loose erratum). Amer. Math. Soc., Providence, RI, 1976.

[4] Jan Denef. Diophantine sets over algebraic integer rings. II. *Trans. Amer. Math. Soc.*, 257(1):227–236, 1980.

[5] Jan Denef and Leonard Lipshitz. Diophantine sets over some rings of algebraic integers. *J. London Math. Soc.*, 2(3):385–391, 1978.

[6] Keith Devlin. *Mathematics: the new Golden Age*. Penguin Books, New York, 1990.

[7] Natalia Garcia-Fritz and Hector Pasten. Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points. *Math. Ann.*, 377(3-4):989–1013, 2020.

[8] Kazuya Kato, Nobushige Krokawa, and Takeshi Saito. *Suuron I: Fermat no Yume to Ruitairon*. Iwanamishoten, 2005.

[9] Debanjana Kundu, Antonio Lei, and Florian Sprung. Studying Hilbert's 10th problem via explicit elliptic curves. 2022. preprint, ArXiv:2207.07021.

[10] Y. Matijasevic. Enumerable sets are Diophantine. In *Soviet Math. Dokl.*, volume 11, pages 354–358, 1970.

[11] Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert's tenth problem. *Invent. math.*, 181(3):541–575, 2010.

[12] Barry Mazur, Karl Rubin, and Michael Larsen. Diophantine stability. *American J. Mathematics*, 140(3):571–616, 2018.

[13] Barry Mazur, Karl Rubin, and Alexandra Shlapentokh. Defining $\mathbb{Z}$ using unit groups, 2023. preprint, ArXiv:2303.02521.

[14] Thanases Pheidas. Hilbert's tenth problem for a class of rings of algebraic integers. *Proceedings of the American Mathematical Society*, 104(2):611–620, 1988.

[15] Bjorn Poonen. Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers. In *International Algorithmic Number Theory Symposium*, pages 33–42. Springer, 2002.

[16] Anwesh Ray. Remarks on Hilbert's tenth problem and the Iwasawa theory of elliptic curves, 2022. to appear in Bull. Aust. Math. Soc., ArXiv:2206.06296.

[17] Harold N Shapiro and Alexandra Shlapentokh. Diophantine relationships between algebraic number fields. *Commun Pure Appl Math*, 42(8):1113–1122, 1989.

[18] Alexandra Shlapentokh. Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers. *Trans. Amer. Math. Soc.*, 360(7):3541–3555, 2008.

[19] C Videla. Sobre el décimo problema de Hilbert. *Atas da Xa Escola de Algebra, Vitoria, ES, Brasil. Colecao Atas*, 16:95–108, 1989.