Program for the learning workshop "The rank of elliptic curves via additive combinatorics", Okinawa, March 2027

Wataru Kai (Tohoku) Shinichi Kobayashi (Kyushu)
Peter Koymans (Utrecht) Carlo Pagano (Concordia)

November 3, 2026

Contents

1 Dates and venue **1**

2 Objectives **2**

3 Timetable **3**

4 Contents of the elliptic lectures **4**

5 Contents of the additive lectures **6**

6 Contents of the Hilbert 10 lectures **8**

7 Logistics **9**
7.1 Transportation 9
7.2 Visa 9

1 Dates and venue

Dates: 15–19 (Mon–Fri) March 2027

Venue: Okinawa Hotel,[1] Daido 35, Naha, Okinawa, Japan

[1]This workshop will be held within the framework of the RIMS Satellite Seminar series. Consequently, registration is mandatory and the participants (except for locals) are required to stay at the venue hotel.

2 Objectives

The objective of this learn-by-doing workshop is to understand the following recent work of Koymans and Pagano:

Theorem 1 ([KP25], also independently [Zyw25]) *For every number field K, there exists an elliptic curve E over K such that* $\operatorname{rank} E(K) = 1$.

A new ingredient in their work is an additive combinatorics result [Kai23] about simultaneous prime values of degree 1 polynomials in number fields, extending a theorem of Green, Tao and Ziegler for $\mathbb{Q}$. We also explore this topic.

The same type of techniques can be used to show the following extended negative answer to Hilbert's 10th Problem. Let $\mathcal{O}_K$ be the ring of integers of K.

Theorem 2 ([KP24], also independently [ABHS25], [Zyw25]) *There is no algorithm whose input is a polynomial $f \in \mathcal{O}_K[x_1, \ldots, x_d]$ with an arbitrary number of variables, and whose output is* **yes** *or* **no** *depending on whether the equation $f(x_1, \ldots, x_d) = 0$ has a solution in $\mathcal{O}_K$.*

References for this section

[KP25] Peter Koymans and Carlo Pagano, "Elliptic curves of rank one over number fields," arXiv:2505.16910 [math.NT], 2025. `https://arxiv.org/abs/2505.16910`

[Zyw25] David Zywina, "Rank one elliptic curves and rank stability," arXiv:2505.16960 [math.NT], 2025. `https://arxiv.org/abs/2505.16960`

[Kai23] Wataru Kai, "Linear patterns of prime elements in number fields," 2023. `https://arxiv.org/abs/2306.16983`

[ABHS25] Levent Alpöge, Manjul Bhargava, Wei Ho, Ari Shnidman, "Rank stability in quadratic extensions and Hilbert's tenth problem for the ring of integers of a number field", Invent. math. 243, 1129–1139 (2026). `https://link.springer.com/article/10.1007/s00222-025-01392-3`

3 Timetable

[Monday]

Elliptic 1: overview, Galois cohomology
Additive 1: overview, von Mangoldt functions

Elliptic 2: 2-descent
Additive 2: classical applications of Fourier
Hilbert's Tenth 1: Diophantine sets

[Tuesday]

Additive 3: Gowers norms
Elliptic 3: Selmer ranks as a transition process

Elliptic 4: first reduction step
Additive 4: Mitsui and Vaughan

[Wednesday]

Additive 5: orthogonality
Hilbert's Tenth 2: propagating negative answers

Free discussion

[Thursday]

Elliptic 5: additive combinatorics I
Elliptic 6: additive combinatorics II

Elliptic 7: auxiliary twisting I
Elliptic 8: auxiliary twisting II

[Friday]

Hilbert's Tenth 3: construction of rank-stable elliptic curves
Research talk / bonus lecture (possibly)

Free discussion / departure

4 Contents of the elliptic lectures

1. Background on Galois cohomology

This lecture has two parts. In part 1, state Corollary 1.1 and Theorem 1.3 of [KP25] and give high-level overview of the proof.

In part 2, several background results on Galois cohomology will be recalled without proof. Important ingredients are:

- Bijection between $\mathrm{Hom}(G_K, \mathbb{F}_2)$ and K^*/K^{*2} (Kummer theory).
- Quadratic Hilbert symbols (locally and globally), and Hilbert reciprocity.

Note: we can give specific references for Kummer theory/Hilbert symbols if needed, but all required background material can already be found on wikipedia:

- `https://en.wikipedia.org/wiki/Kummer_theory`
- `https://en.wikipedia.org/wiki/Hilbert_symbol`

2. Background on elliptic curves

Give a full proof of 2-descent (following Proposition X.1.4 of Silverman's "arithmetic of elliptic curves" [Silv]). The last part about (b_1, b_2) should be skipped.

Also cover the first page of Section X.4 of Silverman for the isogeny ϕ given by multiplication by 2 (i.e. the standard commutative diagram defining the n-Selmer group).

Note: If time allows, prove Lemma 3.2 of [KP24].

3. Selmer ranks as a transition process

Cover Section 4 of [KP24]. The most important result is Lemma 4.7, and should be given in some detail using the results 4.1–4.6, which can be covered in much less (or even no) detail.

Note: In particular, proofs of Proposition 4.1 and 4.6 can be skipped if not enough time, but statements should at least be given. Sketch the proof of Lemma 4.9, most important ingredient is that the final step is +2 because of 2-torsion of elliptic curve.

4. First reduction step

Give proof of Lemma 2.7.

Give Definition 3.2 of [KP25] (to motivate this definition: emphasize that (P1)-(P4) are a series of conditions that exactly combine to give rank 1 elliptic curves) and give full proof of Theorem 3.3.

Construct $\lambda_1, \ldots, \lambda_5$ (i.e. until bottom of page 12 of [KP25]).

5. Main additive combinatorics step part I

Spend 5 minutes on recalling Kai's theorem (as in [KP24, Theorem A.7]).

Follow the part of [KP25] "Construction of linear forms".

Follow the part of [KP25] "Construction of a convex region".

Note: Give statement of Lemma 3.7 but may skip proof if short on time.

6. Main additive combinatorics step part II

Finish the proof of [KP25] Theorem 3.5 (i.e. all material after Lemma 3.7).

7. Auxiliary twisting part I

Proof of [KP25] Theorem 3.9 until the bottom of page 22.

8. Auxiliary twist part II

Finish proof of [KP25] Theorem 3.9 (page 23-27).

9. Other applications: Zywina's theorem and/or Hilbert10

Bonus lecture, which may become a research lecture on some different topic as well.

Comments

A few comments are in place:

- Carlo and Peter are happy to talk to each individual speaker to give more concrete suggestions/feedback, and we are also happy to give a talk in case no speaker can be found (this may especially be useful as some of the talks follow up on another talk, and might thus be a bit more difficult to prepare for).

- One important ingredient in the rank one paper is Section 4 of our Hilbert 10 paper [KP24] (no further ingredients will be required from this paper, except Lemma 3.2, which is completely elementary).

References for the elliptic curve lectures

[KP24] Peter Koymans and Carlo Pagano, "Hilbert's tenth problem via additive combinatorics," arXiv:2412.01768v3 [math.NT], 2025. `https://arxiv.org/abs/2412.01768`

[KP25] Peter Koymans and Carlo Pagano, "Elliptic curves of rank one over number fields," arXiv:2505.16910 [math.NT], 2025. `https://arxiv.org/abs/2505.16910`

[Silv] Joseph H. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Mathematics 106, Springer, 1986; 2nd edition with corrections 2016. `https://link.springer.com/book/10.1007/978-0-387-09494-6`

5 Contents of the additive lectures

1. Overview

Give a high-level overview of the proof of [Kai23, Theorem 1.1] roughly following [Kai23, Section 2]. Define the von Mangoldt function and its Cramer model along the way.

REFERENCES: [Kai23]. See [Green-Tao] and [Tao-Teravainen] for the case of $\mathbb{Z}$.

NOTE. In this workshop, due to time constraints, let's ignore the Siegel model.

2. Classical use of Fourier analysis

To motivate higher order Fourier analysis, it would be nice to review how classical Fourier analysis was used in additive combinatorics. Sketch the proof of Roth's theorem (3-term Szemerédi theorem) using classical Fourier analysis.

REFERENCES: [Tao, Section 1.2 "Roth's theorem"] or [Green, Lecture 1].

3. Gowers norms, nilsequences

Define the notions of Gowers norms and s-step nilsequences. State the generalized von Neumann theorem ([Green-Tao, Proposition 7.1] or [Kai23, Appendix F]) and the Inverse Theorem of Gowers Norms [LSS, Theorem 1.2]. These reduce the problem to showing that the difference between the von Mangoldt function and its model is asymptotically orthogonal to nilsequences.

If time permits, state some of the basic properties such as: Gowers U^2 norm is captured by Fourier coefficients; a lower bound on the correlation with an s-step nilsequence gives a lower bound of the Gowers U^{s+1} norm (= easy converse to Inverse Theorem); thanks to the von Neumann theorem, the U^{s+1} norm can be used to study complexity s linear configurations such as $(s+2)$-term arithmetic progressions; ...

REFERENCES: primarily [Tao, Section 1.3 "Linear patterns" and Section 1.6.1 "General theory of polynomial maps"] and [Green-Tao, Appendices B, E]; good summaries can also be found in [Leng], [LSS].

4. Mitsui and Vaughan

Explain that Mitsui's Prime Number Theorem implies the asymptotic orthogonality against the *constant* nilsequence [Kai23, Sections 6, 9]. Then explain the Vaughan decomposition (also known by the phrase "Type I/II sums") of the von Mangoldt function following [Kai23, Section 8].

REFERENCES: In addition to the above, [Tao-Teräväinen, Section 7].

NOTE: Let's ignore the difference between the Siegel/Cramer models, and the "negligible sum" in the Vaughan decomposition.

5. Asymptotic orthogonality

Sketch the proof of the fact that Type I sums are asymptotically orthogonal to nilsequences [Kai23, Section 10].[2] Don't try to present too much detail because you will not have enough time.

NOTE: The case of Type II sums [Kai23, Section 11] will be skipped in this workshop due to time constraints.

Comments

If you are the speaker of one of these lectures, Wataru is happy to help you (or please help Wataru clarify/modify the specifications of the lectures).

References for the additive lectures

[Green] Ben Green, "Nilsequences," Lectures at IHES, 2014. https://youtube.com/playlist?list=PLx5f8IelFRgEWvDoOWpvmXwcTY9mCGF4i or https://www.carmin.tv/en/collections/ben-green-nilsequences

[Tao] Terence Tao, "Higher Order Fourier Analysis." https://terrytao.wordpress.com/books/higher-order-fourier-analysis/

[Green-Tao] Ben Green and Terence Tao, "Linear equations in primes," Annals of Mathematics, 2010. https://annals.math.princeton.edu/2010/171-3/p08

[Tao-Teräväinen] Terence Tao and Joni Teräväinen, "Quantitative bounds for Gowers uniformity of the Möbius and von Mangoldt functions," Journal of the European Mathematical Society, 2023. https://ems.press/journals/jems/articles/13625437

[Kai25] Wataru Kai, "Notes on Mitsui's Prime Number Theorem with Siegel zeros," Version 4, 2025. https://arxiv.org/abs/2209.11816v4

[Kai23] Wataru Kai, "Linear patterns of prime elements in number fields," 2023. https://arxiv.org/abs/2306.16983

[Leng] James Leng, "Efficient Equidistribution of Nilsequences," arXiv:2312.10772 [math.NT], 2024. https://arxiv.org/abs/2312.10772

[LSS] James Leng, Ashwin Sah, and Mehtaab Sawhney, "Quasipolynomial bounds on the Inverse Theorem for the Gowers $U^{s+1}[N]$-norm," 2024. http://arxiv.org/abs/2402.17994v3

[Mitsui] Takayoshi Mitsui, "Generalized prime number theorem," Japanese Journal of Mathematics, 1957. https://www.jstage.jst.go.jp/article/jjm1924/26/0/26_0_1/_article/-char/ja/

[2] More precisely: If a Type I sum has non-trivial correlation with a nilsequence, then this bias can be used to construct a nilsequence with similar properties and strictly smaller *step*, enabling the proof by induction on the integer parameter *step*.

6 Contents of the Hilbert 10 lectures

1. Diophantine sets

The task is to convince the audience that if $\mathbb{Z}$ is a *diophantine* subset of $\mathcal{O}_K$, then a negative answer to Hilbert's 10th Problem with $\mathcal{O}_K$-coefficients will follow.

Define what it means for a subset of $\mathbb{Z}^n$ (or of $\mathcal{O}_K^n$) to be:

- recursive;
- listable (= recursively enumerable), or;
- diophantine.

Time permitting, show some basic properties of diophantine subsets such as the stability under union and intersection.

State (but do not prove) the MRDP theorem saying that listable subsets and diophantine subsets in $\mathbb{Z}^n$ coincide, and explain why this implies the negative answer to Hilbert 10 with $\mathbb{Z}$-coefficients.

REFERENCES: The main reference is [Po03] and references therein. See [BhPo25] for a clean general theory of diophantine subsets in R^n, where R is (say) an integral domain.

[Po03] Bjorn Poonen, "Hilbert's Tenth Problem over rings of number-theoretic interest." Notes from Arizona Winter School 2003. `https://math.mit.edu/~poonen/papers/aws2003.pdf`

Videos available on YouTube `https://youtu.be/mg6BWybKbQU`

or on the Winter School's page `https://swc-math.github.io/aws/2003/notes.html`

[BhPo25] Bhargav Bhatt and Bjorn Poonen, "Diophantine sets." `https://arxiv.org/abs/2511.18101`

2. Propagating negative answers

Explain Poonen's theorem:

> Let L/K be an extension of number fields. If there is an elliptic curve E over K such that $1 = \operatorname{rank} E(K) = \operatorname{rank} E(L)$, then $\mathcal{O}_K$ is diophantine inside $\mathcal{O}_L$.

The original account is [Po02]. A more modern and simplified proof is [Po25] (recommended).

Time permitting, explain Shlapentokh's reduction argument: in order to prove $\mathbb{Z} \subset \mathcal{O}_F$ is diophantine for *all* number fields F, it suffices to show $\mathcal{O}_K \subset \mathcal{O}_L$ is diophantine only for *quadratic extensions* L/K (reduction to the case of F totally real (Denef 1980)).

[Po02] Bjorn Poonen, "Using elliptic curves of rank one towards the undecidability of Hilbert's Tenth Problem over rings of algebraic integers." https://arxiv.org/abs/math/0204001

[Po25] Bjorn Poonen, "Rank stability makes rings of integers diophantine." https://arxiv.org/abs/2510.19553

Videos available at https://www.mathematics.uni-bonn.de/him/video-recordings/tp_2025_03_school/definability_decidability_computability

3. Construction of rank-stable elliptic curves

Give a sketch of Koymans–Pagano's construction [KP24]. You may assume that the audience is already familiar with the construction of rank-1 elliptic curves from [KP25].

Alternatively, present Zywina's construction in [Zyw25].

7 Logistics

7.1 Transportation

The venue is 7 minuts walk from the monorail Asato station. You can take the monorail from Naha Airport (code: OKA).

There are direct flights to Naha from many major cities in East Asia.

7.2 Visa

The list of 74 visa-exempt countries and regions can be found here: https://www.mofa.go.jp/j_info/visit/visa/short/novisa.html

General information about visas to Japan: https://www.mofa.go.jp/j_info/visit/visa/index.html