Application of additive combinatorics

Hilbert's tenth problem over rings of integers of number fields [1]

David Kurniadi Angdinata

London School of Geometry and Number Theory

Wednesday, 18 June 2025

[1] Koymans and Pagano (2025) Hilbert's tenth problem via additive combinatorics

Notation

K a number field of degree n, such that $r := \#V_K^{\mathbb{R}} \geq 32$

E an elliptic curve $y^2 = (x - a_1)(x - a_2)(x - a_3)$ over K of root number 1, such that $-1, a_1 - a_2, a_1 - a_3, a_2 - a_3 \in K^\times$ are linearly independent as elements of $K^\times/(K^\times)^2$

T a finite set of places of K that includes the 2-adic primes, the 3-adic primes, the primes of bad reduction for E, and the archimedean places, such that $[K(T) : K(V_K^{\mathbb{R}})] \geq 2^r$

τ_ℓ six places in $V_K^{\mathbb{R}}$, such that

$$\begin{aligned}
&\tau_1(a_3) > \tau_1(a_1) > \tau_1(a_2), \qquad &&\tau_2(a_3) > \tau_2(a_2) > \tau_2(a_1),\\
&\tau_3(a_1) > \tau_3(a_3) > \tau_3(a_2), \qquad &&\tau_4(a_2) > \tau_4(a_3) > \tau_4(a_1),\\
&\tau_5(a_3) > \tau_5(a_1) > \tau_5(a_2), \qquad &&\tau_6(a_3) > \tau_6(a_2) > \tau_6(a_1)
\end{aligned}$$

A suitable twist

Recall that $t \in K^\times/(K^\times)^2$ is a **suitable twist** if it satisfies the following.

- P1 The quadratic character ψ_t is trivial at the places in T.
- P2 There is some $\kappa \in K^\times/(K^\times)^2$ whose quadratic character ψ_κ is ramified at some primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ of K and satisfies

$$\psi_t = \psi_\kappa + \psi_{q_1} + \psi_{q_2} + \psi_{q_3} + \psi_{q_4},$$

  for some primes q_1, q_2, q_3, q_4 of K not in $T' := T \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$.
- P3 There is a basis $(z_1, z_2), \ldots, (z_{11}, z_{12})$ of $\mathrm{Sel}_{\mathcal{L}_{s,t}}(K, E[2])$ such that

$$\prod_{v \in T'} (z_i, q_j)_v = \begin{cases} -1 & \text{if } (i,j) = (1,1), (5,2), (9,3), \\ & \qquad (4,1), (8,2), (12,3), \\ 1 & \text{otherwise.} \end{cases}$$

- P4 The rank of $E^{-t}(K)$ is positive.

Given a suitable twist t, the ranks of $E^t(K)$ and $E^t(K(i))$ can be shown to be equal and positive, which proves that $\mathcal{O}_K$ is Diophantine over $\mathcal{O}_{K(i)}$.

An auxiliary twist

It turns out that constructing a suitable twist reduces to constructing an **auxiliary twist** $\kappa \in K^\times/(K^\times)^2$ satisfying the following.

K1 The quadratic character ψ_κ is

- a unit at the 2-adic primes of K,
- unramified at the odd primes in T, and
- trivial at τ_1, τ_2, τ_3 and non-trivial at τ_4, τ_5, τ_6.

K2 There is a basis $(z_1, z_2), \ldots, (z_{11}, z_{12})$ of $\mathrm{Sel}_{\mathcal{L}_{s,\pi}}(K, E[2])$ such that

$$\mathrm{sgn}(\tau_\ell(z_i)) = \begin{cases} - & \text{if } (i,\ell) = (1,1),(5,3),(9,5), \\ & \qquad\quad (4,2),(8,4),(12,6), \\ + & \text{otherwise,} \end{cases}$$

for some tuple $\pi = (\pi_1, \ldots, \pi_s)$ of primes of K.

Given an auxiliary twist κ, a generalisation of the Green–Tao theorem by Kai says that a generic family of polynomials $L_j(X, Y) \in \mathcal{O}_K[X, Y]$ admits simultaneously prime values q_j that satisfy certain congruence conditions. Then $\kappa \prod_j q_j$ will turn out to be a suitable twist.

The four bivariate polynomials

Let $m \in \mathcal{O}_K$ be a generator of the ideal

$$8 \prod_{\mathfrak{p} \in T \text{ odd}} \mathfrak{p}^{\#\mathrm{Cl}(K)}.$$

Assume that $\kappa \in \mathcal{O}_K$ is coprime to m, which is possible by K1 and strong approximation. Let $\lambda \in \mathcal{O}_K$ be an inverse of κ modulo m coprime to κ.

Let $c(X) := m^2\kappa X + 1$ and $d(Y) := m^2\kappa(m^2\kappa Y + \lambda)$, and define

$$L_1(X, Y) := c(X) + a_1 d(Y), \qquad L_2(X, Y) := c(X) + a_2 d(Y),$$

$$L_3(X, Y) := c(X) + a_3 d(Y), \qquad L_4(X, Y) := d(Y)/m^2\kappa.$$

Kai's theorem will give infinitely many quadruples (q_1, q_2, q_3, q_4) of primes of K such that $L_j(x, y) = q_j$ for each $j = 1, 2, 3, 4$ for some $x, y \in \mathcal{O}_K$, so that $t := \kappa q_1 q_2 q_3 q_4$ clearly satisfies P2.

Point of infinite order

For t to satisfy P4, observe that E^{-t} is given by

$$-(c + a_1 d)(c + a_2 d)(c + a_3 d)\frac{dy^2}{m^2} = (x - a_1)(x - a_2)(x - a_3),$$

for some $c, d \in \mathcal{O}_K$, which always has a rational point

$$P_t := \left(-\frac{c}{d}, \frac{m}{d^2}\right).$$

It then suffices to show that P_t is almost always non-torsion.

Lemma (3.2)

For all but finitely many $d \in K^\times/(K^\times)^2$,

$$E^d(K)_{\text{tor}} = \{\mathcal{O}, (a_1, 0), (a_2, 0), (a_3, 0)\}.$$

Proof.

If $E^d(K)[p]$ is non-trivial for some prime $p > 2$, then $\overline{\rho}_{E,p}$ factors through the quadratic character ψ_d, but $\overline{\rho}_{E,p}$ is almost always irreducible. □

Signs for the polynomials

For t to satisfy P1 and P3, q_j need to satisfy additional conditions at the real places $\sigma \in T$, obtained from enforcing the signs

$$\operatorname{sgn}(\sigma(L_j(X,Y))) = \begin{cases} - & \text{if } j = 1 \text{ and } \sigma = \tau_1, \tau_2, \\ & \quad j = 2 \text{ and } \sigma = \tau_1, \tau_2, \tau_3, \tau_4, \\ & \quad j = 3 \text{ and } \sigma = \tau_3, \tau_5, \tau_6, \\ \operatorname{sgn}(\sigma(\kappa)) & \text{if } j = 4 \text{ and } \sigma \neq \tau_1, \ldots, \tau_6, \\ + & \text{otherwise.} \end{cases}$$

Along with K1, these conditions force t to be trivial at σ.

- If $\ell = 1, 2, 3$, then $\tau_\ell(q_1 q_2 q_3) > 0$, $\tau_\ell(q_4) > 0$, and $\tau_\ell(\kappa) > 0$.
- If $\ell = 4, 5, 6$, then $\tau_\ell(q_1 q_2 q_3) < 0$, $\tau_\ell(q_4) > 0$, and $\tau_\ell(\kappa) < 0$.
- Otherwise, $\sigma(q_1 q_2 q_3) > 0$ and $\sigma(q_4 \kappa) > 0$.

Furthermore, $q_1 \equiv q_2 \equiv q_3 \equiv 1 \mod m\kappa$ and $q_4\kappa \equiv \lambda\kappa \equiv 1 \mod m$, so that t is trivial at the primes in T, and hence t satisfies P1.

Computation of Hilbert symbols

Finally, since $\sigma(q_1), \sigma(q_2), \sigma(q_3) > 0$ at the real places $\sigma \neq \tau_1, \ldots, \tau_6$ and since $q_1 \equiv q_2 \equiv q_3 \equiv 1 \mod m\kappa$,

$$(z_i, q_j)_v = 1, \qquad i = 1, \ldots, 12, \qquad j = 1, 2, 3,$$

for the places $v \in T' \setminus \{\tau_1, \ldots, \tau_6\}$, so that

$$\prod_{v \in T'} (z_i, q_j)_v = \prod_{\ell=1}^{6} (z_i, q_j)_{\tau_\ell}, \qquad i = 1, \ldots, 12, \qquad j = 1, 2, 3.$$

Now $(z_i, q_j)_{\tau_\ell} = -1$ precisely if $\tau_\ell(z_i), \tau_\ell(q_j) < 0$, which occur when

$$(i, j, \ell) = (1, 1, 1), (1, 2, 1), (4, 1, 2), (4, 2, 2), (5, 2, 3), (5, 3, 3), (8, 2, 4), (9, 3, 5), (12, 3, 6).$$

These are precisely the Hilbert symbol conditions enforced in P3, noting that it does not enforce conditions for $(i, j) = (1, 2), (4, 2), (5, 3)$.

Admissibility of the polynomials

Observe that $L_j(X, Y)$ form an admissible family, in the sense that they satisfy the analogue of Bunyakovsky's property in Dickson's conjecture.

Lemma (5.5)

For any prime $\mathfrak{p}$ of K, there are $x, y \in \mathcal{O}_K$ such that

$$\mathfrak{p} \nmid L_1(x, y)L_2(x, y)L_3(x, y)L_4(x, y).$$

Proof.

If $\mathfrak{p} \mid m\kappa$, then $L_1(0, 0) = L_2(0, 0) = L_3(0, 0) = 1$, and $L_4(0, 0) = \lambda$ is coprime to $m\kappa$. Otherwise $\mathfrak{p} \nmid m\kappa$, then there is some $y \in \mathcal{O}_K$ such that $\mathfrak{p} \nmid m^2\kappa y + \lambda$, so that $\mathfrak{p} \nmid L_4(x, y)$ for any $x \in \mathcal{O}_K$. On the other hand, $\#(\mathcal{O}_K/\mathfrak{p}) \geq 5$ since $\mathfrak{p} \nmid 6$, so that there is some $x \in \mathcal{O}_K$ such that

$$x \not\equiv \frac{-a_1 d(y) - 1}{m^2\kappa}, \frac{-a_2 d(y) - 1}{m^2\kappa}, \frac{-a_3 d(y) - 1}{m^2\kappa} \mod \mathfrak{p},$$

and hence $\mathfrak{p} \nmid L_1(x, y)L_2(x, y)L_3(x, y)$. □

Statement of Kai's theorem

A version of Kai's theorem can be stated as follows.

Theorem (A.8)

Let $\phi_1, \dots, \phi_k : \mathbb{Z}^d \to \mathcal{O}_K$ be affine linear forms for some $d \in \mathbb{N}_{>1}$ such that the restriction of ϕ_j to the kernel of $\phi_{j'}$ has finite cokernel whenever $j \neq j'$, and let $\Omega \subseteq \mathbb{R}^d$ be a convex region such that the volume of $\Omega_N := \Omega \cap [-N, N]^d$ is asymptotically N^d. Then

$$\sum_{\vec{x} \in \Omega_N \cap \mathbb{Z}^d} \prod_{j=1}^{k} \Lambda_K(\phi_j(\vec{x})) \sim \frac{N^d}{\operatorname{res}_{s=1} \zeta_K(s)^k} \cdot \prod_p \beta_p,$$

where $\Lambda_K := \Lambda \circ \mathrm{Nm}_{K/\mathbb{Q}}$ is the von Mangoldt function for K and

$$\beta_p := \left(\frac{p^n}{\#(\mathcal{O}_K/(p))^\times} \right)^k \cdot \frac{\#\{\vec{x} \in \mathbb{F}_p^d : \mathfrak{p} \nmid \prod_{j=1}^k \phi_j(\vec{x}) \text{ for all } \mathfrak{p} \mid p\}}{p^d}.$$

Note that the full version considers affine linear forms $\mathbb{Z}^d \to I$ with a uniformity condition over all fractional ideals I of K.

Assumptions in Kai's theorem

For each $j = 1, 2, 3, 4$, the 1-homogeneous part of $L_j(X, Y)$ defines an affine linear form $\phi_j : \mathbb{Z}^{2n} \to \mathcal{O}_K$ by fixing a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. If $j \neq j'$, then $\phi_j(\vec{x}, \vec{y}) = 0$ implies that $\phi_{j'}(\vec{x}, \vec{y}) \not\equiv 0$ since $a_j \neq a_{j'}$, or in other words that the restriction of ϕ_j to the kernel of $\phi_{j'}$ has finite cokernel.

The signs enforced on $\sigma(L_j(X, Y))$ define a convex region $\Omega \subseteq \mathbb{R}^{2n}$.

Lemma (5.6, 5.7)

The volume of Ω_N is asymptotically N^{2n}.

Sketch of proof.

For a surjective linear operator $T : \mathbb{R}^{2n} \to \mathbb{R}^{2r}$, the volume of

$$T^{-1}\left(\prod_{\ell=1}^{2r}(x_\ell, \infty)\right) \cap [-N, N]^{2n}, \qquad (x_1, \ldots, x_{2r}) \in \mathbb{R}^{2r}$$

is asymptotically N^{2n}. While Ω is defined by $4r$ embeddings, the signs enforced on $\sigma(L_j(X, Y))$ and $\sigma(a_j)$ reduce this to $2r$ embeddings. □

Intuition for Kai's theorem

Assume now that the coefficients of $\phi_j : \mathbb{Z}^d \to \mathcal{O}_K$ are fixed. If $\phi_j(\vec{x})$ is prime for some $\vec{x} \in \Omega_N \cap \mathbb{Z}^d$, then $\Lambda_K(\phi_j(\vec{x})) \sim \log dN$, since composite prime powers are asymptotically negligible compared to primes. Thus

$$\sum_{\vec{x} \in \Omega_N \cap \mathbb{Z}^d} \prod_{j=1}^{k} \Lambda_K(\phi_j(\vec{x})) \sim \#S_N \cdot \log^k dN,$$

where S_N is the set of $\vec{x} \in \Omega_N \cap \mathbb{Z}^d$ such that $\phi_1(\vec{x}), \ldots, \phi_r(\vec{x})$ are simultaneously prime. Kai's theorem then says $\#S_N > 0$ whenever $\prod_p \beta_p > 0$, which is equivalent to the admissibility of ϕ_j.

Note that when $K = \mathbb{Q}$, this says that

$$\#S_N \sim \frac{N^d}{\log^k dN} \cdot \prod_p \left(\frac{p}{p-1}\right)^k \cdot \frac{\#\{\vec{x} \in \mathbb{F}_p^d : p \nmid \prod_{j=1}^k \phi_j(\vec{x})\}}{p^d},$$

which is simply a multivariate version of the Hardy–Littlewood conjecture.