Hilbert’s tenth problem: How additive combinatorics comes into play

J'ignore • 13 Jul 2025

Continuing the previous post, we would like to sketch out how additive combinatorics helps us to solve Hilbert’s tenth problem for rings of integers $\mathcal{O}_K$ of general number fields. As explained previously, We are reduced to showing existence of a certain elliptic curve E with whose group of rational points has positive rank but doesn’t grow under a fixed finite extensions K/F of number fields. In fact, we can further relax it as follows:

> (MRS24, Theorem 3.1 and 4.8) If for every quadratic extension K/F of number fields, there exists an abelian variety A/F such that $rkA(F) = rkA(K) > 0$, then Hilbert’s tenth problem has a negative solution for the ring of integers of every number field.

This strengthening is needed for the proof in [ABHS] but not for the one in [KP]. We will present the former proof since it is shorter, but for the latter, there are great expositions by the authurs in the recorded talks L1 and L2.

WLOG by taking Weil restriction we can assume F contains a primitive l-th root of unity for some odd prime l to be chosen. The main player is the hyperelliptic curve $y^2 = x^l + 1$ of genus $\frac{l-1}{2}$. For $n \in F^\times$, let C_n denotes the twist $y^2 = x^l + n$. Note that for any $\lambda \in F^\times$, C_n and $C_{n\lambda^{2l}}$ are isomorphic over F. There is a natural isomorphism of μ_l on C_n, hence on its Jacobian J_n.

For a quadratic extension $K = F(\sqrt{q})$, the K-quadratic twist C_n^K of C_n is the curve $qy^2 = x^l + n$, which is isomorphic to $C_{q^l n}$ over K, similarly $J_n^K \cong J_{q^l n}$. We also have μ_l-twists C_{nr^2} for $r \in F^\times$, as C_{nr^2} is isomorphic to C_n over $F(r^{1/l})$.

Since we have an injection $\mathbb{Z}[\zeta] \hookrightarrow \mathrm{End}(J_n)$, we can view $1 - \zeta$ as a self-isogeny ϕ of J_n of degree l and study its Selmer group $\mathrm{Sel}_\phi(J_n)$ (analogous to ususal Selmer group). In particular, from the long exact sequence induced from the short exact sequence

$$0 \to J_n[\phi] \to J_n \xrightarrow{\phi} J_n \to 0$$

we have that $rk_{\mathbb{Z}[\zeta]} J_n(F) \leq \dim_{\mathbb{F}_l} \mathrm{Sel}_\phi(J_n)$.

The key realization is that we can find a large set of primes $\mathfrak{p}$ of F such that the local conditions they impose on the ϕ-Selmer group is vacuous, in the sense that $T_{\mathfrak{p}} := H^1(F_{\mathfrak{p}}, J_n[\phi]) = 0$. (Recall that $Sel_\phi(J_n) = ker(T \to \prod T_{\mathfrak{p}}/W_{\mathfrak{p}})$ where $T := H^1(F, J_n[\phi])$ and $W_{\mathfrak{p}}$ is the image of the boundary map $J_n(F_{\mathfrak{p}}) \to T_{\mathfrak{p}}$.) This set of primes consists of those that are coprime to l and remain inert or ramify in $F(\sqrt{n})/F$, by the following lemma.

> Suppose $\mathfrak{p} \nmid \ell$ is inert or ramified in $F(\sqrt{n})/F$. Then $T_{\mathfrak{p}} = 0$.

Proof: Since F contains μ_ℓ, we see that the galois module $J_n[\phi]$ is isomorphic to its own Cartier dual. Hence, local Tate duality gives $H^2(F_{\mathfrak{p}}, J_n[\phi]) \cong H^0(F_{\mathfrak{p}}, J_n[\phi])$, and the local Euler characteristic formula reads $\#T_{\mathfrak{p}} = \#H^0(F_{\mathfrak{p}}, J_n[\phi]) \cdot \#H^2(F_{\mathfrak{p}}, J_n[\phi]) = (\#J_n[\phi](F_{\mathfrak{p}}))^2 = 1$. The last equality follows because $\sqrt{n} \notin F_{\mathfrak{p}}$.

The starting point is a result by Yu that enables us to use μ_l-twist to produce curves with zero Selmer group (and thus the group of rational points is of rank zero):

> There exists $r \in \mathcal{O}_F$ such that $\mathrm{Sel}_\phi(J_{q^l r^2}) = 0$. Moreover, we can choose r such that $r \notin \mathfrak{p}$ for all primes $\mathfrak{p}$ that ramify in K.

The next result shows that if we further twist by Σ-units where Σ is essentially (up to finitely many primes) the set of silent primes, the ϕ-Selmer rank stays unchanged.

> There is a subset of primes Σ which is the union of the set of silent primes S_{inert} with a finite set of primes S such that if $t \in \mathcal{O}_{F,\Sigma}^\times$ and $t \in F_{\mathfrak{p}}^{\times l}$ for all $\mathfrak{p} \in S$, then $Sel_\phi(J_{q^l r^2 t^2}) = 0$.

The idea is that both Selmer groups $Sel_\phi(J_{q^l r^2})$ and $Sel_\phi(J_{q^l r^2 t^2})$ can be viewed as living inside the common ambient space $T := H^1(F, J_{q^l}[\phi])$ since $F(\sqrt{q^l r^2}) = F(\sqrt{q^l}) \Rightarrow J_{q^l}[\phi] \cong J_{q^l r^2}[\phi]$. It remains to show that their corresponding local conditions $W_{\mathfrak{p}}$ are equal inside $T_{\mathfrak{p}}$ for all primes $\mathfrak{p}$. If $\mathfrak{p} \in S$, this is because the two curves are isomorphic over $F_{\mathfrak{p}}$. Otherwise, if $\mathfrak{p}$ is inert or ramified in K, then $T_{\mathfrak{p}} = 0$ by the above lemma.