

Effectivity in Faltings' Theorem.

Levent Alpoge

Diophantus, may your soul be with Satan because of the difficulty of the other theorems of yours, and in particular of the present theorem. — Chortasmenos, ~ 1400.

Diophantus, may your soul be with Satan because of the difficulty of the other theorems of yours, and in particular of the present theorem. — Chortasmenos, ~ 1400 .

Theorem (Faltings).

Let K/\mathbb{Q} be a number field. Let C/K be a smooth projective hyperbolic curve. Then: $C(K)$ is finite.

Diophantus, may your soul be with Satan because of the difficulty of the other theorems of yours, and in particular of the present theorem. — Chortasmenos, ~ 1400 .

Theorem (Faltings).

Let K/\mathbb{Q} be a number field. Let C/K be a smooth projective hyperbolic curve. Then: $C(K)$ is finite.

- Obviously, we'd like to actually find $C(K)$ given C/K ,

Diophantus, may your soul be with Satan because of the difficulty of the other theorems of yours, and in particular of the present theorem. — Chortasmenos, ~ 1400 .

Theorem (Faltings).

Let K/\mathbb{Q} be a number field. Let C/K be a smooth projective hyperbolic curve. Then: $C(K)$ is finite.

- ▶ Obviously, we'd like to actually find $C(K)$ given C/K , i.e. produce a finite-time algorithm computing $(C, K) \mapsto C(K)$.

Theorem (A.-Lawrence).

*There is an algorithm that, on input (C, K) with K/\mathbb{Q} a number field and C/K a smooth projective hyperbolic curve, outputs $C(K)$ **if it terminates**.*

Theorem (A.-Lawrence).

*There is an algorithm that, on input (C, K) with K/\mathbb{Q} a number field and C/K a smooth projective hyperbolic curve, outputs $C(K)$ **if it terminates**. Assuming the Fontaine-Mazur, Grothendieck-Serre, Hodge, and Tate conjectures, this algorithm always terminates.*

Theorem (A.-Lawrence).

*There is an algorithm that, on input (C, K) with K/\mathbb{Q} a number field and C/K a smooth projective hyperbolic curve, outputs $C(K)$ **if it terminates**. Assuming the Fontaine-Mazur, Grothendieck-Serre, Hodge, and Tate conjectures, this algorithm always terminates.*

- ▶ (This is really a theorem about abelian varieties.)

Theorem (A.-Lawrence).

There is an algorithm that, on input (g, K, S) with $g \in \mathbb{Z}^+$, K/\mathbb{Q} a number field, and S a finite set of places of K , outputs $\mathcal{A}_g(\mathfrak{o}_{K,S})$ **if it terminates**.

Theorem (A.-Lawrence).

There is an algorithm that, on input (g, K, S) with $g \in \mathbb{Z}^+$, K/\mathbb{Q} a number field, and S a finite set of places of K , outputs $\mathcal{A}_g(\mathfrak{o}_{K,S})$ **if it terminates**. Assuming the Fontaine-Mazur, Grothendieck-Serre, Hodge, and Tate conjectures, this algorithm always terminates.

Theorem (A.-Lawrence).

*There is an algorithm that, on input (g, K, S) with $g \in \mathbb{Z}^+$, K/\mathbb{Q} a number field, and S a finite set of places of K , outputs $\mathcal{A}_g(\mathfrak{o}_{K,S})$ **if it terminates**. Assuming the Fontaine-Mazur, Grothendieck-Serre, Hodge, and Tate conjectures, this algorithm always terminates.*

- ▶ Our key argument closely follows (and indeed we depended quite a bit upon) the paper "Anabelian geometry and descent obstructions on moduli spaces" by Patrikis-Voloch-Zarhin.

Theorem (A.).

There is a finite-time algorithm that, on input (\mathfrak{o}, K, S) with \mathfrak{o} an order in a totally real field, K/\mathbb{Q} totally real with $[K : \mathbb{Q}]$ odd, and S a finite set of places of K , outputs $\mathcal{H}_{\mathfrak{o}}(\mathfrak{o}_{K,S})$ (i.e. the A/K good outside S and $\mathrm{GL}_2(\mathfrak{o})$ -type over K).

Theorem (A.).

There is a finite-time algorithm that, on input (\mathfrak{o}, K, S) with \mathfrak{o} an order in a totally real field, K/\mathbb{Q} totally real with $[K : \mathbb{Q}]$ odd, and S a finite set of places of K , outputs $\mathcal{H}_{\mathfrak{o}}(\mathfrak{o}_{K,S})$ (i.e. the A/K good outside S and $\mathrm{GL}_2(\mathfrak{o})$ -type over K).

- ▶ $K = \mathbb{Q}$ and $\mathfrak{o} = \mathbb{Z}$: Murty-Pasten. Independently, $K = \mathbb{Q}$: von Känel. Key point in his argument, which we build upon: Serre's conjecture is known over \mathbb{Q} , so the relevant abelian varieties are quotients of $J_0(N_S)$ for N_S explicit, now bound heights using Masser-Wüstholz/Bost.

Theorem (A.).

There is a finite-time algorithm that, on input (\mathfrak{o}, K, S) with \mathfrak{o} an order in a totally real field, K/\mathbb{Q} totally real with $[K : \mathbb{Q}]$ odd, and S a finite set of places of K , outputs $\mathcal{H}_{\mathfrak{o}}(\mathfrak{o}_{K,S})$ (i.e. the A/K good outside S and $\mathrm{GL}_2(\mathfrak{o})$ -type over K).

- ▶ $K = \mathbb{Q}$ and $\mathfrak{o} = \mathbb{Z}$: Murty-Pasten. Independently, $K = \mathbb{Q}$: von Känel. Key point in his argument, which we build upon: Serre's conjecture is known over \mathbb{Q} , so the relevant abelian varieties are quotients of $J_0(N_S)$ for N_S explicit, now bound heights using Masser-Wüstholz/Bost.
- ▶ Each $H_{\mathfrak{o}}$ contains lots of complete curves, thus giving unconditional algorithms for a class of curves over odd-degree totally real fields.

Theorem (A.).

There is a finite-time algorithm that, on input (\mathfrak{o}, K, S) with \mathfrak{o} an order in a totally real field, K/\mathbb{Q} totally real with $[K : \mathbb{Q}]$ odd, and S a finite set of places of K , outputs $\mathcal{H}_{\mathfrak{o}}(\mathfrak{o}_{K,S})$ (i.e. the A/K good outside S and $\mathrm{GL}_2(\mathfrak{o})$ -type over K).

- ▶ $K = \mathbb{Q}$ and $\mathfrak{o} = \mathbb{Z}$: Murty-Pasten. Independently, $K = \mathbb{Q}$: von Känel. Key point in his argument, which we build upon: Serre's conjecture is known over \mathbb{Q} , so the relevant abelian varieties are quotients of $J_0(N_S)$ for N_S explicit, now bound heights using Masser-Wüstholz/Bost.
- ▶ Each $H_{\mathfrak{o}}$ contains lots of complete curves, thus giving unconditional algorithms for a class of curves over odd-degree totally real fields.
- ▶ We'll solve $x^6 + 4y^3 = 1$ (and some twists) over such K using a slightly modified argument.

Quick reminder: Faltings' first proof.

- ▶ Parshin: via an old construction of Kodaira, produce a finite-to-one map $C \rightarrow A_g$ for some g .

- ▶ Parshin: via an old construction of Kodaira, produce a finite-to-one map $C \rightarrow A_g$ for some g . Thus $\mathcal{C} \rightarrow \mathcal{A}_g$, with $\mathcal{C}/\mathfrak{o}_{K,S}$ the minimal proper regular model (and S explicit and large).

- ▶ Parshin: via an old construction of Kodaira, produce a finite-to-one map $C \rightarrow A_g$ for some g . Thus $\mathcal{C} \rightarrow \mathcal{A}_g$, with $\mathcal{C}/\mathfrak{o}_{K,S}$ the minimal proper regular model (and S explicit and large).
- ▶ Thus by properness we reduce to dealing with $\mathcal{A}_g(\mathfrak{o}_{K,S})$, i.e. g -dimensional A/K with good reduction outside S .

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ The first map takes $A \mapsto \rho_{A,\ell}$, the Galois representation corresponding to the ℓ -adic rational Tate module $T_\ell(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ The first map takes $A \mapsto \rho_{A,\ell}$, the Galois representation corresponding to the ℓ -adic rational Tate module $T_\ell(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
(Or: " $A \mapsto L(s, A)$ ".)

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ The first map takes $A \mapsto \rho_{A,\ell}$, the Galois representation corresponding to the ℓ -adic rational Tate module $T_\ell(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
(Or: " $A \mapsto L(s, A)$ ".)
- ▶ The second takes $\rho \mapsto (\text{tr}(\rho(\text{Frob}_p)))_{p \in T}$, i.e. records the traces of ρ at a Faltings-Serre set of primes T (depending explicitly on g, K, S).

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ The first map takes $A \mapsto \rho_{A,\ell}$, the Galois representation corresponding to the ℓ -adic rational Tate module $T_\ell(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.
(Or: " $A \mapsto L(s, A)$ ".)
- ▶ The second takes $\rho \mapsto (\text{tr}(\rho(\text{Frob}_p)))_{p \in T}$, i.e. records the traces of ρ at a Faltings-Serre set of primes T (depending explicitly on g, K, S).
(Or: " $L(s) \mapsto$ its first few Dirichlet coeff.s".)

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ Fibres of the first map: $A, B/K$ map to the same ρ iff $A \sim_K B$.

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ Fibres of the first map: $A, B/K$ map to the same ρ iff $A \sim_K B$. **Key finiteness:** if $A \sim_K B$, then $h(B) \ll_{h(A), [K:\mathbb{Q}], g} 1$ (Faltings, Raynaud (explicit), Masser-Wüstholz (also explicit)).

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ Fibres of the first map: $A, B/K$ map to the same ρ iff $A \sim_K B$. **Key finiteness:** if $A \sim_K B$, then $h(B) \ll_{h(A), [K:\mathbb{Q}], g} 1$ (Faltings, Raynaud (explicit), Masser-Wüstholz (also explicit)).
- ▶ The second map is easily injective ("Faltings' Lemma").

$$\left\{ A/K : \begin{array}{l} \dim A = g, \\ N_A \ll_S 1 \end{array} \right\} \xrightarrow{\text{/isog.}} \left\{ \rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Q}_\ell) \right\} \hookrightarrow \mathbb{Z}^T$$

- ▶ Fibres of the first map: $A, B/K$ map to the same ρ iff $A \sim_K B$. **Key finiteness:** if $A \sim_K B$, then $h(B) \ll_{h(A), [K:\mathbb{Q}], g} 1$ (Faltings, Raynaud (explicit), Masser-Wüstholz (also explicit)).
- ▶ The second map is easily injective ("Faltings' Lemma").
It is also evident that the image of the composition is finite!
 (Purity, aka Weil's proof of RH for curves:
 $a_p := \text{tr}(\rho_{A,\ell}(\text{Frob}_p)) \in \mathbb{Z}$, and also $|a_p| \leq 2g \cdot \sqrt{N_m p}$.)

- ▶ **Ineffectivity in Faltings' proof:** given $(a_p)_{p \in T} \in \mathbb{Z}^T$, we don't know if there is an A/K (of dimension g and good outside S) mapping to it.

- ▶ **Ineffectivity in Faltings' proof:** given $(a_p)_{p \in T} \in \mathbb{Z}^T$, we don't know if there is an A/K (of dimension g and good outside S) mapping to it.

Either there is none, or else, if we were to find *one* such A/K , then all other such B/K mapping to it would have explicitly bounded height and so we could find them all.

- ▶ **Ineffectivity in Faltings' proof:** given $(a_p)_{p \in T} \in \mathbb{Z}^T$, we don't know if there is an A/K (of dimension g and good outside S) mapping to it.

Either there is none, or else, if we were to find *one* such A/K , then all other such B/K mapping to it would have explicitly bounded height and so we could find them all.

- ▶ So, just like in Vojta's proof, the ineffectivity arises because we do not know a priori whether a given $(a_p)_{p \in T}$ has a corresponding A/K or not.

But it's not hopeless...

- ▶ Well... for each n , $(a_p)_{p \in T} \pmod{\ell^n}$ should at least be the traces of a rep. $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}/\ell^n)$ unram. outside S and the primes above ℓ .

- ▶ Well... for each n , $(a_p)_{p \in T} \pmod{\ell^n}$ should at least be the traces of a rep. $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}/\ell^n)$ unram. outside S and the primes above ℓ .
- ▶ That rep. should "look" pure of weight 1 (i.e. for $Nm \mathfrak{p} \ll \ell^n$, $\text{tr}(\rho(\text{Frob}_{\mathfrak{p}})) \in \mathbb{Z}/\ell^n$ should be the reduction of an $a_p \in \mathbb{Z}$ with $|a_p| \leq 2g \cdot \sqrt{Nm \mathfrak{p}}$) and have cyclotomic similitude character.

- ▶ Well... for each n , $(a_p)_{p \in T} \pmod{\ell^n}$ should at least be the traces of a rep. $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}/\ell^n)$ unram. outside S and the primes above ℓ .
- ▶ That rep. should "look" pure of weight 1 (i.e. for $Nm \mathfrak{p} \ll \ell^n$, $\text{tr}(\rho(\text{Frob}_{\mathfrak{p}})) \in \mathbb{Z}/\ell^n$ should be the reduction of an $a_p \in \mathbb{Z}$ with $|a_p| \leq 2g \cdot \sqrt{Nm \mathfrak{p}}$) and have cyclotomic similitude character.
- ▶ For each $\lambda | (\ell)$, that rep. should also arise from a finite commutative étale group scheme over $\mathfrak{o}_{K,\lambda}$ of order $\ell^{2g \cdot n}$.

- ▶ Well... for each n , $(a_p)_{p \in T} \pmod{\ell^n}$ should at least be the traces of a rep. $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}/\ell^n)$ unram. outside S and the primes above ℓ .
- ▶ That rep. should "look" pure of weight 1 (i.e. for $Nm \mathfrak{p} \ll \ell^n$, $\text{tr}(\rho(\text{Frob}_{\mathfrak{p}})) \in \mathbb{Z}/\ell^n$ should be the reduction of an $a_p \in \mathbb{Z}$ with $|a_p| \leq 2g \cdot \sqrt{Nm \mathfrak{p}}$) and have cyclotomic similitude character.
- ▶ For each $\lambda | (\ell)$, that rep. should also arise from a finite commutative étale group scheme over $\mathfrak{o}_{K,\lambda}$ of order $\ell^{2g \cdot n}$.
- ▶ Each of these can at least be checked in finite time...

- ▶ So we can do the above steps "by day" — i.e. while trying to falsify that a given $(a_p)_{p \in T}$ comes from an A/K of dimension g and good outside S .

- ▶ So we can do the above steps "by day" — i.e. while trying to falsify that a given $(a_p)_{p \in T}$ comes from an A/K of dimension g and good outside S .
- ▶ On the other hand, "by night", we can just search A/K of larger and larger height and check if $a_p = \text{tr}(\rho_{A,\ell}(\text{Frob}_p))$ for each $p \in T$.

- ▶ So we can do the above steps "by day" — i.e. while trying to falsify that a given $(a_p)_{p \in T}$ comes from an A/K of dimension g and good outside S .
- ▶ On the other hand, "by night", we can just search A/K of larger and larger height and check if $a_p = \text{tr}(\rho_{A,\ell}(\text{Frob}_p))$ for each $p \in T$.
- ▶ Is this enough?

- ▶ So we can do the above steps "by day" — i.e. while trying to falsify that a given $(a_p)_{p \in T}$ comes from an A/K of dimension g and good outside S .
- ▶ On the other hand, "by night", we can just search A/K of larger and larger height and check if $a_p = \text{tr}(\rho_{A,\ell}(\text{Frob}_p))$ for each $p \in T$.
- ▶ Is this enough?
- ▶ Not quite, but almost...

- ▶ If an $(a_p)_{p \in T}$ "survives forever", then (Kőnig's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_\ell)$ which:

- ▶ If an $(a_p)_{p \in T}$ "survives forever", then (Kőnig's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_\ell)$ which:
 - ▶ is unramified outside S and the primes over ℓ ,

- ▶ If an $(a_p)_{p \in T}$ "survives forever", then (Kőnig's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_\ell)$ which:
 - ▶ is unramified outside S and the primes over ℓ ,
 - ▶ satisfies $\text{tr}(\rho(\text{Frob}_p)) \in \mathbb{Z}$ and $|\text{tr}(\rho(\text{Frob}_p))| \leq 2g \cdot \sqrt{\text{Nm } \mathfrak{p}}$,

- If an $(a_p)_{p \in T}$ "survives forever", then (Kőnig's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_\ell)$ which:
- is unramified outside S and the primes over ℓ ,
 - satisfies $\text{tr}(\rho(\text{Frob}_p)) \in \mathbb{Z}$ and $|\text{tr}(\rho(\text{Frob}_p))| \leq 2g \cdot \sqrt{N_{\mathbb{m} \mathfrak{p}}}$,
 - has $\text{tr}(\rho(\text{Frob}_p)) = a_p$ for each $\mathfrak{p} \in T$,

- ▶ If an $(a_{\mathfrak{p}})_{\mathfrak{p} \in T}$ "survives forever", then (Kőnig's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_{\ell})$ which:
- ▶ is unramified outside S and the primes over ℓ ,
 - ▶ satisfies $\text{tr}(\rho(\text{Frob}_{\mathfrak{p}})) \in \mathbb{Z}$ and $|\text{tr}(\rho(\text{Frob}_{\mathfrak{p}}))| \leq 2g \cdot \sqrt{N_{\mathfrak{m}} \mathfrak{p}}$,
 - ▶ has $\text{tr}(\rho(\text{Frob}_{\mathfrak{p}})) = a_{\mathfrak{p}}$ for each $\mathfrak{p} \in T$,
 - ▶ has cyclotomic similitude character,

- If an $(a_p)_{p \in T}$ "survives forever", then (Kőnig's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_\ell)$ which:
- is unramified outside S and the primes over ℓ ,
 - satisfies $\text{tr}(\rho(\text{Frob}_p)) \in \mathbb{Z}$ and $|\text{tr}(\rho(\text{Frob}_p))| \leq 2g \cdot \sqrt{N_{\mathfrak{m}} \mathfrak{p}}$,
 - has $\text{tr}(\rho(\text{Frob}_p)) = a_p$ for each $\mathfrak{p} \in T$,
 - has cyclotomic similitude character,
 - and, for each $\lambda | (\ell)$, has the property that $\rho|_{\text{Gal}(\overline{\mathbb{Q}}_\ell/K_\lambda)}$ arises from an ℓ -divisible group over $\mathfrak{o}_{K,\lambda}$.

- ▶ If an $(a_p)_{p \in T}$ "survives forever", then (Kőnig's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_\ell)$ which:
 - ▶ is unramified outside S and the primes over ℓ ,
 - ▶ satisfies $\text{tr}(\rho(\text{Frob}_p)) \in \mathbb{Z}$ and $|\text{tr}(\rho(\text{Frob}_p))| \leq 2g \cdot \sqrt{N_{\mathfrak{m}} p}$,
 - ▶ has $\text{tr}(\rho(\text{Frob}_p)) = a_p$ for each $p \in T$,
 - ▶ has cyclotomic similitude character,
 - ▶ and, for each $\lambda | (\ell)$, has the property that $\rho|_{\text{Gal}(\overline{\mathbb{Q}}_\ell/K_\lambda)}$ arises from an ℓ -divisible group over $\mathfrak{o}_{K,\lambda}$.

- ▶ Thus e.g. for each $\lambda | (\ell)$: $\rho|_{\text{Gal}(\overline{\mathbb{Q}}/K_\lambda)}$ is crystalline (thus de Rham) with Hodge-Tate weights $\underbrace{\{0, \dots, 0\}}_g, \underbrace{\{-1, \dots, -1\}}_g$.

- ▶ If an $(a_p)_{p \in T}$ "survives forever", then (König's Lemma) it at least arises from a $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \text{GSp}_{2g}(\mathbb{Z}_\ell)$ which:
 - ▶ is unramified outside S and the primes over ℓ ,
 - ▶ satisfies $\text{tr}(\rho(\text{Frob}_p)) \in \mathbb{Z}$ and $|\text{tr}(\rho(\text{Frob}_p))| \leq 2g \cdot \sqrt{N_{\mathfrak{p}}}$,
 - ▶ has $\text{tr}(\rho(\text{Frob}_p)) = a_p$ for each $p \in T$,
 - ▶ has cyclotomic similitude character,
 - ▶ and, for each $\lambda | (\ell)$, has the property that $\rho|_{\text{Gal}(\overline{\mathbb{Q}}_\ell/K_\lambda)}$ arises from an ℓ -divisible group over $\mathfrak{o}_{K,\lambda}$.

- ▶ Thus e.g. for each $\lambda | (\ell)$: $\rho|_{\text{Gal}(\overline{\mathbb{Q}}/K_\lambda)}$ is crystalline (thus de Rham) with Hodge-Tate weights $\underbrace{\{0, \dots, 0\}}_g, \underbrace{\{-1, \dots, -1\}}_g$.

- ▶ ($\rho^{\text{s.s.}}$ satisfies the same properties (exactness of $D_{\text{crys.}}$) so wlog ρ is semisimple.)

- ▶ So, being finitely ramified and de Rham at primes above ℓ , by Fontaine-Mazur + Grothendieck-Serre, it is a summand of $H^i(X, \mathbb{Q}_\ell)(j)$ with X/K smooth projective.

- ▶ So, being finitely ramified and de Rham at primes above ℓ , by Fontaine-Mazur + Grothendieck-Serre, it is a summand of $H^i(X, \mathbb{Q}_\ell)(j)$ with X/K smooth projective.
- ▶ By Tate the corresponding projector is a \mathbb{Q}_ℓ -linear combination of correspondences.

- ▶ So, being finitely ramified and de Rham at primes above ℓ , by Fontaine-Mazur + Grothendieck-Serre, it is a summand of $H^i(X, \mathbb{Q}_\ell)(j)$ with X/K smooth projective.
- ▶ By Tate the corresponding projector is a \mathbb{Q}_ℓ -linear combination of correspondences.
- ▶ The endomorphism ring of $H^i(X)$ is semisimple, so it is also a $\overline{\mathbb{Q}}$ -linear combination of correspondences.

- ▶ So, being finitely ramified and de Rham at primes above ℓ , by Fontaine-Mazur + Grothendieck-Serre, it is a summand of $H^i(X, \mathbb{Q}_\ell)(j)$ with X/K smooth projective.
- ▶ By Tate the corresponding projector is a \mathbb{Q}_ℓ -linear combination of correspondences.
- ▶ The endomorphism ring of $H^i(X)$ is semisimple, so it is also a $\overline{\mathbb{Q}}$ -linear combination of correspondences.
- ▶ Thus we end up with a motive over K with E -coefficients with ℓ -adic realization ρ .

- ▶ So, being finitely ramified and de Rham at primes above ℓ , by Fontaine-Mazur + Grothendieck-Serre, it is a summand of $H^i(X, \mathbb{Q}_\ell)(j)$ with X/K smooth projective.
- ▶ By Tate the corresponding projector is a \mathbb{Q}_ℓ -linear combination of correspondences.
- ▶ The endomorphism ring of $H^i(X)$ is semisimple, so it is also a $\overline{\mathbb{Q}}$ -linear combination of correspondences.
- ▶ Thus we end up with a motive over K with E -coefficients with ℓ -adic realization ρ .
- ▶ Restricting scalars, we end up with a motive over K with \mathbb{Q} -coefficients whose ℓ -adic realization admits ρ as a summand.

- ▶ So, being finitely ramified and de Rham at primes above ℓ , by Fontaine-Mazur + Grothendieck-Serre, it is a summand of $H^i(X, \mathbb{Q}_\ell)(j)$ with X/K smooth projective.
- ▶ By Tate the corresponding projector is a \mathbb{Q}_ℓ -linear combination of correspondences.
- ▶ The endomorphism ring of $H^i(X)$ is semisimple, so it is also a $\overline{\mathbb{Q}}$ -linear combination of correspondences.
- ▶ Thus we end up with a motive over K with E -coefficients with ℓ -adic realization ρ .
- ▶ Restricting scalars, we end up with a motive over K with \mathbb{Q} -coefficients whose ℓ -adic realization admits ρ as a summand.
- ▶ Our knowledge of Hodge-Tate weights implies the corresponding Betti realization is a \mathbb{Q} -Hodge structure of weight $\underbrace{\{(1, 0), \dots, (1, 0)\}}_{g \cdot [E:\mathbb{Q}]} \cup \underbrace{\{(0, 1), \dots, (0, 1)\}}_{g \cdot [E:\mathbb{Q}]}$.

- ▶ So, being finitely ramified and de Rham at primes above ℓ , by Fontaine-Mazur + Grothendieck-Serre, it is a summand of $H^i(X, \mathbb{Q}_\ell)(j)$ with X/K smooth projective.
- ▶ By Tate the corresponding projector is a \mathbb{Q}_ℓ -linear combination of correspondences.
- ▶ The endomorphism ring of $H^i(X)$ is semisimple, so it is also a $\overline{\mathbb{Q}}$ -linear combination of correspondences.
- ▶ Thus we end up with a motive over K with E -coefficients with ℓ -adic realization ρ .
- ▶ Restricting scalars, we end up with a motive over K with \mathbb{Q} -coefficients whose ℓ -adic realization admits ρ as a summand.
- ▶ Our knowledge of Hodge-Tate weights implies the corresponding Betti realization is a \mathbb{Q} -Hodge structure of weight $\underbrace{\{(1, 0), \dots, (1, 0)\}}_{g \cdot [E:\mathbb{Q}]} \cup \underbrace{\{(0, 1), \dots, (0, 1)\}}_{g \cdot [E:\mathbb{Q}]}$.
- ▶ We've found an abelian variety! First over \mathbb{C} (Riemann), then over $\overline{\mathbb{Q}}$ (Hodge, really absolute Hodge), then over K (restricting scalars).

- ▶ In the end we see that if a tuple $(a_p)_{p \in T}$ "survives all days", then it arises from a subrepresentation of $\rho_{A,\ell}$ for A/K good outside S (though potentially higher-dimensional).

- ▶ In the end we see that if a tuple $(a_{\mathfrak{p}})_{\mathfrak{p} \in T}$ "survives all days", then it arises from a subrepresentation of $\rho_{A,\ell}$ for A/K good outside S (though potentially higher-dimensional).
- ▶ Since we can compute $\text{End}_K(A)$ in finite time (another theorem of Masser-Wüstholz) for a given A/K , this is also fine: "by night" we instead search higher- and higher-dimensional B/K of larger and larger height, factorize $\rho_{B,\ell}$ into irrep.s, and (if there are $2g$ -dimensional combinations of such) check their Frobenius traces at $\mathfrak{p} \in T$.

- ▶ In the end we see that if a tuple $(a_p)_{p \in T}$ "survives all days", then it arises from a subrepresentation of $\rho_{A,\ell}$ for A/K good outside S (though potentially higher-dimensional).
- ▶ Since we can compute $\text{End}_K(A)$ in finite time (another theorem of Masser-Wüstholz) for a given A/K , this is also fine: "by night" we instead search higher- and higher-dimensional B/K of larger and larger height, factorize $\rho_{B,\ell}$ into irrep.s, and (if there are $2g$ -dimensional combinations of such) check their Frobenius traces at $p \in T$.
- ▶ Eventually (per the conjectures) we find such a B/K , and then if $(a_p)_{p \in T}$ arises from an A/K , by Poincaré complete reducibility we have $B \sim_K A \times C$, and so

$$h(A) \stackrel{\text{Bost}}{\leq} h(A \times C) + O_{\dim B}(1) \stackrel{\text{Masser-Wüstholz}}{\ll} h(B), [K:\mathbb{Q}], \dim B \quad 1.$$

And unconditionally...?

- ▶ Let now K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd. Let also F/\mathbb{Q} be totally real, and S a finite set of places of K .

- ▶ Let now K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd. Let also F/\mathbb{Q} be totally real, and S a finite set of places of K .
- ▶ We're now after $\mathcal{H}_{\mathfrak{o}_F}(\mathfrak{o}_{K,S})$, i.e. the A/K good outside S of $\mathrm{GL}_2(F)$ -type over K .

- ▶ Let now K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd. Let also F/\mathbb{Q} be totally real, and S a finite set of places of K .
- ▶ We're now after $\mathcal{H}_{\mathfrak{o}_F}(\mathfrak{o}_{K,S})$, i.e. the A/K good outside S of $GL_2(F)$ -type over K .
- ▶ If we knew all such A/K were modular, we'd be done: they'd all correspond to Hilbert modular forms over K , thus (Jacquet-Langlands) be quotients of Jac (explicit Shim. curve), so we'd again use Masser-Wüstholz/Bost.

- ▶ Let now K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd. Let also F/\mathbb{Q} be totally real, and S a finite set of places of K .
- ▶ We're now after $\mathcal{H}_{\mathfrak{o}_F}(\mathfrak{o}_{K,S})$, i.e. the A/K good outside S of $GL_2(F)$ -type over K .
- ▶ If we knew all such A/K were modular, we'd be done: they'd all correspond to Hilbert modular forms over K , thus (Jacquet-Langlands) be quotients of Jac (explicit Shim. curve), so we'd again use Masser-Wüstholz/Bost.
- ▶ We'll get away with using potential modularity.

- ▶ Recall that being $\mathrm{GL}_2(F)$ -type buys us λ -adic Tate modules, i.e. 2-dimensional rep.s $\rho_{A,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \rightarrow \mathrm{GL}_2(\mathfrak{o}_{F,\lambda})$.

- ▶ Recall that being $GL_2(F)$ -type buys us λ -adic Tate modules, i.e. 2-dimensional reps $\rho_{A,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_{F,\lambda})$.

Lemma (adapting M. Dimitrov's for Hilb. mod. forms).

Once $Nm \lambda \gg_{F,K,S} 1$, $\rho_{A,\lambda} \pmod{\lambda}$ has image containing $SL_2(\mathbb{F}_\ell)$

- ▶ Recall that being $GL_2(F)$ -type buys us λ -adic Tate modules, i.e. 2-dimensional reps $\rho_{A,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_{F,\lambda})$.

Lemma (adapting M. Dimitrov's for Hilb. mod. forms).

Once $Nm \lambda \gg_{F,K,S} 1$, $\rho_{A,\lambda} \pmod{\lambda}$ has image containing $SL_2(\mathbb{F}_\ell)$ (and thus satisfies the "Taylor-Wiles hypothesis").

- ▶ Recall that being $GL_2(F)$ -type buys us λ -adic Tate modules, i.e. 2-dimensional reps $\rho_{A,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_{F,\lambda})$.

Lemma (adapting M. Dimitrov's for Hilb. mod. forms).

Once $Nm \lambda \gg_{F,K,S} 1$, $\rho_{A,\lambda} \pmod{\lambda}$ has image containing $SL_2(\mathbb{F}_\ell)$ (and thus satisfies the "Taylor-Wiles hypothesis").

- ▶ So find a large λ , and then determine all possible $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_F/\lambda)$ (unram. outside \dots , correct det., \dots) explicitly (Hermite-Minkowski).

- ▶ Recall that being $GL_2(F)$ -type buys us λ -adic Tate modules, i.e. 2-dimensional reps $\rho_{A,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_{F,\lambda})$.

Lemma (adapting M. Dimitrov's for Hilb. mod. forms).

Once $Nm \lambda \gg_{F,K,S} 1$, $\rho_{A,\lambda} \pmod{\lambda}$ has image containing $SL_2(\mathbb{F}_\ell)$ (and thus satisfies the "Taylor-Wiles hypothesis").

- ▶ So find a large λ , and then determine all possible $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_F/\lambda)$ (unram. outside \dots , correct det., \dots) explicitly (Hermite-Minkowski).
- ▶ Given ρ , follow Taylor's (I used Snowden's) proof to compute a totally real Galois L_ρ/K , so that any such A/K is modular over $L_{\rho_{A,\lambda} \pmod{\lambda}}$.

- ▶ Recall that being $GL_2(F)$ -type buys us λ -adic Tate modules, i.e. 2-dimensional reps $\rho_{A,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_{F,\lambda})$.

Lemma (adapting M. Dimitrov's for Hilb. mod. forms).

Once $Nm \lambda \gg_{F,K,S} 1$, $\rho_{A,\lambda} \pmod{\lambda}$ has image containing $SL_2(\mathbb{F}_\ell)$ (and thus satisfies the "Taylor-Wiles hypothesis").

- ▶ So find a large λ , and then determine all possible $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_F/\lambda)$ (unram. outside \dots , correct det., \dots) explicitly (Hermite-Minkowski).
- ▶ Given ρ , follow Taylor's (I used Snowden's) proof to compute a totally real Galois L_ρ/K , so that any such A/K is modular over $L_{\rho_{A,\lambda} \pmod{\lambda}}$.
- ▶ Only not-completely-explicit step: invocation of Moret-Bailly's theorem, which guarantees a totally real point on a twist of a Hilbert modular variety.

- ▶ Recall that being $GL_2(F)$ -type buys us λ -adic Tate modules, i.e. 2-dimensional reps $\rho_{A,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_{F,\lambda})$.

Lemma (adapting M. Dimitrov's for Hilb. mod. forms).

Once $Nm \lambda \gg_{F,K,S} 1$, $\rho_{A,\lambda} \pmod{\lambda}$ has image containing $SL_2(\mathbb{F}_\ell)$ (and thus satisfies the "Taylor-Wiles hypothesis").

- ▶ So find a large λ , and then determine all possible $\rho : \text{Gal}(\overline{\mathbb{Q}}/K) \rightarrow GL_2(\mathfrak{o}_F/\lambda)$ (unram. outside \dots , correct det., \dots) explicitly (Hermite-Minkowski).
- ▶ Given ρ , follow Taylor's (I used Snowden's) proof to compute a totally real Galois L_ρ/K , so that any such A/K is modular over $L_{\rho_{A,\lambda} \pmod{\lambda}}$.
- ▶ Only not-completely-explicit step: invocation of Moret-Bailly's theorem, which guarantees a totally real point on a twist of a Hilbert modular variety. Well, you can just brute force once you know the point exists...

- ▶ Now the kicker (which I learned from Snowden's paper). We know A/K is modular over the totally real Galois L/K , but $[L : \mathbb{Q}]$ might be even! ...

- ▶ Now the kicker (which I learned from Snowden's paper). We know A/K is modular over the totally real Galois L/K , but $[L : \mathbb{Q}]$ might be even! ...
 - Solvable descent applied to $L/L^{2\text{-Sylow}}$! :)

- ▶ Now the kicker (which I learned from Snowden's paper). We know A/K is modular over the totally real Galois L/K , but $[L : \mathbb{Q}]$ might be even! ...
 - Solvable descent applied to $L/L^{2\text{-Sylow!}}$:)
- ▶ So we get an explicit finite set of totally real L/K with $[L : \mathbb{Q}]$ odd such that any relevant A/K is modular over L , and then Masser-Wüstholz/Bost again.

► Finally, $x^6 + 4y^3 = 1$.

- ▶ Finally, $x^6 + 4y^3 = 1$. Let K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd, $a \in K^\times$, and $C_a : x^6 + 4y^3 = a^2$.

- ▶ Finally, $x^6 + 4y^3 = 1$. Let K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd, $a \in K^\times$, and $C_a : x^6 + 4y^3 = a^2$.
- ▶ The hypergeometric family associated to $\Delta(3, 6, 6)$ (arithmetic!) gives a nonconstant $C_a \rightarrow A_2$.

- ▶ Finally, $x^6 + 4y^3 = 1$. Let K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd, $a \in K^\times$, and $C_a : x^6 + 4y^3 = a^2$.
- ▶ The hypergeometric family associated to $\Delta(3, 6, 6)$ (arithmetic!) gives a nonconstant $C_a \rightarrow A_2$. Explicitly, using the Belyi $f : C_a \rightarrow \mathbb{P}^1$ via $f(P) := \frac{x(P)^6}{a^2}$, A_P is the quotient of the Jac. of (the desing. of) $y^6 = x^4(1-x)^3(1-f(P) \cdot x)$ by the same with $y^3 = \dots$.

- ▶ Finally, $x^6 + 4y^3 = 1$. Let K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd, $a \in K^\times$, and $C_a : x^6 + 4y^3 = a^2$.
- ▶ The hypergeometric family associated to $\Delta(3, 6, 6)$ (arithmetic!) gives a nonconstant $C_a \rightarrow A_2$. Explicitly, using the Belyi $f : C_a \rightarrow \mathbb{P}^1$ via $f(P) := \frac{x(P)^6}{a^2}$, A_P is the quotient of the Jac. of (the desing. of) $y^6 = x^4(1-x)^3(1-f(P) \cdot x)$ by the same with $y^3 = \dots$.
- ▶ Because of the $y^6 = \dots$, these A_P have $\mathbb{Z}[\zeta_3] \hookrightarrow \text{End}_{K(\zeta_3)}(A_P)$. So they're $\text{GL}_2(\mathbb{Z}[\zeta_3])$ -type over $K(\zeta_3)$.

- ▶ Finally, $x^6 + 4y^3 = 1$. Let K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd, $a \in K^\times$, and $C_a : x^6 + 4y^3 = a^2$.
- ▶ The hypergeometric family associated to $\Delta(3, 6, 6)$ (arithmetic!) gives a nonconstant $C_a \rightarrow A_2$. Explicitly, using the Belyi $f : C_a \rightarrow \mathbb{P}^1$ via $f(P) := \frac{x(P)^6}{a^2}$, A_P is the quotient of the Jac. of (the desing. of) $y^6 = x^4(1-x)^3(1-f(P) \cdot x)$ by the same with $y^3 = \dots$.
- ▶ Because of the $y^6 = \dots$, these A_P have $\mathbb{Z}[\zeta_3] \hookrightarrow \text{End}_{K(\zeta_3)}(A_P)$. So they're $\text{GL}_2(\mathbb{Z}[\zeta_3])$ -type over $K(\zeta_3)$. Not good enough...

- ▶ Finally, $x^6 + 4y^3 = 1$. Let K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd, $a \in K^\times$, and $C_a : x^6 + 4y^3 = a^2$.
- ▶ The hypergeometric family associated to $\Delta(3, 6, 6)$ (arithmetic!) gives a nonconstant $C_a \rightarrow A_2$. Explicitly, using the Belyi $f : C_a \rightarrow \mathbb{P}^1$ via $f(P) := \frac{x(P)^6}{a^2}$, A_P is the quotient of the Jac. of (the desing. of) $y^6 = x^4(1-x)^3(1-f(P) \cdot x)$ by the same with $y^3 = \dots$.
- ▶ Because of the $y^6 = \dots$, these A_P have $\mathbb{Z}[\zeta_3] \hookrightarrow \text{End}_{K(\zeta_3)}(A_P)$. So they're $\text{GL}_2(\mathbb{Z}[\zeta_3])$ -type over $K(\zeta_3)$. Not good enough...
- ▶ Arithmeticity of $\Delta(3, 6, 6)$ means $B_6 \hookrightarrow \text{End}_{\mathbb{Q}}^0(A_P)$, so at least there are other endo.s... In fact (compare Frob. traces of the 2-dim'l rep.s over $K(\zeta_3)$) A_P/K is GL_2 -type over K .

- ▶ Finally, $x^6 + 4y^3 = 1$. Let K/\mathbb{Q} be totally real with $[K : \mathbb{Q}]$ odd, $a \in K^\times$, and $C_a : x^6 + 4y^3 = a^2$.
- ▶ The hypergeometric family associated to $\Delta(3, 6, 6)$ (arithmetic!) gives a nonconstant $C_a \rightarrow A_2$. Explicitly, using the Belyi $f : C_a \rightarrow \mathbb{P}^1$ via $f(P) := \frac{x(P)^6}{a^2}$, A_P is the quotient of the Jac. of (the desing. of) $y^6 = x^4(1-x)^3(1-f(P) \cdot x)$ by the same with $y^3 = \dots$.
- ▶ Because of the $y^6 = \dots$, these A_P have $\mathbb{Z}[\zeta_3] \hookrightarrow \text{End}_{K(\zeta_3)}(A_P)$. So they're $\text{GL}_2(\mathbb{Z}[\zeta_3])$ -type over $K(\zeta_3)$. Not good enough...
- ▶ Arithmeticity of $\Delta(3, 6, 6)$ means $B_6 \hookrightarrow \text{End}_{\mathbb{Q}}^0(A_P)$, so at least there are other endo.s... In fact (compare Frob. traces of the 2-dim'l rep.s over $K(\zeta_3)$) A_P/K is GL_2 -type over K .
- ▶ Easy to compute an explicit \mathcal{F} for which each A_P/K is $\text{GL}_2(F)$ -type for some $F \in \mathcal{F}$, so we're done.

Thanks!