Umberto Zannier

Scuola Normale Superiore

September 17, 2019

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへぐ

Abelian varieties

For an integer g > 0 let us consider the complex *principally polarized abelian varieties* (p.p.a.v.) of dimension g, up to isomorphism.

Abelian varieties

For an integer g > 0 let us consider the complex *principally polarized abelian varieties* (p.p.a.v.) of dimension g, up to isomorphism.

They are known to correspond to the complex points $\mathcal{A}_g(\mathbb{C})$, where \mathcal{A}_g is a (quasi-projective) algebraic variety, and we have

$$\dim \mathcal{A}_g = \frac{g(g+1)}{2}.$$

Abelian varieties

For an integer g > 0 let us consider the complex *principally polarized abelian varieties* (p.p.a.v.) of dimension g, up to isomorphism.

They are known to correspond to the complex points $\mathcal{A}_g(\mathbb{C})$, where \mathcal{A}_g is a (quasi-projective) algebraic variety, and we have

$$\dim \mathcal{A}_g = \frac{g(g+1)}{2}.$$

Example: for g = 1, we find $A_1 =$ the affine line \mathbb{A}^1 , where an elliptic curve up to isomorphism corresponds to its *j*-invariant.

Abelian varieties

For an integer g > 0 let us consider the complex *principally polarized abelian varieties* (p.p.a.v.) of dimension g, up to isomorphism.

They are known to correspond to the complex points $\mathcal{A}_g(\mathbb{C})$, where \mathcal{A}_g is a (quasi-projective) algebraic variety, and we have

$$\dim \mathcal{A}_g = \frac{g(g+1)}{2}.$$

Example: for g = 1, we find $A_1 =$ the affine line \mathbb{A}^1 , where an elliptic curve up to isomorphism corresponds to its *j*-invariant.

Jacobians

Inside \mathcal{A}_g we have the subvariety \mathcal{T}_g (*Torelli locus*) defined here as the closure of Jacobians of curves of genus g, so e.g. $\mathcal{T}_1 = \mathcal{A}_1$.

For g > 1 we have (essentially due to RIEMANN)

$$\dim \mathcal{T}_g = 3g - 3.$$

Hence dim $T_g = \dim A_g$ for $g \le 3$, and in fact one has $T_g = A_g$ for $1 \le g \le 3$.

On the other hand, dim $A_g > \dim T_g$ for $g \ge 4$, so in particular:

・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・
・

Hence dim $\mathcal{T}_g = \dim \mathcal{A}_g$ for $g \leq 3$, and in fact one has $\mathcal{T}_g = \mathcal{A}_g$ for $1 \leq g \leq 3$.

On the other hand, dim $\mathcal{A}_g > \dim \mathcal{T}_g$ for $g \ge 4$, so in particular:

Remark: For $g \ge 4$ there exist (complex) p.p. abelian varieties of dimension g and not isomorphic to any Jacobian.

Hence dim $\mathcal{T}_g = \dim \mathcal{A}_g$ for $g \leq 3$, and in fact one has $\mathcal{T}_g = \mathcal{A}_g$ for $1 \leq g \leq 3$.

On the other hand, dim $\mathcal{A}_g > \dim \mathcal{T}_g$ for $g \ge 4$, so in particular:

Remark: For $g \ge 4$ there exist (complex) p.p. abelian varieties of dimension g and not isomorphic to any Jacobian.

Now, isogeny is a weaker form of isomorphism, and we may ask whether any complex (p.p.)a.v. is isogenous to a Jacobian.

Hence dim $\mathcal{T}_g = \dim \mathcal{A}_g$ for $g \leq 3$, and in fact one has $\mathcal{T}_g = \mathcal{A}_g$ for $1 \leq g \leq 3$.

On the other hand, dim $\mathcal{A}_g > \dim \mathcal{T}_g$ for $g \ge 4$, so in particular:

Remark: For $g \ge 4$ there exist (complex) p.p. abelian varieties of dimension g and not isomorphic to any Jacobian.

Now, isogeny is a weaker form of isomorphism, and we may ask whether any complex (p.p.)a.v. is isogenous to a Jacobian.

An isogeny is determined by its kernel, which has countably many possibilities, and one deduces that

The p.p.a.v. of dimension g isogenous to some Jacobian form a **countable** union of algebraic varieties of dimension 3g - 3 in A_g .

Since $\ensuremath{\mathbb{C}}$ is not countable, this implies the improved

Since \mathbb{C} is not countable, this implies the improved

Remark: For $g \ge 4$ there exist complex a.v. of dimension g and not isogenous to any Jacobian.

Since \mathbb{C} is not countable, this implies the improved

Remark: For $g \ge 4$ there exist complex a.v. of dimension g and not isogenous to any Jacobian.

However this argument fails if we work over a *countable* field, even if alg. closed, like $\overline{\mathbb{Q}}$. Indeed, KATZ and OORT raised the following

Since $\ensuremath{\mathbb{C}}$ is not countable, this implies the improved

Remark: For $g \ge 4$ there exist complex a.v. of dimension g and not isogenous to any Jacobian.

However this argument fails if we work over a *countable* field, even if alg. closed, like $\overline{\mathbb{Q}}$. Indeed, KATZ and OORT raised the following

Question: (KATZ-OORT) Do there exist a.v. defined over $\overline{\mathbb{Q}}$ and not isogenous to any Jacobian ?

Since $\ensuremath{\mathbb{C}}$ is not countable, this implies the improved

Remark: For $g \ge 4$ there exist complex a.v. of dimension g and not isogenous to any Jacobian.

However this argument fails if we work over a *countable* field, even if alg. closed, like $\overline{\mathbb{Q}}$. Indeed, KATZ and OORT raised the following

Question: (KATZ-OORT) Do there exist a.v. defined over $\overline{\mathbb{Q}}$ and not isogenous to any Jacobian ?

Intuition seems to suggest an affirmative answer, despite the failure of the above argument.

Since $\ensuremath{\mathbb{C}}$ is not countable, this implies the improved

Remark: For $g \ge 4$ there exist complex a.v. of dimension g and not isogenous to any Jacobian.

However this argument fails if we work over a *countable* field, even if alg. closed, like $\overline{\mathbb{Q}}$. Indeed, KATZ and OORT raised the following

Question: (KATZ-OORT) Do there exist a.v. defined over $\overline{\mathbb{Q}}$ and not isogenous to any Jacobian ?

Intuition seems to suggest an affirmative answer, despite the failure of the above argument.

However some attempts suggest it might be not easy to prove such expectation. For instance, we note that the 'isogeny orbit' of any $x \in \mathcal{A}_g(\mathbb{C})$ is complex-dense.

Remarks.

(i) Actually KATZ was especially interested in the analogue question over $\overline{\mathbb{F}_p}$. Recent work of SHANKAR-TSIMERMAN provides some (surprising) evidence we might have a negative answer now.

Remarks.

(i) Actually KATZ was especially interested in the analogue question over $\overline{\mathbb{F}_p}$. Recent work of SHANKAR-TSIMERMAN provides some (surprising) evidence we might have a negative answer now.

(ii) This kind of question fits within a general 'specialization' motivation, as in SERRE's phrasing (letter to RIBET 1981): " Il s'agit de prouver que "tout" ce qui est réalisable sur un corps de type fini sur \mathbb{Q} l'est aussi (par spécialisation) sur un corps de nombres. "

Remarks.

(i) Actually KATZ was especially interested in the analogue question over $\overline{\mathbb{F}_p}$. Recent work of SHANKAR-TSIMERMAN provides some (surprising) evidence we might have a negative answer now.

(ii) This kind of question fits within a general 'specialization' motivation, as in SERRE's phrasing (letter to RIBET 1981): " Il s'agit de prouver que "tout" ce qui est réalisable sur un corps de type fini sur \mathbb{Q} l'est aussi (par spécialisation) sur un corps de nombres. "

Now, a way to attack the Katz-Oort problem could depend on suitable characterizations of \mathcal{T}_g inside \mathcal{A}_g . For instance ARBARELLO-DE CONCINI gave an important one in 1984 (and then an application of the ideas in 1987).

A more general question: The same question arises on replacing \mathcal{T}_g by any prescribed proper (closed) subvariety $\mathcal{X} \subsetneq \mathcal{A}_g$. This suggests to seek arguments not using the special nature of \mathcal{T}_g .

A more general question: The same question arises on replacing \mathcal{T}_g by any prescribed proper (closed) subvariety $\mathcal{X} \subsetneq \mathcal{A}_g$. This suggests to seek arguments not using the special nature of \mathcal{T}_g .

- CHAI-OORT (2012) gave an affirmative answer even to this more general issue, but *conditionally* on the *André-Oort conjecture*.

A more general question: The same question arises on replacing \mathcal{T}_g by any prescribed proper (closed) subvariety $\mathcal{X} \subsetneq \mathcal{A}_g$. This suggests to seek arguments not using the special nature of \mathcal{T}_g .

- CHAI-OORT (2012) gave an affirmative answer even to this more general issue, but *conditionally* on the *André-Oort conjecture*.

- Shortly afterwards TSIMERMAN (2012) reconsidered substantially their arguments and gave an unconditional proof. (Later he also did the last step for the André-Oort conjecture.)

A more general question: The same question arises on replacing \mathcal{T}_g by any prescribed proper (closed) subvariety $\mathcal{X} \subsetneq \mathcal{A}_g$. This suggests to seek arguments not using the special nature of \mathcal{T}_g .

- CHAI-OORT (2012) gave an affirmative answer even to this more general issue, but *conditionally* on the *André-Oort conjecture*.

- Shortly afterwards $T_{SIMERMAN}$ (2012) reconsidered substantially their arguments and gave an unconditional proof. (Later he also did the last step for the André-Oort conjecture.)

Proofs: Both arguments worked with appropriate sequences of a.v. of *Weyl CM type*; this is invariant by isogeny, which was the starting point for proving (with heavy work) that eventually some member was not isogenous to any Jacobian (or to any $x \in \mathcal{X}$).

The a.v. so exhibited have strong arithmetical restrictions, and are highly 'special' in several ways.

▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□▶ ▲□▶

The a.v. so exhibited have strong arithmetical restrictions, and are highly 'special' in several ways.

Then, in the spirit of $\operatorname{SerRE}\nolimits$'s phrasing, it looks natural to ask for

a.v. $/\overline{\mathbb{Q}},$ not isogenous to any Jacobian and with 'generic' properties

in some sense. Let us see a few interpretations, in a hierarchy:

The a.v. so exhibited have strong arithmetical restrictions, and are highly 'special' in several ways.

Then, in the spirit of SERRE's phrasing, it looks natural to ask for

a.v. $/\overline{\mathbb{Q}}$, not isogenous to any Jacobian and with 'generic' properties in some sense. Let us see a few interpretations, in a hierarchy:

No CM: The CM property is not shared by any continuous family. Actually CHAI-OORT explicitly asked for examples without CM.

Trivial End: A $\overline{\mathbb{Q}}$ -generic point $x \in \mathcal{A}_g$ has $End(x) = \mathbb{Z}$, in particular no CM. This could already be a 'natural' condition.

Hodge-generic: This requires that the so-called *Mumford-Tate* group of x is maximal, i.e. GSp_{2g} . It implies the former property of a trivial endomorphism ring. It is again known that the points in $\mathcal{A}_g(\mathbb{C})$ which are not Hodge-generic form a countable union of proper subvarieties.

Hodge-generic: This requires that the so-called *Mumford-Tate* group of x is maximal, i.e. GSp_{2g} . It implies the former property of a trivial endomorphism ring. It is again known that the points in $\mathcal{A}_g(\mathbb{C})$ which are not Hodge-generic form a countable union of proper subvarieties.

Galois-generic: A property known to be yet stronger is to be (ℓ) -Galois-generic (say over $\overline{\mathbb{Q}}$), defined in terms of the Galois representation on torsion points (of order a power of the prime ℓ). This last property has arithmetic nature and is not directly defined in geometric terms, though believed to be equivalent to Hodge-generic (as proved in many cases by several authors).

'Generic' abelian varieties not isogenous to Jacobians

Jointly with MASSER we have used a different method toward these issues. We have statements of several types, of which we offer some examples. We refer to Jacobians of dimension $g \ge 4$, though the results hold for the more general question above.

Jointly with MASSER we have used a different method toward these issues. We have statements of several types, of which we offer some examples. We refer to Jacobians of dimension $g \ge 4$, though the results hold for the more general question above.

Theorem 1

There exists a set $\mathcal{N} \subset \mathcal{A}_g(\overline{\mathbb{Q}})$, complex-dense in $\mathcal{A}_g(\mathbb{C})$, representing pairwise non-isogenous p.p.a.v., each being ℓ -Galois-generic and not isogenous to any Jacobian.

The method yields further information on such p.p.a.v.. For instance let us see two aspects:

(i) Beyond the said complex-denseness, in a sense 'the majority' of p.p.a.v. defined over $\overline{\mathbb{Q}}$ are not isogenous to any Jacobian. We can express this vague meaning through estimates as follows.

(i) Beyond the said complex-denseness, in a sense 'the majority' of p.p.a.v. defined over $\overline{\mathbb{Q}}$ are not isogenous to any Jacobian. We can express this vague meaning through estimates as follows.

Take first a dominant rational map $\phi : \mathcal{A}_g \to \mathbb{A}^G$ ($G = \dim \mathcal{A}_g$), defined over \mathbb{Q} , and finite above an open set $A \subset \mathbb{A}^G$. We may then take e.g. the box B(T) of integer points $(p_1, ..., p_G) \in A$ with $|p_i| \leq T$ and consider the a.v. $x \in \mathcal{A}_g$ such that $\phi(x) \in B(T)$.

(i) Beyond the said complex-denseness, in a sense 'the majority' of p.p.a.v. defined over $\overline{\mathbb{Q}}$ are not isogenous to any Jacobian. We can express this vague meaning through estimates as follows.

Take first a dominant rational map $\phi : \mathcal{A}_g \to \mathbb{A}^G$ ($G = \dim \mathcal{A}_g$), defined over \mathbb{Q} , and finite above an open set $A \subset \mathbb{A}^G$. We may then take e.g. the box B(T) of integer points $(p_1, ..., p_G) \in A$ with $|p_i| \leq T$ and consider the a.v. $x \in \mathcal{A}_g$ such that $\phi(x) \in B(T)$. Each such x is defined over a number field (of bounded degree) and their number is $\gg T^G$. On the other hand, we have:

(i) Beyond the said complex-denseness, in a sense 'the majority' of p.p.a.v. defined over $\overline{\mathbb{Q}}$ are not isogenous to any Jacobian. We can express this vague meaning through estimates as follows.

Take first a dominant rational map $\phi : \mathcal{A}_g \to \mathbb{A}^G$ ($G = \dim \mathcal{A}_g$), defined over \mathbb{Q} , and finite above an open set $A \subset \mathbb{A}^G$. We may then take e.g. the box B(T) of integer points $(p_1, ..., p_G) \in A$ with $|p_i| \leq T$ and consider the a.v. $x \in \mathcal{A}_g$ such that $\phi(x) \in B(T)$. Each such x is defined over a number field (of bounded degree) and their number is $\gg T^G$. On the other hand, we have:

Theorem 2

The number of $x \in A_g$ with $\phi(x) \in B(T)$, which either are not ℓ -Galois-generic or which are isogenous to some Jacobian, is $\ll T^{G-\gamma}$ for some constant $\gamma > 0$.

Fields of definition of a.v. not isogenous to Jacobians

(ii) The very question of Katz-Oort concerns a minimal field of definition, so one seeks it as small as possible.

Fields of definition of a.v. not isogenous to Jacobians

(ii) The very question of Katz-Oort concerns a minimal field of definition, so one seeks it as small as possible.

- The CM examples coming from the proofs of CHAI-OORT and TSIMERMAN are automatically defined over $\overline{\mathbb{Q}}$, though the minimal degree of a number field of definition is expected to tend to infinity.

Fields of definition of a.v. not isogenous to Jacobians

(ii) The very question of Katz-Oort concerns a minimal field of definition, so one seeks it as small as possible.

- The CM examples coming from the proofs of CHAI-OORT and TSIMERMAN are automatically defined over $\overline{\mathbb{Q}}$, though the minimal degree of a number field of definition is expected to tend to infinity.

- Theorem 2 above instead produces infinitely many examples such that the degree of a number field of definition is bounded.

Fields of definition of a.v. not isogenous to Jacobians

(ii) The very question of Katz-Oort concerns a minimal field of definition, so one seeks it as small as possible.

- The CM examples coming from the proofs of CHAI-OORT and TSIMERMAN are automatically defined over $\overline{\mathbb{Q}}$, though the minimal degree of a number field of definition is expected to tend to infinity.

- Theorem 2 above instead produces infinitely many examples such that the degree of a number field of definition is bounded.

- More precisely, one can add to the above theorems the uniform bound 2^{16g^4} for the degree of a (variable !) number field of definition for the a.v. in question.

- For small g, \mathcal{A}_g is known to be unirational, even over \mathbb{Q} .

- For small g, \mathcal{A}_g is known to be unirational, even over \mathbb{Q} .

Example:

 $\overline{g=1}$: We have already noted that $\mathcal{A}_1=\mathbb{A}^1$.

g = 2: We have dim $A_2 = 3$ and we may parameterize rationally A_2 by points $(a, b, c) \in \mathbb{A}^3$, corresponding to the Jacobian of the curve $y^2 = x(x-1)(x-a)(x-b)(x-c)$ (so-called *Rosenhain coordinates*).

- For small g, \mathcal{A}_g is known to be unirational, even over \mathbb{Q} .

Example:

 $\overline{g=1}$: We have already noted that $\mathcal{A}_1=\mathbb{A}^1$.

g = 2: We have dim $A_2 = 3$ and we may parameterize rationally A_2 by points $(a, b, c) \in \mathbb{A}^3$, corresponding to the Jacobian of the curve $y^2 = x(x-1)(x-a)(x-b)(x-c)$ (so-called *Rosenhain coordinates*).

In these cases (which should include every $g \leq 5$) our a.v. can be also taken to be defined over \mathbb{Q} .

- For small g, \mathcal{A}_g is known to be unirational, even over \mathbb{Q} .

Example:

 $\overline{g=1}$: We have already noted that $\mathcal{A}_1=\mathbb{A}^1$.

g = 2: We have dim $A_2 = 3$ and we may parameterize rationally A_2 by points $(a, b, c) \in \mathbb{A}^3$, corresponding to the Jacobian of the curve $y^2 = x(x-1)(x-a)(x-b)(x-c)$ (so-called *Rosenhain coordinates*).

In these cases (which should include every $g \leq 5$) our a.v. can be also taken to be defined over \mathbb{Q} .

- It seems not known whether \mathcal{A}_6 is unirational, but for $g \geq 7$ FREITAG, MUMFORD, TAI proved that \mathcal{A}_g is of general type. Therefore, if we believe in the conjectures of LANG and VOJTA, the points in \mathcal{A}_g defined over any given number field should not be Zariski-dense, and we could **not hope** to answer affirmatively the general question with a **single** number field of definition.

When g = 1 the question is not sensible, but we may modify it by taking a *real-algebraic curve* $\mathcal{X} \subset \mathcal{A}_1(\mathbb{C}) = \mathbb{C}$ and asking a

When g = 1 the question is not sensible, but we may modify it by taking a *real-algebraic curve* $\mathcal{X} \subset \mathcal{A}_1(\mathbb{C}) = \mathbb{C}$ and asking a

Modified question: Do there exist elliptic curves defined over $\overline{\mathbb{Q}}$ and not isogenous to any curve with *j*-invariant in \mathcal{X} ?

When g = 1 the question is not sensible, but we may modify it by taking a *real-algebraic curve* $\mathcal{X} \subset \mathcal{A}_1(\mathbb{C}) = \mathbb{C}$ and asking a

Modified question: Do there exist elliptic curves defined over $\overline{\mathbb{Q}}$ and not isogenous to any curve with *j*-invariant in \mathcal{X} ?

Example: Let $\mathcal{X} = \{z \in \mathbb{C} : z + \overline{z} = 0\}.$

Now we are asking whether all elliptic curves over $\overline{\mathbb{Q}}$ are isogenous to some *E* with j(E) purely imaginary.

When g = 1 the question is not sensible, but we may modify it by taking a *real-algebraic curve* $\mathcal{X} \subset \mathcal{A}_1(\mathbb{C}) = \mathbb{C}$ and asking a

Modified question: Do there exist elliptic curves defined over $\overline{\mathbb{Q}}$ and not isogenous to any curve with *j*-invariant in \mathcal{X} ?

Example: Let $\mathcal{X} = \{z \in \mathbb{C} : z + \overline{z} = 0\}.$

Now we are asking whether all elliptic curves over $\overline{\mathbb{Q}}$ are isogenous to some *E* with j(E) purely imaginary.

We can prove results similar to the above ones, by (variation/simplification of) the same method. For instance:

Theorem 3

There exist elliptic curves defined over $\mathbb{Q}(i)$ and not isogenous to any elliptic curve E with $j(E) \in \mathcal{X}$.

Remarks.

(i) Note that in the theorem we cannot replace $\mathbb{Q}(i)$ by \mathbb{Q} (take $\mathcal{X} = \text{real line}$).

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

Remarks.

(i) Note that in the theorem we cannot replace $\mathbb{Q}(i)$ by \mathbb{Q} (take $\mathcal{X} = \text{real line}$).

(ii) Any elliptic curve over $\overline{\mathbb{Q}}$ is isogenous to some elliptic curve with *j*-invariant in a(ny) prescribed disk of \mathbb{C} .

Remarks.

(i) Note that in the theorem we cannot replace $\mathbb{Q}(i)$ by \mathbb{Q} (take $\mathcal{X} = \text{real line}$).

(ii) Any elliptic curve over $\overline{\mathbb{Q}}$ is isogenous to some elliptic curve with *j*-invariant in a(ny) prescribed disk of \mathbb{C} .

(iii) In fact, it may be easily proved that there exists a real *analytic* curve $\mathcal{X} \subset \mathbb{C}$ such that all elliptic curves over $\overline{\mathbb{Q}}$ are isogenous to some curve with *j*-invariant in \mathcal{X} . Hence that \mathcal{X} is algebraic is crucial. (Similarly for the case of abitrary *g*, discussed previously.)

We shall illustrate briefly some aspects of the proofs, in the simpler case of the analogue question for g = 1.

We shall illustrate briefly some aspects of the proofs, in the simpler case of the analogue question for g = 1.

Isogenies between elliptic curves.

Let E_1, E_2 be elliptic curves with *j*-invariants u_1, u_2 . We have $u_i = j(\tau_i)$ for some $\tau_i \in \mathcal{H} =$ upper-half plane $\{z : \Im z > 0\}$. We have E_i analytically isomorphic to $\mathbb{C}/(\mathbb{Z}\tau_i + \mathbb{Z})$.

Write $E_1 \sim E_2$, or $u_1 \sim u_2$, if they are isogenous. This amounts to

We shall illustrate briefly some aspects of the proofs, in the simpler case of the analogue question for g = 1.

Isogenies between elliptic curves.

Let E_1, E_2 be elliptic curves with *j*-invariants u_1, u_2 . We have $u_i = j(\tau_i)$ for some $\tau_i \in \mathcal{H}$ = upper-half plane $\{z : \Im z > 0\}$. We have E_i analytically isomorphic to $\mathbb{C}/(\mathbb{Z}\tau_i + \mathbb{Z})$.

Write $E_1 \sim E_2$, or $u_1 \sim u_2$, if they are isogenous. This amounts to (i) $\Phi_n(u_1, u_2) = 0$ where Φ_n is some modular polynomial, or equivalently

(ii) $\tau_2 = g\tau_1$ for some $g \in PGL_2(\mathbb{Q})$.

We shall illustrate briefly some aspects of the proofs, in the simpler case of the analogue question for g = 1.

Isogenies between elliptic curves.

Let E_1, E_2 be elliptic curves with *j*-invariants u_1, u_2 . We have $u_i = j(\tau_i)$ for some $\tau_i \in \mathcal{H}$ = upper-half plane $\{z : \Im z > 0\}$. We have E_i analytically isomorphic to $\mathbb{C}/(\mathbb{Z}\tau_i + \mathbb{Z})$.

Write $E_1 \sim E_2$, or $u_1 \sim u_2$, if they are isogenous. This amounts to (i) $\Phi_n(u_1, u_2) = 0$ where Φ_n is some modular polynomial, or equivalently

(ii) $\tau_2 = g\tau_1$ for some $g \in PGL_2(\mathbb{Q})$.

In general it may be quite difficult to decide whether two given elliptic curves (say over $\overline{\mathbb{Q}}$) are or are not isogenous (deep algorithms due to MASSER-WUESTHOLZ or FALTINGS-SERRE).

We want to exhibit a curve not \sim to anything in \mathcal{X} , with its *j*-invariant in a 'large' integer box $B = \{a + ib : |a|, |b| \le N\}$.

We want to exhibit a curve not \sim to anything in \mathcal{X} , with its *j*-invariant in a 'large' integer box $B = \{a + ib : |a|, |b| \le N\}$.

Step 1. We remove from *B* all points isogenous to something in \mathcal{X} by means of an isogeny of degree $\leq (\log N)^3$. Bounding deg Φ_n one proves there are $\ll N(\log N)^{10}$ such points.

We want to exhibit a curve not \sim to anything in \mathcal{X} , with its *j*-invariant in a 'large' integer box $B = \{a + ib : |a|, |b| \le N\}$.

Step 1. We remove from *B* all points isogenous to something in \mathcal{X} by means of an isogeny of degree $\leq (\log N)^3$. Bounding deg Φ_n one proves there are $\ll N(\log N)^{10}$ such points.

Step 2. If another point in *B* is $\sim x \in \mathcal{X}$ then the isogeny-degree *m* must be $> (\log N)^3$. By MASSER-WUESTHOLZ we find $m \ll d^5 \log N$ for d = degree of a field of definition of *x*. Then $d \gg m^c$, c > 0. We now take conjugates of *x* over $\mathbb{Q}(i)$ and obtain 'many' points $x_i \in \mathcal{X}$ all isogenous to *x*.

We want to exhibit a curve not \sim to anything in \mathcal{X} , with its *j*-invariant in a 'large' integer box $B = \{a + ib : |a|, |b| \le N\}$.

Step 1. We remove from *B* all points isogenous to something in \mathcal{X} by means of an isogeny of degree $\leq (\log N)^3$. Bounding deg Φ_n one proves there are $\ll N(\log N)^{10}$ such points.

Step 2. If another point in *B* is $\sim x \in \mathcal{X}$ then the isogeny-degree *m* must be $> (\log N)^3$. By MASSER-WUESTHOLZ we find $m \ll d^5 \log N$ for d = degree of a field of definition of *x*. Then $d \gg m^c$, c > 0. We now take conjugates of *x* over $\mathbb{Q}(i)$ and obtain 'many' points $x_i \in \mathcal{X}$ all isogenous to *x*.

Step 3. We interpret these isogenies in terms of corresponding $\tau_i \in \mathcal{H}$ (transcendental setting). We obtain 'many' $g_i \in PGL_2(\mathbb{Q})$, with estimates for their heights ($\ll m^C$).

Step 4. We view these g_i 's as rational points in a certain real-analytic variety $V \subset \mathbb{R}^4$. By results of PILA-WILKIE the number of rational points in such varieties can be estimated efficiently (by $\ll_{\epsilon} m^{\epsilon}$) if we stay out of the *algebraic part* of *V*.

Step 4. We view these g_i 's as rational points in a certain real-analytic variety $V \subset \mathbb{R}^4$. By results of PILA-WILKIE the number of rational points in such varieties can be estimated efficiently (by $\ll_{\epsilon} m^{\epsilon}$) if we stay out of the *algebraic part* of V.

Step 5. It turns out that either \mathcal{X} is modular (and then we conclude in an even simpler way) or this algebraic part is empty.

Step 4. We view these g_i 's as rational points in a certain real-analytic variety $V \subset \mathbb{R}^4$. By results of PILA-WILKIE the number of rational points in such varieties can be estimated efficiently (by $\ll_{\epsilon} m^{\epsilon}$) if we stay out of the *algebraic part* of V.

Step 5. It turns out that either \mathcal{X} is modular (and then we conclude in an even simpler way) or this algebraic part is empty.

Step 6. Then the estimates from above and below for the number of these rational points are contradictory for large enough N (thus large m) and $0 < \epsilon < c$, concluding the proof.

Now \mathcal{H} is replaced by the *Siegel space* \mathcal{H}_g , which somewhat uniformizes \mathcal{A}_g .

Now $\mathcal H$ is replaced by the Siegel space $\mathcal H_g$, which somewhat uniformizes $\mathcal A_g.$

The above pattern remains, though with new features; in particular:

Now \mathcal{H} is replaced by the Siegel space \mathcal{H}_g , which somewhat uniformizes \mathcal{A}_g .

The above pattern remains, though with new features; in particular:

(i) One uses SERRE's version of *Hilbert-irreducibility* for infinite degree extensions, so to obtain many ℓ -Galois generic objects.

Now \mathcal{H} is replaced by the Siegel space \mathcal{H}_g , which somewhat uniformizes \mathcal{A}_g .

The above pattern remains, though with new features; in particular:

(i) One uses SERRE's version of *Hilbert-irreducibility* for infinite degree extensions, so to obtain many ℓ -Galois generic objects.

(ii) One has to use the *Rosati length* in place of the degree of an isogeny. (This is technical, but crucial.)

Now \mathcal{H} is replaced by the Siegel space \mathcal{H}_g , which somewhat uniformizes \mathcal{A}_g .

The above pattern remains, though with new features; in particular:

(i) One uses SERRE's version of *Hilbert-irreducibility* for infinite degree extensions, so to obtain many ℓ -Galois generic objects.

(ii) One has to use the *Rosati length* in place of the degree of an isogeny. (This is technical, but crucial.)

(iii) The algebraic part of the relevant V is found to be a union of so-called *weakly special* subvarietes of \mathcal{A}_g , studied by authors like MOONEN, OORT, PINK,.... The theory yields that a weakly special proper subvariety containing a Hodge-generic point is itself a point, which allows to conclude.