Arithmetic and geometry:
3 conjectures about dense sets of points

Frans Oort

10-XII-2012

A talk in the joint colloquium of:

Department of Mathematics, *National Taiwan University* (NTUmath)
Institute of Mathematics, *Academia Sinica* (IoMAS)

0. Introduction. In this talk I discuss three *conjectures* in arithmetic geometry. They have a common aspect, and I will start by explaining the statements from that perspective.

In my talk I need three different *concepts* in algebraic geometry, and I will spend some time to explain these ideas, and to give illustrative examples.

The three conjectures:

(MM) The Manin-Mumford conjecture (folklore; first proofs: Raynaud, 1983).

(AO) The André-Oort conjecture (1989-1995).

(HO) The Hecke Orbit conjecture (FO, 1995).

We need the following concepts:

- Abelian varieties.
- Moduli spaces.
- The Zariski topology

With Ching-Li Chai together I have a long lasting cooperation (for the last 17 years). Several results below are tokens of that joint enterprise. I thank Ching-Li Chai heartily for sharing his deep insight with me, and for his open mind during our many discussions.

(1) Common formulation.
Let me first tell you (a much to vague) formulation of these conjectures.

General problem: **sets of points in a variety.**
These conjectures, in some sense, are very similar. We like to present first the general problem, specifying later all particulars in the three cases mentioned.

Study a variety V and a set of points $\Gamma \subset V$. In all examples the space V on the one hand has a *geometric* flavor, although it can be defined over a non-algebraically closed field (a number field, a finite field, a function field). On the other hand the set Γ, feeling like a discrete set of loose points in V, has an *arithmetic* flavour: viewing more and more points (in some cases), we have to enlarge the base field.

On can ask:

$$\boxed{\text{What is the closure } \Gamma \subset (\Gamma)^{\text{closure}} \subset V \ ?}$$

All three conjectures describe the possibilities for this closure for every possible Γ. In this way we obtain a bridge between the **arithmetic** (connected with points in Γ), and the **geometry**, of $(\Gamma)^{\text{closure}} \subset V$. We will discuss for what kind of topology the closure is considered.

As mentioned before, we will study 3 conjectures (notions involved to be explained later):

(MM) Manin-Mumford (folklore; first proofs: Raynaud, 1983).
$V = A$ an abelian variety, $\Gamma \subset \mathrm{Tors}(A(k))$; what is the closure of Γ?

(AO) The André-Oort conjecture (1989-1995).
$V = \mathcal{A}_g$ a moduli space, and Γ a set of "special points"; what is the closure of Γ?
`http://en.wikipedia.org/wiki/Andr%C3%A9%E2%80%93Oort_conjecture`

(HO) The Hecke Orbit conjecture (FO, 1995).
$V = \mathcal{A}_g$ a moduli space and $\Gamma = \mathcal{H}(x)$ a "Hecke orbit"; what is the closure of Γ?

As said, later I will introduce these concepts to you in detail. For the moment I just want to emphasize that these conjectures in arithmetic geometry all have the same appearance, with different main characters in the theater.

(2) An example: $\mathbb{Q}(\sqrt{-1}) \subset \mathbb{C}$.
We study the space $V = \mathbb{C}$, the one-dimensional affine space over the complex numbers. (We could write $V = \mathbb{A}^1_{\mathbb{C}}$ and consider $V(\mathbb{C}) = \mathbb{A}^1(\mathbb{C}) = \mathbb{C}$ to be precise.)

Consider an element $\tau \in \mathbb{C}$ such that $[\mathbb{Q}(\tau) : \mathbb{Q}] = 2$ and $\tau \notin \mathbb{R}$. Let $\Lambda := \mathbb{Z}{\cdot}1 + \mathbb{Z}{\cdot}\tau$. This is a *lattice* in $\mathbb{C}$ (a discrete subgroup, which generates $\mathbb{C}$ as an $\mathbb{R}$-vector space). Note that $\mathbb{Q}(\tau)$ is the set of division points of Λ: the set of $z \in \mathbb{Z}$ such that there exists $n \in \mathbb{Z}$ with $nz \in \Lambda$:

$$\mathbb{Q}(\tau) = \cup_n \ \frac{1}{n}{\cdot}\Lambda.$$

Write $\Gamma = \mathbb{Q}(\tau)$.

Claim. Γ is dense in $\mathbb{C}$, i.e.

$$\mathbb{Q}(\tau) =: \Gamma \subset (\Gamma)^{\text{closure}} = V := \mathbb{C}.$$

This looks very easy. However we will see that this will be the basic pattern for these conjectures.

I did not tell you which topology was considered, and rightfully you assumed that this is the "classical" topology.
However for the formulation of the conjectures we need a concept of "closure" that is different, central in algebraic geometry, which works over any base field, especially in arithmetic situations.

(3) The Zariski topology.

We study algebraic varieties, given by polynomial equations either in affine or in projective space, over an arbitrary ground field. Oscar Zariski (1899–1986) introduced a topology on any algebraic variety V by requiring that the *closed sets are finite unions of subvarieties* defined over that base field (and the whole set and the empty set are open and closed).
`http://en.wikipedia.org/wiki/Zariski_topology`
Easy exercise: this gives a topology on V.

At first sight this looks very strange. For example, the closed sets in an algebraic curve C are (the whole set C or) a finite set of points in C. We see immediately that this is not a Hausdorff space.

Is this useful?
Example. Let $V = \mathbb{C}$, and consider $S = (0,1) \subset \mathbb{R} \subset \mathbb{C}$, the interval of real points between 0 and 1. The Zariski closure of $S \subset S^{\mathrm{Zar}} = \mathbb{C} = V$ equals V (this is the only closed set containing an infinite set of points).

We are not playing an innocent games. Analyzing results (around 1822) by Poncelet (1788–1867) we see a “continuity principle”, something Poncelet was convinced it was true; he used it without giving a proof. Understanding the Zariski topology and the example $S^{\mathrm{Zar}} = \mathbb{C}$ just given we find a proof of this “principe de continuité” by Poncelet; see [1].

We can go much further. Modern algebraic geometry uses the Zariski topology in all kind of aspects (like cohomology of sheaves), and we see that this topology gives us the right approach.

All considerations below will use the Zariski topology.
Note. For a variety V over $\mathbb{C}$ the statement “Γ is classically dense in $V(\mathbb{C})$” implies “$\Gamma \subset V$ is Zariski dense”. The converse does not hold in general.

(4) Abelian varieties.

Definition of an abelian variety. Let K be a field. An abelian variety A over K is a group variety over K that is irreducible and projective.

Remark. Conditions in the definition imply that the group law on A is commutative.

However the name **abelian** variety did not originate in this commutativity, but in the fact that **Niels Henrik Abel** (1802–1829) constructed such varieties in order to compute integrals on a Riemann surface. That construction will appear later in my talk.

Torsion elements. For a commutative group G and $n \in \mathbb{Z}_{>0}$ we write

$$G[n] = \{g \in G \mid ng = 0\},$$

i.e. the subgroup of "n-torsion elements". We write

$$\mathrm{Tors}(G) := \cup_n \ G[n]$$

for the (subset) (subgroup of) all torsion elements.

For an abelian variety over K, with $k = \overline{k}$ an algebraically closed field containing K we will be interested in

$$\mathrm{Tors}(A(k)) = \cup_n \ A(k)[n],$$

the group of all torsion points on A.

Remark. You see that I take some care to study abelian varieties over some base field, although many points on A can only be studied over larger fields. Why? For arithmetic reasons, for applications in number theory, we like to obtain information on abelian varieties over a "small field" (such as a finite extension of $\mathbb{Q}$, a number field, or abelian varieties over a finite field). It turns out that such situations can provide methods and insight which gets lost over k. We will come back to this.

Examples of abelian varieties.
(4.1) Elliptic curves. Let $E \subset \mathbb{P}^2_K$ be a nonsingular, cubic curve with a rational point $0 \in E(K)$. This is an abelian variety. The theory of elliptic curves enters as essential tool in many mathematical proofs. The arithmetic of elliptic curves is one of the (most beautiful and) useful ingredients in recent results in number theory.

(4.2) Complex tori. Let A be an abelian variety of dimension g over $\mathbb{C}$. Let $\mathfrak{t} = \mathfrak{t}_{A,0}$ be the tangent space at the origin. A choice of a base gives $\mathfrak{t} \cong \mathbb{C}^g$. From the theory of commutative complex Lie groups we obtain a homomorphism $\exp : \mathfrak{t} \to A(\mathbb{C})$. This homomorphism is surjective and its kernel $\Lambda \subset \mathfrak{t}$ is a discrete subgroup (use the fact that $A(\mathbb{C})$ is compact). We obtain an exact sequence: **Complex uniformization**

$$0 \to \mathbb{Z}^{2g} \cong \Lambda \longrightarrow \mathfrak{t} \cong \mathbb{C}^g \longrightarrow \ A(\mathbb{C}) \to 0,$$

$$A(\mathbb{C}) \cong \mathfrak{t}/\Lambda \cong \mathbb{C}^g/\mathbb{Z}^{2g}.$$

Comments. (a) The map $\mathbb{C}^g \to \ A(\mathbb{C})$ is also the covering map by the universal covering as topological spaces, and we conclude that $\Lambda \cong \pi_1(A(\mathbb{C}), 0)$ is the fundamental group.
(b) For elliptic curves, $g = 1$ all of this was constructed by Weierstrass (1815–1897):

$$\exp = [\wp : \wp' : 1] : \mathfrak{t} \cong \mathbb{C} \longrightarrow E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}).$$

(c) Let E be an elliptic curve over $\mathbb{Q}$. The geometry and topology of $E(\mathbb{C})$ are well-understood, as we have seen. However the arithmetic of E over $\mathbb{Q}$ does not follow from this. E.g. how can we find the structure of the group $E(\mathbb{Q})$ only knowing $E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z}{\cdot}1 + \mathbb{Z}{\cdot}\tau)$?
(d) Conversely, for $g > 1$ there exist complex tori $\mathbb{C}^g/\Lambda$ which do not come from an abelian variety. This part of the theory (i.e. which complex tori are algebraizable) is well-understood: Lefschetz (1884–1972), and many others.

(4.3) The Jacobian of an algebraic curve. Let X be an algebraic curve (non-singular, irreducible and projective) over a field K. There exists an abelian variety $J = \mathrm{Jac}(X)$, uniquely determined by X, and $\mathrm{genus}(X) = g = \dim(J)$ (we will not enter into the definition and the construction; relevant: the theory of *Picard varieties* and of *Albanese varieties*).

Conversely, for $g > 3$ there are "many" abelian varieties that are not isomorphic with the Jacobian of a curve. Below we will come back to this aspect.
Comment. The Jacobian of a rational curve is trivial. Any curve of genus $g > 1$ does not allow a group structure. It is this aspect that make elliptic curves interesting and useful: these are the only curves that are abelian varieties at the same time.
Comment. The Jacobian of a curve reflects cohomology of that curve: the geometry makes the abstract algebra related to the curve geometric. This point of view has many applications.

(4.4) Abelian varieties over a finite field. An abelian variety A over a finite field $K = \mathbb{F}_q$ with $q = p^n$ has a homomorphism

$$\pi = \pi_A : A \to A \text{ defined by } \pi(x_0 : x_1 : \cdots : x_N) = (x_0^q : x_1^q : \cdots : x_N^q).$$

(**Note**: as A is defined over $\mathbb{F}_q$ this indeed defines a map from A into itself.) This is called the *Frobenius* homomorphism. A deep theorem by Adré Weil (1906–1998) says:
Theorem (Weil). *For every homomorphism*

$$\psi : \mathbb{Z}[\pi_A] \to \mathbb{C}, \ \textit{we have} \ \mid \psi(\pi_A) \mid = \sqrt{q}.$$

Furthermore a theorem by Honda (1932–1975) and Tate (1925–) says conversely that any algebraic integer with this property (a Weil q-number) comes as the Frobenius of an abelian variety over $\mathbb{F}_q$. Such numbers can be easily constructed, and these (deep) theorems show the existence of an abelian variety with arithmetic properties which can be computed. See [19] and see [15] for an overview and many references

Open problem. In the Honda-Tate theory (for abelian varieties over a finite field) the only known proof uses complex uniformization. *Does there exist a proof using (only) methods from algebraic geometry*?

Dense sets of torsion points.

Theorem. *Let A be an abelian variety over a field K of dimension* $\dim(A) = g$. *Let* $n \in \mathbb{Z}_{>0}$ *be a positive integer* **not divisible by the characteristic of K.** *Then*

$$A(k)[n] \cong (\mathbb{Z}/n)^{2g}.$$

Comments. (a) A proof over $K \subset \mathbb{C}$ using complex uniformization is easy.
(b) An algebraic proof of this fact is available over any base field.
(c) The condition "*n is not divisible by the characteristic of K*" is essential; without this condition the conclusion of the theorem is false.

Theorem. *Let B be an abelian variety over a field K. Let $k \supset K$ be an algebraically closed field. The set of torsion points* $\mathrm{Tors}(B(k))$ *is Zariski dense in B:*

$$(\mathrm{Tors}(B(k)))^{\mathrm{Zar}} = B.$$

Comments. For an abelian variety over $\mathbb{C}$ this density is easy to show (using complex uniformization).

For an abelian variety A over a finite field K this density is easy to show: $A(\mathbb{F}_q)$ is a finite commutative group, hence all such points are torsion, hence $A(\mathbb{F}) = \mathrm{Tors}(A(\mathbb{F})) \subset A$, for $\mathbb{F} := \overline{\mathbb{F}_p}$, is dense.

(5) The Manin-Mumford conjecture. Let A be an abelian variety over a field K. Let $K \subset k$ be an algebraic closure. Consider a set $\Gamma \subset \mathrm{Tors}(A(k))$. What is the Zariski closure Γ^{Zar} of this set. For example, suppose that $X \subset A$ is an *algebraic curve* contained in A; what is the Zariski closure

$$(X \cap \mathrm{Tors}(A(k)))^{\mathrm{Zar}} \overset{?}{=} ?$$

Either this intersection is finite, or this intersection is not finite, and in that case $(X \cap \mathrm{Tors}(A(k)))^{\mathrm{Zar}} = X$.

First formulation of this conjecture:
(5.1) For an *algebraic curve* $X \subset A$ over $\mathbb{C}$

$$\#(X \cup \mathrm{Tors}(A(k))) = \infty \Longleftrightarrow (X \cap \mathrm{Tors}(A(k)))^{\mathrm{Zar}} = X \Longleftrightarrow X = E,$$

where $E = X \subset$ is an elliptic curve containing at least one torsion point of A.

Note. If $\beta \in \mathrm{Tors}(A(k))$ and $B \subset A$ is an abelian subvariety then the torsion points of A contained in $X = \beta + B$ give a dense subset of X.

Comment. Replacing $\mathbb{C}$ by $\overline{\mathbb{F}_p}$ gives a very wrong statement $\cdots$.
Question. How to formulate a version of (MM) over a finite field?

The Manin-Mumford conjecture, general version.
Work over k, an algebraically closed field *of characteristic zero. Let $X \subset A$ be any (Zariski) closed subset. Then* $(X \cap \mathrm{Tors}(A(k)))^{\mathrm{Zar}} = X$ *(i.e. there is a set of torsion points on A contained in X dense in X) if and only if*

$$X = \cup_i^{<\infty} \ (\beta_i + B_i)$$

where $\beta_i \in \mathrm{Tors}(A(k))$ and $B_i \subset A$ is an abelian subvariety fore every i.

Clearly $\cup_i^{<\infty} \ (\beta_i + B_i)$ contains a dense set of torsion points. The conjecture says that these are the only cases.

This conjecture has been proved, the first proofs (in 1983) by Raynaud (1938–). Later several other proofs appeared. It seems that this is now fairly well understood.

`http://en.wikipedia.org/wiki/Arithmetic-of-abelian-varieties`

D. Roessler – *A note on the Manin-Mumford conjecture.* [A] van der Geer, Gerard (ed.) et al., Number fields and function fields – two parallel worlds. Boston, MA: Birkhuser. Prog. Math. 239, 311-318 (2005).
Summary: R. Pink and the author [in: Proc. ICM 2002, Beijing, China, Vol. I, 539–546 (2002; Zbl 1026.14012)] gave a short proof of the Manin-Mumford conjecture, which was inspired by an earlier model-theoretic proof by Hrushovski. The proof given in [loc. cit.] uses a difficult unpublished ramification-theoretic result of Serre. It is the purpose of this note to show how the proof given in [loc. cit.] can be modified so as to circumvent the reference to Serre's result. J. Oesterlé and R. Pink contributed several simplifications and shortcuts to this note.

(6) Moduli spaces.
We try to classify, to parametrize isomorphism classes of geometric objects. This enterprise has a long history. For algebraic curves and for abelian varieties this has been well-understood by now: recent work by Grothendieck (1928–) and Mumford (1937–), building on classical results and questions, give a complete picture. This is a rich topic. Here we only mention the *moduli space of polarized abelian varieties.* This exists over the base ring $\mathbb{Z}$ (thus enabling to compare results of $\mathbb{C}$ with results in characteristic p). Here is the classical description:

Here is the theory for $g = 1$, the case of elliptic curves. Let $\mathfrak{h}_1 = \{z \in \mathbb{C} \mid \Im(z) > 0\}$, the "Siegel upper half plane". The group $\Delta = \mathrm{SL}_2(\mathbb{Z})/\{\pm 1\}$ acts on $\mathfrak{h}_1$ (in a well-known way), and this action is properly discontinuous; we have

$$\mathcal{A}_1(\mathbb{C}) \quad \cong \quad \Delta\backslash\mathfrak{h}_1,$$

where $j(E) \in \mathbb{C} = \mathcal{A}_1(\mathbb{C})$ corresponds with

$$j(E) \quad \leftrightarrow \quad (\tau \bmod \Delta) \qquad \text{iff} \quad E(\mathbb{C}) \cong \mathbb{C}/(\mathbb{Z}{\cdot}1 + \mathbb{Z}{\cdot}\tau).$$

This gives a complete classification of elliptic curves (up to isomorphism) over $\mathbb{C}$.

An elliptic curve E with $\mathbb{Z} \subsetneqq \mathrm{End}(E)$ is said to be a CM elliptic curve (CM stands for Complex Multiplication). In case E is over $\mathbb{C}$ and $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, any element of $\mathrm{End}(E)$ can be given by a complex multiplication $\times z : \mathbb{C} \to \mathbb{C}$ with $z{\cdot}\Lambda \subset \Lambda$.

Description of $\mathcal{A}_g(\mathbb{C})$.
Choose $g \in \mathbb{Z}_{\geq 1}$ and take $K = \mathbb{C}$ as base field.
Define:

$$\mathfrak{h}_g := \{\tau \in (\mathbb{C}^g)^g = \mathrm{Mat}(g \times g, \mathbb{C}) \mid \tau = {}^t\tau, \;\; \Im(\tau) > 0\};$$

this is called the "Siegel upper half space"; if (A, λ) is a principally polarized abelian variety then there exist $\tau \in \mathbb{C}^g$, and isomorphism $A(\mathbb{C}) \cong T_\tau$ such that:

the matrix τ is symmetric, i.e. $\tau = {}^t\tau$;
the matrix $\Im(\tau)$ is positive definite.

Conversely, if $\tau \in \mathfrak{h}_g$, the complex torus T_τ is algebraizable, and the standard hermitian form gives a principal polarization. Moreover, $T_\tau \cong T_\sigma$ iff there exists

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}) : \quad \sigma = (A\tau + B)(C\tau + D)^{-1}.$$

One shows that the action of $\mathrm{Sp}_{2g}(\mathbb{Z})$ operating in this way on $\mathfrak{h}_g$ is properly discontinuous, and that there is an isomorphism of complex spaces: there exists a variety $\mathcal{A}_g$ over $\mathbb{C}$ with

$$\mathcal{A}_g(\mathbb{C}) \quad \cong \quad \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathfrak{h}_g$$

where $[(A, \lambda)] = x \in \mathcal{A}_g(\mathbb{C})$ corresponds with

$$x \quad \leftrightarrow \quad (\tau \bmod \mathrm{Sp}_{2g}(\mathbb{Z})) \quad \text{iff} \quad A(\mathbb{C}) = \mathbb{C}^g/\Lambda_\tau.$$

(I did not define the notion of a polarization on an abelian variety, please ignore this detail in case you do not know the definition.)

CM **abelian varieties. Special points, special subvarieties.**
A simple abelian variety B over a field of dimension g is said to admit sufficiently many complex multiplications if $\mathrm{End}^0(B)$ contains a subfield of degree $2g$ over $\mathbb{Q}$.

We say that the moduli point $[(A, \lambda)] = x \in \mathcal{A}_g$ is a CM-point; instead of this terminology we will, equivalently, say that $x \in \mathcal{A}_g$ is a special point:

$$\boxed{\text{CM-point in } \mathcal{A}_g \quad = \quad \text{special point in } \mathcal{A}_g.}$$

Easy observation. Write $\mathrm{CM}(\mathcal{A}_g)$ for the set of CM points in $\mathcal{A}_g(\mathbb{C})$. We can see: $\mathrm{CM}(\mathcal{A}_g) \subset \mathcal{A}_g(\mathbb{C})$ is classically dense. Hence this set is Zariski dense in $\mathcal{A}_g$. For $g = 1$ we can use considerations mentioned in (2).

Question. Let $\Gamma \subset \mathrm{CM}(\mathcal{A}_g) \subset (\mathcal{A}_g)_{\mathbb{C}}$ be some set of CM points. What could be the Zariski closure of Γ?
Example. Let $(\mathcal{T}_g)_{\mathbb{C}} \subset (\mathcal{A}_g)_{\mathbb{C}}$ be the Torelli locus consisting of Jacobians of algebraic curves over $\mathbb{C}$. Write $\mathrm{CM}(\mathcal{T}_g) = \mathcal{T}_g \cap \mathrm{CM}(\mathcal{A}_g)$. What is the closure of $\mathrm{CM}(\mathcal{T}_g)$?
(Difficulty: a curve X determines $\mathrm{Jac}(X)$, but in general endomorphisms of J are difficult to describe in the geometry of X.)
Example. Let $m \geq 2$ be a prime number. Consider curves given by (an affine equation) $Y^m = X(X-1)(X-\lambda)$ for variable λ this gives a family of curves in $\mathcal{A}_g$ with $g = m-1$. What are the CM points in this family?
(2), $g = 1$**.** Already for $m = 2$, the case of elliptic curves this is not obvious; we can see that the number of CM curves in this family is infinite, but it is hard to write down “all” vales of λ for which this takes place.
(3), $g = 1$**.** For $m = 3$ all such curves are geometrically isomorphic: there is only one curve, and it gives a CM Jacobian.
($m = 5, m = 7$**),** $g = 4, 6$**.** For $m = 5$ and $m = 7$ the number of CM Jacobians in this family is infinite.
($m =$ **prime** ≥ 11**),** $g = m - 1$**.** For a prime number at least 11 we expect the number of CM Jacobians in this family to be finite, ?! Can we explain why this should be true?

(7) The André-Oort conjecture.

AO The André-Oort conjecture (1989-1995)
`http://en.wikipedia.org/wiki/Andr%C3%A9%E2%80%93Oort_conjecture`
`http://en.wikipedia.org/wiki/Shimura_variety`

Definition. A *special subvariety*, or a special subset, S of $\mathcal{A}_g = \mathcal{A}_{g,1} \otimes \mathbb{C}$ is:

- a (Zariski-) closed (algebraic) subvariety $S \subset \mathcal{A}_g$, such that
- there exist an algebraic subgroup $H \subset \mathrm{Sp}(2g)$ defined over $\mathbb{Q}$, and
- a CM-point $x = (\tau \bmod \mathrm{Sp}_{2g}(\mathbb{Z})) \in A(\mathbb{C}) = \mathbb{C}^g/\Lambda_\tau$ with
- $$\Pi(H(\mathbb{R})^+ \cdot \tau) = S \subset \mathcal{A}_g(\mathbb{C});$$
  here $\Pi : \mathfrak{h}_g \to \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathfrak{h}_g = \mathcal{A}_g(\mathbb{C})$ is the natural projection.

Remark / warning. In general for a subgroup $H \subset \mathrm{Sp}(2g)$ and a CM-point $x \in A(\mathbb{C})$ the set $\Pi(H(\mathbb{R})^+ \cdot \tau)$ is not Zariski closed. Here is an easy example; consider the subgroup $H \subset \mathrm{SL}_2$ consisting of matrices $\begin{pmatrix} 1 & T \\ 0 & 1 \end{pmatrix}$. Clearly this is an algebraic subgroup defined over $\mathbb{Q}$. However, for any $x \in A(\mathbb{C})$ the set $\Pi(H(\mathbb{R})^+ \cdot \tau)$ is not Zariski closed.

Property. *Let V be a Shimura variety,* (or: $V = (\mathcal{A}_g)_\mathbb{C}$) *and let $S \subset V$ be a special subvariety. The set of special points in S is dense in S.*
By "dense" we mean Zariski dense in S, but the set of special points is also dense in $S(\mathbb{C})$ in the classical topology.

One can wonder whether the "converse" of this is true:

(AO) Conjecture (Yves André and Frans Oort). *Let V be a Shimura variety;* (or: $V = (\mathcal{A}_g)_\mathbb{C}$;) *let $\Lambda \subset V(\mathbb{C})$ be a set of special points. Then* (?) *the Zariski closure of Λ inside V is a finite union of special subvarieties.* Or: *If a subvariety $S \subset V$ contains a Zariski-dense set of special points, then* (?) *S is a special subvariety.*

Comment. There is a striking analogy between (MM) on the one hand and (AO) on the other hand. In fact this was the motivation for formulating this conjecture.

Many partial results have been proved. It seems that the general case now is proved (either under GRH or unconditionally).

An **analogy** (MM) ↔ (AO).
Define $\beta + B \subset A$ to be a "torsion subvariety" of an abelian variety A over $\mathbb{C}$.
In (MM) the closure of a set of torsion points is a finite union of torsion subvarieties.
In (AO) we expect the closure of a set of special points to be a finite union of a special subvarieties.
Moreover we can "feel" the moduli space $\mathcal{A}_g$ as a group object. In fact in some cases (Serre-Tate parameters, I will not enter into details) the CM points are precisely the torsion points.

We see that "translating" (MM) terminology and theory into special points in (AO) the conjecture is natural.

However this is an analogy: proofs for (MM) do not translate into proofs for (AO) as far as I know.

(8) An application of AO: abelian varieties not isogenous to a Jacobian.
We can construct abelian varieties by taking an algebraic curve C (say non-singular and projective) and construct its Jascobian $J = J_C = \mathrm{Jac}(C)$. Moreover we can construct even more abelian varieties by considering isogenies $J \to J/N$. Can we construct all abelian varieties in this way? We say that abelian varieties A, B are *isogenous* if there exists a surjective homomorphism $A \to B$ with finite kernel.

We ask geometry for help and insight. We see that (over a base field K) the moduli space $\mathcal{T}_g$ of Jacobians for curves of genus g is a closed subset of $\mathcal{A}_g$, and (for $g > 3$) we have:

$$\mathcal{T}_g \subset \mathcal{A}_g, \quad \dim(\mathcal{T}_g) = 3g - 3 < g(g+1)/2 = \dim(\mathcal{A}_g).$$

Hence our question does make sense.

In fact: *for every $g \in \mathbb{Z}_{>3}$ there exists an abelian variety A over $K = \mathbb{C}$ such that there is no curve C with an isogeny $J_C \to J_C/N \cong A$.*
We sketch a proof. All abelian varieties isogenous to a Jacobian are on a countable union of "Hecke translates" of $\mathcal{T}_g$, hence on a countable union of lower dimensional subvarieties (for $g > 3$). As $\mathbb{C}$ is *uncountable* this shows the existence of a point outside this countable union of lower dimensional subvarieties. □

However is the base field is countable this proof breaks down.

Theorem (Ching-Li Chai & Frans Oort, Jakob Tsimerman). *For every $g > 3$ there exists an abelian variety A over $k := \overline{\mathbb{Q}}$ not isogenous to a Jacobian.*
See [7], [20].

Open problem *Does there exist for every $g > 3$ an abelian variety A over $k := \overline{\mathbb{F}_p}$ not isogenous to a Jacobian ?*
Perhaps the question in itself is not interesting, but it may be the starting point in finding new methods in geometry over finite fields.

(9) HO: The Hecke Orbit conjecture (FO, 1995).

We say that abelian varieties A, B are *isogenous* if there exists a surjective homomorphism $A \to B$ with finite kernel. For a point $x \in \mathcal{A}_g$ defining an abelian variety A we consider the *Hecke orbit* of x consisting of all points belonging to abelian varieties isognous with A. We write $\mathcal{H}(x) \subset \mathcal{A}_g$.

Easy. For every $x \in \mathcal{A}_g(\mathbb{C})$ its Hecke orbit $\mathcal{H}(x) \subset \mathcal{A}_g$ is classically dense. Hence it is Zariski dense.
For a proof one can use complex uniformization

$$\mathfrak{h}_g \to \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathfrak{h}_g = \mathcal{A}_g(\mathbb{C})$$

and the fact that $\mathrm{Sp}_{2g}(\mathbb{Q}) \subset \mathrm{Sp}_{2g}(\mathbb{R})$ is classically dense.

Note that for $g = 1$ any Hecke orbit is non-finite, hence for elliptic curves Zariski density of $\mathcal{H}(x) \subset \mathcal{A}_1(\mathbb{C})$ follows easily.

We change our point of view. We fix a prime number. We write $\mathcal{A}_g$ for the space of polarized abelian varieties of dimension g over a field of characteristic p. We wonder:

$$\boxed{\text{Given } x \in \mathcal{A}_g, \text{ what is } (\mathcal{H}(x))^{\mathrm{Zar}} \text{ ?}}$$

Easy example. Study elliptic curves, $g = 1$, in characteristic $p > 0$.
(ord) For an elliptic curve which does have a torsion point of exact order p, such an elliptic curve is called *ordinary*, one can show that its isogeny class (say over an algebraically closed field) is non-finite. Hence in this case for $x = j(E) \in \mathcal{A}_1$ we have

$$(\mathcal{H}(x))^{\mathrm{Zar}} = \mathcal{A}_1.$$

(ss) For every p there exists an ellliptic curve with no torsion points of exact order p. Such an elliptic curve is called *supersingular*. For every p the number of supersingular j-values is finite. Hence the Hecke orbit of a supersingular j-value is *not dense*. In fact in this case:

$$\mathcal{H}(x) = (\mathcal{H}(x))^{\mathrm{Zar}} \subsetneqq \mathcal{A}_1.$$

One can show that the number of supersingular j-values is close to $p/(12)$.

Both Ching-Li Chai and I started thinking about what could be the Zariski closure of a Hecke orbit in positive characteristic (although our approaches initially were very different.

An abelian variety of dimension g in characteristic p is called *ordinary* if

$$\#(A(k)[p]) = p^g$$

(the maximal possible number of p-torsion elements).

For an abelian variety in characteristic p one defines its Newton polygon, which is basically the Newton polygon of the characteristic polynomial of the Frobenius morphisms (one has to do some work to give a good and precise definition). One shows that the Newton polygon does not change under isogenies. Moreover Grothendieck (1928–) and Katz (1943–) showed that a Newton polygon ξ defines a closed subset $W_\xi \subset \mathcal{A}_g$ where almost all abelian varieties have Newton polygon equal to ξ; hence in that case

$$\mathcal{H}(x) \subset W_\xi.$$

In case $g = 1$ this explains everything: there are only two Newton polygons possible, and we have seen what $(\mathcal{H}(x))^{\mathrm{Zar}}$ is in both cases.

Theorem (Ching-Li Chai, 1995). *For every p, for every g and $x \in \mathcal{A}_g$ an ordinary point,*

$$\mathcal{H}(x)^{\mathrm{Zar}} = \mathcal{A}_g.$$

(The easy proof in characteristic zero can be taken as motivation for stating this result, but the proof here is deep and quite involved.) See [2], [4].

(HO) Conjecture (FO, 1995) *For every $x \in \mathcal{A}_g$ belonging to the Newton Polygon ξ*

$$\mathcal{H}(x)^{\mathrm{Zar}} = W_\xi \subset \mathcal{A}_g.$$

See [10]. This conjecture has been proved by Ching-Li Chai and FO (and we are currently writing down a proof). See [3], [16]. In one stage of the argument we need a result by Chia-Fu Yu, see [21].

Does this mean work is finished? Here are some open problems.

(AO) *in positive characteristic.*

For this powerful conjecture/theory we cannot offer an analogous problem in positive charactersitic. At several occasions Ching-Li Chai and I thought we had a good candidate, but every time we found out that we were on the wrong track. Some fundamentally new insight seems necessary.

(AVff) *classification of isogeny classes of abelian varieties over finite fields.*

Can we give a proof of the Honda-Tate theory using methods of algebraic geometry? the fact that we know the theorem and a proof, but that we do not have a conceptually better proof shows we still do not understand the essence of the problem (I think).

(HO) *the Hecke orbit problem.*

Already many years Ching-Li Chai and I try to find a better, more direct proof of our theorem. Also here, the statement is clear, but a more general structure (doing also this for Shimura varieties) and better insight in the interplay between Hecke actions and deformation theory seems necessary.

Abelian varieties not isogenous to a Jacobian.

We expect that for any $g > 3$ and any p there exsits an abelian variety over $\overline{\mathbb{F}_p}$ not isogenous to a Jacobian. We have tried several attempts, and we know of several colleagues who sought to show this. The fact that we cannot access this problems seems ot indicate that the is some lack of insight in some fundamental structure behind this problem.

Mathematicians are curious.
Asking questions cries for structure behind the problem.

As Yuri Manin (1937–) once said:

"Good proofs are proofs that make us wiser."

" I see the process of mathematical creation as a kind of recognizing a preexisting pattern."
See [9].

References

[1] H. Bos, C. Kers, F. Oort & D. Raven – *Poncelets closure theorem.* Expos. Math. **5** (1987), 269–364.

[2] C.-L. Chai – *Every ordinary symplectic isogeny class in positive characteristic is dense in the moduli.* Invent. Math. **121** (1995), 439–479.

[3] C.-L. Chai – *Hecke orbits on Siegel modular varieties.* Geometric Methods in Algebra and Number Theory (Ed. Fedor Bogomolov,Yuri Tschinkel). 71–
`http://www.cims.nyu.edu/ tschinke/princeton/papers/.miami/submitted/chai.pdf`

[4] C.-L. Chai & F. Oort – *Moduli of abelian varieties and p-divisible groups.* Clay Mathematics Proceedings, Vol. 8. Arithmetic geometry, Clay Mathematics Institute Summer School, Gttingen 2006 (Editors: H. Darmon, D. Ellwood, B. Hassett and Y. Tschinkel). AMS, Clay Math. Proc., 8, Amer. Math. Soc., Providence, RI, 2009; pp. 441–536.

[5] C.-L. Chai & F. Oort – *Hypersymmetric abelian varieties.* Pure and Applied Mathematics Quarterly **2** (2006), 1–27 [Special Issue: In honor of John H. Coates]

[6] C.-L. Chai & F. Oort - *Monodromy and irreducibility of leaves.* Ann. Math. **173** (2011), pp. 1359 – 1396.
`http://annals.math.princeton.edu/2011/173-3/p03`

[7] C.-L. Chai & F. Oort – *Abelian varieties isogenous to a Jacobian.* Ann. of Math. **176** (2012), 589–635.

[8] A. J. de Jong & F. Oort – *Purity of the stratification by Newton polygons.* Journ. Amer. Math. Soc. **13** (2000), 209 - 241.

[9] Yu. Manin – *Good proofs are proofs that make us wiser.* Interview by Martin Aigner and Vasco A. Schmidt. The Berlin Intelligencer, 1998, pp. 16–19.

[10] F. Oort, *Some questions in algebraic geometry.* Unpublished manuscript, June 1995. Available at `http://www.math.uu.nl/people/oort/`.

[11] F. Oort, *Minimal p-divisible groups.* Ann. of Math. **161** (2005), 1 – 16.

[12] F. Oort, *Simple p-kernels of p-divisible groups.* Advances in Mathematics **198** (2005), 275 - 310. Special volume in honor of Michael Artin: Part I - Edited by Aise Johan De Jong, Eric M. Friedlander, Lance W. Small, John Tate, Angelo Vistoli , James Jian Zhang.

[13] F. Oort - *Foliations in moduli spaces of abelian varieties.* Journ. Amer. Math. Soc. 17 (2004), 267 – 296.

[14] F. Oort - *Foliations in moduli spaces of abelian varieties and dimension of leaves.* Algebra, Arithmetic and Geometry: In Honor of Yu. I. Manin (Manin Festschrift; Eds:Y. Tschinkel and Yu. Zarhin), Vol. II, Progress in Mathematics Vol. 270, Birkhuser, (2009); pp. 465 – 501.

[15] F. Oort, *Abelian varieties over finite fields.* Summer School on "Varieties over finite fields", Göttingen, 25-VI — 6-VII-2007. Higher-dimensional geometry over finite fields. Proceedings of the NATO Advanced Study Institute 2007 (Editors: Dmitry Kaledin, Yuri Tschinkel). IOS Press, 2008, pp. 123 – 188.

[16] F. Oort, *Moduli of abelian varieties in mixed and in positive characteristic.* The Handbook of Moduli (G. Farkas, I, Morrison, editors), Vol. III, pp. 75–134.. [To appear in 2012.]

[17] F. Oort & Th. Zink – *Families of p-divisible groups with constant Newton polygon.* http://arXiv.org/abs/math/0209264 Documenta Mathematica **7** (2002), 183 – 201, see http://www.mathematik.uni-bielefeld.de/documenta http://www.mathematik.uni-bielefeld.de/documenta/vol-07/09.html

[18] J. Tate – *Endomorphisms of abelian varieties over finite fields.* Invent. Math. **2** (1966), 134 – 144.

[19] J. Tate, *Class d'isogenie des variétés abéliennes sur un corps fini* (d'après T. Honda). Séminaire Bourbaki, 1968/69, no. 352. Lecture Notes Math. 179, Springer-Verlag, 1971, 95–110.

[20] J. Tsimerman – *The existence of an abelian variety over $\overline{\mathbb{Q}}$ isogenous to no Jacobian.* Ann. of Math. **176** (2012), n 637–650.

[21] C.-F. Yu – *Discrete Hecke orbit problems for Hilbert-Blumenthal varieties.* NCTS/TPE-Math Technical Report 2006-1, 20 pp, 1-20.

[22] T. Zink, *On the slope filtration.* Duke Math. J. **109** (2001), 79 - 95.

[23] T. Zink, *De Jong-Oort purity for p-divisible groups.* Algebra, Arithmetic and Geometry - Volume II: In Honor of Yu. I. Manin (Manin Festschrift; Editors: Y. Tschinkel and Yu. Zarhin), Progress in Mathematics Vol. 270, Birkhäuser, (2009); pp. 693 – 701 .

Frans Oort
Mathematisch Instituut
P.O. Box. 80.010
NL - 3508 TA Utrecht
The Netherlands
email: f.oort@uu.nl