Abelian varieties over finite fields

Frans Oort (Utrecht University)

Ieder nadeel heb zijn voordeel.
Johan Cruijff
(Every disadvantage have its advantage.)

The Lenstra Treurfeest — A farewell conference,
in honor of Hendrik W. Lenstra jr
Berkeley, 21/22/23 - III - 2003
Informal notes. Not for publication

Some ideas, principles of thought and proof:

- *Study abelian varieties over finite fields, but also abelian varieties varying in a family* **number theory ánd geometry**.
- A well-know technique in algebraic geometry: *study structures by degenerations.* For abelian varieties in characteristic p we do not degenerate the abelian variety, but specialize the p-structure, "go to the boundary", and draw conclusions for the starting position.
- *Supersingular abelian varieties* show a totally different behavior in contrast with non-supersingular abelian varieties.

1 Sufficiently many Complex Multiplications, smCM.

(1.1) Definition. An abelian variety A of dimension g over a field K is said to admit *sufficiently many Complex Multiplications*, abbreviated smCM, iff $\mathrm{End}^0(A)$ contains a commutative semi-simple algebra of rank $2g$ over $\mathbb{Q}$. An abelian variety which admits smCM we will call a CM abelian variety. If confusion could arise we will say "sufficiently many Complex Multiplications over K".

Equivalently: write $A \sim \sum B_i$ up to isogeny as a direct sum of K-simple abelian varieties; A is said to admit smCM iff every $\mathrm{End}^0(B_i)$ contains a number field of degree $2{\cdot}\mathrm{dim}B_i$ over $\mathbb{Q}$.

(1.2) Remarks. For an elliptic curve E smCM is equivalent with $\mathrm{End}(E) \neq \mathbb{Z}$.

Confusion might arise when we say "A has complex multiplications" because it might mean smCM, or it might mean $\mathrm{End}(A) \neq \mathbb{Z}$, different concepts for $\mathrm{dim}A > 1$.

For a simple abelian variety A over $\mathbb{C}$ the notion smCM is equivalent with the fact that $\mathrm{End}^0(A) = L$ is a field of degree $2{\cdot}\mathrm{dim}A$ over $\mathbb{Q}$. In this case the field L is a CM-field. The field L together with the action $\iota : L \to \mathrm{End}(\mathfrak{t}_{A,0})$ on the tangent space is called a CM-type. The notions smCM and CM-type are related, but not the same.

In general $\mathrm{End}^0(A)$ is not a field; for example the endomorphism algebra of a supersingular elliptic curve E over $m := \overline{\mathbb{F}_p}$ equals $Q_{p,\infty}$, the quaternion algebra over $\mathbb{Q}$ ramified precisely at p and ∞. If A (is simple and) has smCM, and $E = \mathrm{End}^0(A)$ is a field, then $E/\mathbb{Q}$ is a CM-field, and the Rosati involution is complex conjugation.

For an abelian variety over a field K, and an extension $K \subset L$ of fields it can happen that $\mathrm{End}(A) \subsetneqq \mathrm{End}(A \otimes_K L)$. It can happen that A does not admit smCM (over K) and $A \otimes_K L$ does admit smCM (over L). Be careful, e.g. some people say "E is an elliptic curve over $\mathbb{Q}$ with complex multiplications" meaning that E is defined over $\mathbb{Q}$, and that there exists an extension $K \subset L$ such that $\mathrm{End}(E \otimes_K L)$ is an imaginary quadratic field.

An abelian variety over $\mathbb{C}$ has smCM, is of CM-type, iff its Mumford-Tate group is commutative; see [3], page 63, [21], page 347.

2 (1966) J. Tate: A over $\mathbb{F}_q$.

(2.1) Theorem (1966, Tate). *An abelian variety over a finite field admits* smCM.
See [45]. For elliptic curves this was proved earlier by M.Deuring.

(2.2) Definition. *Let $q = p^n$ be a prime power. An algebraic integer λ is called a q-Weil number if for every embedding $\varphi : \mathbb{Q}(\lambda) \to \mathbb{C}$ we have $|\varphi(\lambda)| = \sqrt{q}$. We say that λ and λ' are* conjugate *if there exists an isomorphism $\mathbb{Q}(\lambda) \cong \mathbb{Q}(\lambda')$ sending $\lambda \mapsto \lambda'$*

(2.3) Let $K = \mathbb{F}_q$, let A be an abelian variety over K and let $\pi_A := F^n : A \to A^{(q)} = A$ be its K-Frobenius endomorphism. A. Weil proved that π_A is a q-Weil number.

(2.4) *Let K be a finite field, let A and B be K-simple abelian varieties. Suppose π_A and π_B are conjugate. Then A and B are K-isogenous.*
This follows from [45]: see [46], page 99.

3 (1967-1968) Abelian varieties over finite fields: Honda-Serre-Tate theory.

(3.1) Theorem (Honda - Serre - Tate). *Let $K = \mathbb{F}_q$. There is a bijection between the set of K-isogeny classes of K-simple abelian varieties and the set of conjugacy classes of q-Weil numbers given by $A \mapsto \pi_A$.*

For every abelian variety A over $m := \overline{\mathbb{F}_p}$ there exists an m-isogeny $A \sim B_0$, and an abelian variety B in characteristic zero which is a lift of B_0, such that B has smCM.

For details and references, see [46]; also see [43].

(3.2) Remark. In this theory we find a proof of a conjecture by Manin, see [19], page 76: *For every prime number p and every symmetric Newton polygon there exists an abelian variety A over a finite field K of characteristic p with this Newton polygon.*
See [46], page 98. For a pure characteristic p proof, see [17], Section 5.

(3.3) Remark / Question. As Mumford-Norman-FO proved, see [25], see [24], every abelian variety can be lifted from characteristic p to characteristic zero.

Can we lift every abelian variety defined over a finite field to a CM abelian variety in characteristic zero? See (6.2).

4 (1968 - 1973) Grothendieck's theorem on smCM.

(4.1) It is not difficult to show: An abelian variety with smCM over $\mathbb{C}$ is defined over a finite extension of $\mathbb{Q}$ (i.e. over a number field).

It is easy to see: There are abelian varieties in positive characteristic with smCM which cannot be defined over a finite field.

Keeping these in mind we can appreciate:

(4.2) Theorem (Grothendieck). *Let K be a field, let A be an abelian variety over K with* smCM. *We write $k = \overline{K}$. There exists a finite extension L of the prime field of K, an abelian variety B over L, and an isogeny $A \otimes k \sim B \otimes k$*
See [22], Th. on page 220; see [29].

I.e. "*the isogeny class of A with smCM can be defined over a finite extension L of the prime field $\mathbb{P}$ of K*: either $\mathbb{P} = \mathbb{Q}$, with $[L : \mathbb{Q}] < \infty$, and L is a number field, or $\mathbb{P} = \mathbb{F}_p$, and $L = \mathbb{F}_q$ is a finite field.

(4.3) Remark. Here is an ingredient of the proof. Suppose that k is an algebraically closed field, S an irreducible scheme, algebraic and smooth over k. Let $A \to S$ an abelian scheme. Let $\eta \in S$ be the generic point. Let ℓ be a prime number different from the characteristic of k. We obtain a representation

$$\rho_{A,\ell} = \rho : \pi_1(S, \overline{\eta}) \to \mathrm{Aut}(T_\ell(A_\eta)).$$

Suppose that the image of $\rho_{A,\ell}$ is *finite*. Then there exists a finite surjective morphism $T \to S$, an abelian variety B over k and an isogeny $B \times_{\mathrm{Spec}(k)} T \to A \times_S T$; moreover, in characteristic zero this isogeny can be chosen to be an isomorphism, and in positive characteristic it can be chosen to be purely inseparable.

5 (1974) H. W. Lenstra & FO: CM can be a field.

In general the endomorphism algebra of an abelian variety is not a field, even not in case of a simple CM abelian variety. Clearly, a supersingular abelian variety over m has a non-commutative endomorphism ring. However:

(5.1) Theorem (H. W. Lenstra jr & FO). *Suppose given a prime number p and a symmetric Newton polygon ξ. Assume $\xi \neq \sigma$;* i.e. ξ has at least one slope not equal to $\frac{1}{2}$. *There exist "many"* CM-*fields L and abelian varieties A over $m := \overline{\mathbb{F}_p}$ such that* $\mathrm{End}^0(A) \cong L$.
See [17].

We can easily see that for a given $\xi \neq \sigma$ all fields L satisfying the theorem above have an intersection which equals $\mathbb{Q}$. Hence:

(5.2) Corollary. *For every $\xi \neq \sigma$ there exists an abelian variety A over an algebraically closed field k of characteristic p with* $\mathrm{End}(A) = \mathbb{Z}$ *such that the Newton polygon of A equals ξ.*

(5.3) Remark. Why is this interesting? We can determine the number of geometrically irreducible components of W_σ using the endomorphism algebra of a supersingular abelian variety, see [18], 4.9. Then, I had the vague hope that, using the fact recorded in the corollary might give access tot the irreducibility of W_ξ of $\xi \neq \sigma$; up to now, this attempt failed.

(5.4) Remark. A non-trivial deformation of a CM abelian variety *in characteristic zero* produces a non-CM abelian variety; this can be seen by using the complex theory describing a complex torus by a lattice; the analogous statement is false in positive characteristic (many examples can be given). I would like to show the result of the corollary above via a general method which would enable us to determine the endomorphism algebra of the generic fiber of a deformation; up to now, I do not know such a theory.

6 (1992) CM-liftings.

Suppose given a field A_0 over a finite field (hence, by Tate, a CM abelian variety). Can we lift this to a CM abelian variety in characteristic zero? In the Honda - Serre - Tate theory we see that there exists an abelian variety B_0 over $m = \overline{\mathbb{F}_p}$ with $B_0 \sim A_0 \otimes m$ which can be lifted to a CM abelian variety in characteristic zero: *the isogeny class of $A_0 \otimes m$ can be CM-lifted.* Can we construct CM-liftings up to isomorphism? As we shall see, in general the answer is negative.

(6.1) It is easy to see: If A_0 is an abelian variety over m of dimension g, with p-rank $f(A_0) \geq g-1$ then there exists a CM-lifting of A_0 to characteristic zero. The case $f(A_0) = g$ is called the *ordinary case*; I say A_0 is *almost ordinary* if $f(A_0) = g-1$.

(6.2) Theorem. *Let p be a prime number, and let ξ be a symmetric Newton polygon. Assume that $\xi \neq \sigma$ and suppose that $f(\xi) < g-1$. Then there exist infinitely many abelian varieties over m with Newton polygon equal to ξ which cannot be CM-lifted to characteristic zero.*
See [33].

7 (2002) C.-L. Chai: Monodromy.

(7.1) Theorem (C.-L. Chai). *Let $Z \subset \mathcal{B} := \mathcal{A}_{g,1,N} \otimes k$ be a locally closed subscheme, smooth over* $\mathrm{Spec}(k)$ *where $k = \overline{k} \supset \mathbb{F}_p$, and $N \in \mathbb{Z}_{\geq 3}$ not divisible by p. Let ℓ be a prime number not dividing pN. Assume:*
(i) *Z is Hecke-ℓ-stable, and*
(ii) *the Hecke-ℓ-action on the set $\pi_0(Z)$ is transitive, and*
(iii) $\eta \notin W_\sigma$ (equivalently: Z contains a non-supersingular point).
Consider an irreducible component Z^0 of Z, with generic point $\eta \in Z^0$. Then:

$$\rho_{A,\ell} : \pi_1(Z^0, \overline{\eta}) \longrightarrow \mathrm{Sp}(T_\ell, <,>_\ell) \cong \mathrm{Sp}_{2g}(\mathbb{Z}_\ell)$$

is surjective, *and*

$$Z \textit{ is irreducible, i.e. } Z = Z^0.$$

See [2], 4.4.

(7.2) From this theorem by Chai we have another proof of Corollary (5.2).

8 (2002) Irreducibility of NP-strata.

(8.1) For the supersingular stratum $W_\sigma \subset \mathcal{A}_{g,1} \otimes \overline{\mathbb{F}_p}$ the number of components is given by class numbers:

$$\#(\pi_0(W_\sigma)) = H_g(p,1) \quad \text{if} \quad g \quad \text{is odd},$$

$$\#(\pi_0(W_\sigma)) = H_g(1,p) \quad \text{if} \quad g \quad \text{is even}.$$

We see that (in general, i.e. for p large) the supersingular locus is reducible. See [18], 4.9. For non-supersingular strata the situation is totally different:

(8.2) Theorem. *For every $\xi \supsetneqq \sigma$ the locus $W_\xi \subset \mathcal{A} = \mathcal{A}_{g,1} \otimes \mathbb{F}_p$ is* geometrically irreducible. I.e.

$$\xi \neq \sigma \quad \Rightarrow \quad \#(\pi_0(W_\xi)) = 1.$$

This was expected as Conjecture 8B in [34].

(8.3) Here are some of the ingredients in a proof of this theorem:
(i) *For every symmetric Newton polygon ξ the inclusion*

$$W_\sigma \subset W_\xi \subset \mathcal{B} := \mathcal{A}_{g,1,N} \otimes k$$

defines a well defined map $\pi_0(W_\sigma) \to \pi_0(W_\xi)$ which is surjective (EO-strata, and much more....);
(ii) *the action of Hecke on $\pi_0(W_\sigma)$ is transitive* (precise information on W_σ, see [18]);
(iii) *hence the action of Hecke-ℓ on $\pi_0(W_\sigma) \twoheadrightarrow \pi_0(W_\xi)$ is transitive* (use strong approximation);
(iv) *then apply* (7.1).

Epilogue. The Honda - Serre - Tate theory has provided us with strong tools. Geometric aspects give additional methods. Combining these two aspects (arithmetic ánd geometry) we obtain beautiful results. Here are some of such aspects as discussed above:

- a proof of the Manin conjecture: by the Honda-Serre-Tate theory, see [46], or by a geometric proof, see [36];
- an answer to the question of CM-liftability: first use number theory, as in [17], then use geometry: families of abelian varieties, and finish with CM-theory in characteristic zero, as in [33];
- use representation theory, the RH for abelian varieties over finite fields (Weil) and Grothendieck's semi-simplicity theorem to arrive at (7.1), then use geometry and number theory, see (8.3) to arrive at (8.2).

These are just a few examples of a rich and ever growing interaction between number theory and geometry.

Not all references below are needed for this talk, but I include relevant literature for completeness sake.

References

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

[2] C.-L. Chai – *Monodromy of Hecke-invariant subvarieties.* Manuscripts 22 - XI - 2002; 7 pp.

[3] P. Deligne – *Hodge cycles on abelian varieties.* Hodge cycles, motives and Shimura varieties (Eds P. Deligne et al). Lect. Notes Math. **900**, Springer – Verlag 1982; pp. 9 - 100.

[4] M. Deuring – *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Sem. Univ. Hamburg **14** (1941), 197 - 272.

[5] S. J. Edixhoven, B. J. J. Moonen & F. Oort (Editors) – *Open problems in algebraic geometry.* Bull. Sci. Math. **125** (2001), 1 - 22.
See: http://www.math.uu.nl/people/oort/

[6] T. Ekedahl – *On supersingular curves and abelian varieties.* Math. Scand. **60** (1987), 151 - 178.

[7] G. van der Geer – *Cycles on the moduli space of abelian varieties.* In: *Moduli of curves and abelian varieties.* Ed: C. Faber & E. Looijenga. Aspects Math., E33, Vieweg, Braunschweig, 1999; pp 65–89.

[8] A. Grothendieck – *Groupes de Barsotti-Tate et cristaux de Dieudonné.* Sém. Math. Sup. **45**, Presses de l'Univ. de Montreal, 1970.

[9] T. Ibukiyama, T. Katsura & F. Oort - *Supersingular curves of genus two and class numbers.* Compos. Math. **57** (1986), 127 - 152.

[10] T. Katsura & F. Oort - *Families of supersingular abelian surfaces.* Compos. Math. **62** (1987), 107 - 167.

[11] T. Katsura & F. Oort - *Supersingular abelian varieties of dimension two or three and class numbers.* Algebraic geometry, Sendai 1985 (Ed. T. Oda). Adv. Stud. in Pure Math. **10** (1987), Kinokuniya Cy Tokyo and North-Holland Cy Amsterdam, 1987 ; pp. 253 - 281.

[12] A. J. de Jong – *Homomorphisms of Barsotti-Tate groups and crystals in positive characteristics.* Invent. Math. **134** (1998) 301-333, Erratum **138** (1999) 225.

[13] A. J. de Jong & F. Oort – *Purity of the stratification by Newton polygons.* J. Amer. Math. Soc. **13** (2000), 209-241. See: http://www.ams.org/jams/2000-13-01/

[14] N. M. Katz – *Slope filtration of F–crystals.* Journ. Géom. Alg. Rennes, Vol. I, Astérisque **63** (1979), Soc. Math. France, 113 - 164.

[15] H.-P. Kraft – *Kommutative algebraische p-Gruppen (mit Anwendungen auf p-divisible Gruppen und abelsche Varietäten).* Sonderforsch. Bereich Bonn, September 1975. Ms. 86 pp.

[16] H.-P. Kraft & F. Oort – *Finite group schemes annihilated by p.* [In preparation.]

[17] H. W. Lenstra jr & F. Oort – *Simple abelian varieties having a prescribed formal isogeny type.* Journ. Pure Appl. Algebra **4** (1974), 47 - 53.

[18] K.-Z. Li & F. Oort – *Moduli of supersingular abelian varieties.* Lecture Notes Math. 1680, Springer - Verlag 1998.

[19] Yu. I. Manin – *The theory of commutative formal groups over fields of finite characteristic.* Usp. Math. **18** (1963), 3-90; Russ. Math. Surveys **18** (1963), 1-80.

[20] Elena Mantovan – *On certain unitary group Shimura varieties.* Harvard PhD-thesis, April 2002.

[21] D. Mumford – *A note of Shimura's paper "Discontinuous groups and abelian varieties".* Math. Ann. **181** (1969), 345 - 351.

[22] D. Mumford – *Abelian varies.* Tata Inst. Fund Research and Oxford Univ. Press 1970 (2nd printing 1974).

[23] P. Norman – *An algorithm for computing moduli of abelian varieties.* Ann. Math. **101** (1975), 499 - 509.

[24] P. Norman – *Lifting abelian varieties.* Invent. Math. **64** (1981), 431 - 443.

[25] P. Norman & F. Oort – *Moduli of abelian varieties.* Ann. Math. **112** (1980), 413 - 439.

[26] T. Oda & F. Oort – *Supersingular abelian varieties.* Itl. Sympos. Algebr. Geom. Kyoto 1977 (Ed. M. Nagata). Kinokuniya Book-store 1987, pp. 3 - 86.

[27] A. Ogus – *Supersingular K3 crystals.* Journ. Géom. Algébr., Rennes 1978, Vol. II. Astérisque **64**, Soc. Math. France 1979, 3 - 86

[28] F. Oort – *Commutative group schemes.* Lect. Notes Math. 15, Springer - Verlag 1966.

[29] F. Oort – *The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field.* Journ. Pure Appl. Algebra **3** (1973), 399 - 408.

[30] F. Oort – *Subvarieties of moduli spaces.* Invent. Math. **24** (1974), 95 - 119.

[31] F. Oort – *Which abelian surfaces are products of elliptic curves?* Math. Ann. **214** (1975), 35 - 47.

[32] F. Oort – *Moduli of abelian varieties and Newton polygons.* Compt. Rend. Acad. Sc. Paris **312** Sér. I (1991), 385 - 389.

[33] F. Oort – *CM-liftings of abelian varieties.* Journ. Algebraic Geometry **1** (1992), 131 - 146.

[34] F. Oort – *Some questions in algebraic geometry,* preliminary version. Manuscript, June 1995. http://www.math.uu.nl/people/oort/

[35] F. Oort – *A stratification of a moduli space of polarized abelian varieties.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 345 - 416.

[36] F. Oort — *Newton polygons and formal groups: conjectures by Manin and Grothendieck.* Ann. Math. **152** (2000), 183 - 206.

[37] F. Oort – *Newton polygon strata in the moduli space of abelian varieties.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 417 - 440.

[38] F. Oort – *Foliations in moduli spaces of abelian varieties.* [To appear] See: http://www.math.uu.nl/people/oort/

[39] F. Oort – *Minimal p-divisible groups.* [To appear] See: http://www.math.uu.nl/people/oort/

[40] F. Oort & Th. Zink – *Families of p-divisible groups with constant Newton polygon.* Documenta Mathematica **7** (2002), 183 – 201. See http://www.mathematik.uni-bielefeld.de/ documenta

[41] V. Platonov & A. Rapinchuk – *Algebraic groups and number theory.* Academic Press 1994.

[42] T. Shioda – *Supersingular K3 surfaces.* In: *Algebraic Geometry,* Copenhagen 1978 (Ed. K. Lønsted). Lect. Notes Math. 732, Springer - Verlag (1979), 564 - 591.

[43] W. Waterhouse – *Abelian varieties over finite fields.* Ann. scient. Éc. Norm. Sup. 4e Ser. **2** (1969), 521 - 560.

[44] T. Wedhorn – *The dimension of Oort strata of Shimura varieties of* PEL*-type.* In: *Moduli of abelian varieties.* (Ed. C. Faber, G. van der Geer, F. Oort). Progress Math. 195, Birkhäuser Verlag 2001; pp. 441 - 471.

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

[46] J. Tate – *Classes d'isogénies de variétés abéliennes sur un corps fini (d'àpres T. Honda).* Sém. Bourbaki **21** (1968/69), Exp. 352.

[47] Th. Zink – *The display of a formal p-divisible group.* [To appear in Astérisque.]

[48] Th. Zink – *On the slope filtration.* Duke Math. J. Vol. **109** (2001), 79-95.

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