Complex Multiplication

Ching-Li Chai

Department of Mathematics
University of Pennsylvania

Colloquium, University of Minnesota, April 29, 2010

Outline

Elliptic curves

§1 Review of elliptic curves

- Weistrass theory
- the j-invariant
- CM elliptic curves

Elliptic curves basics

Equivalent definitions of an `elliptic curve` E:

- a projective curve with an algebraic group law;
- a projective curve of genus one together with a rational point (= the origin);
- over $\mathbb{C}$: a complex torus of the form $E_\tau = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$, where $\tau \in \mathfrak{H} :=$ upper-half plane;
- over a field F with $6 \in F^\times$: given by an affine equation

$$y^2 = 4x^3 - g_2 x - g_3, \quad g_2, g_3 \in F.$$

Weistrass theory

For $E_\tau = \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$, let

$$\begin{aligned} x_\tau(z) &= \wp(\tau, z) \\ &= \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z - m\tau - n)^2} - \frac{1}{(m\tau + n)^2} \right) \end{aligned}$$

$y_\tau(z) = \frac{d}{dz}\wp(\tau, z)$

Then E_τ satisfies the Weistrass equation

$$y_\tau^2 = 4x_\tau^3 - g_2(\tau)\,x_\tau - g_3(\tau)$$

with

- $g_2(\tau) = 60 \displaystyle\sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^4}$
- $g_3(\tau) = 140 \displaystyle\sum_{(0,0)\neq(m,n)\in\mathbb{Z}^2} \frac{1}{(m\tau+n)^6}$

The j-invariant

Elliptic curves are classified by their j-invariant

$$j = 1728 \frac{g_2^3}{g_2^3 - 27 g_3^2}$$

Over $\mathbb{C}$, $j(E_\tau)$ depends only on the lattice $\mathbb{Z}\tau + \mathbb{Z}$ of E_τ. So $j(\tau)$ is a `modular function` for $\mathrm{SL}_2(\mathbb{Z})$:

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau)$$

for all $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$.

We have a Fourier expansion

$$j(\tau) = \frac{1}{q} + 744 + 196884\, q + 21493760\, q^2 + \cdots,$$

where $q = q_\tau = e^{2\pi\sqrt{-1}\,\tau}$.

CM elliptic curves

Let E be an elliptic curve over $\mathbb{C}$. Then for $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ we have

$$\mathrm{End}^0(E) := \begin{cases} \mathbb{Z}, \text{or} \\ \text{an imaginary quadratic field } K \end{cases}$$

In the latter case, E is said to admit `complex multiplication`, i.e.

- $\mathrm{End}(E)$ is an `order` in an imaginary quadratic field K
- $E(\mathbb{C}) \cong \mathbb{C}/\mathbb{Z}\tau + \mathbb{Z}$ for some $\tau \in K$.

CM curves in history

§2 CM elliptic curves in the history of arithmetic

- Fermat
- Euler
- congruent numbers

Portraits of Fermat & Euler

Figure: Fermat

Figure: Euler

Fermat

§2 CM elliptic curves in the history of arithmetic

1. The two Diophantine equations considered by Fermat,

$$x^4 + y^4 = z^2$$

and

$$x^3 + y^3 = z^3$$

both correspond to elliptic curves, with affine equations

$$u^4 + 1 = v^2$$

and

$$u^3 + v^3 = 1$$

respectively.

Fermat's curves, continued

The first curve $u^4+1=v^2$ admits a non-trivial automorphism

$$(u,v) \mapsto (\sqrt{-1}u,v),$$

so has endomorphisms by $\mathbb{Z}[\sqrt{-1}]$.

Fermat's method of descent for this curve is a 2-descent, applied to the endomorphism $[2]=[1-\sqrt{-1}]\circ[1+\sqrt{-2}]$.

The second curve $u^3+v^3=1$ has a non-trivial automorphism

$$(u,v) \mapsto (e^{2\pi\sqrt{-1}/3}u,v),$$

so has endomorphisms by $\mathbb{Z}[(-1+\sqrt{-3})/2]$.

Euler

2. The birth of the theory of elliptic functions hands of Euler in 1751 (Euler's addition theorem) was stimulated by Fagnano's remarkable discovery:

The differential equation

$$\frac{dx}{\sqrt{1-x^4}} = \frac{dy}{\sqrt{1-y^4}}$$

has a `rational integral`

$$x^2y^2 + x^2 + y^2 = 1\,.$$

The curve $u^2 = 1 - x^4$ is an elliptic curve with endomorphism by $\mathbb{Z}[\sqrt{-1}]$.

Congruent numbers

3. Three equivalent formulations of a property for a positive square-free integer n:

- (Diophantus, `Arithmetica` V.7, III.19, around 250 AD; anonymous Arabic manuscript, before 972) $\exists\delta \in \mathbb{Q}$ such that $\delta^2 - n, \delta^2 + n \in \mathbb{Q}^{\times 2}$.
- $\exists$ a right triangle with `rational` sides and area n.
- The cubic equation $y^2 = x^3 - n^2 x$ has a rational solution (a, b) with $b \neq 0$.
  Note that this elliptic curve has endomorphism by $\mathbb{Z}[(-1+\sqrt{-3})/2]$.

Congruent numbers, continued

An integer n satisfying these equivalent properties is called a `congruent number`.

For instance 5 is a congruent number:

- $(41/12)^2 - 5 = (31/12)^2$, $(41/12)^2 + 5 = (49/12)^2$
- $(3/2)^2 + (20/3)^2 = (41/6)^2$, $5 = (1/2) \times (3/2) \times (20/3)$.

Fermat proved that 1 and 2 are not congruent numbers.
Zagier showed that $n = 153$ is a congruent number, where the denominator of δ has 46 digits.

CM theory for elliptic curves

§3 CM theory for imaginary quadratic fields:
From Kronecker to Weber/Fueter and Hasse/Deuring.

- Kronecker's Jugentraum
- explicit reciprocity law for imaginary quadratic fields
- $\sqrt[3]{j}$ and $\sqrt{j-1728}$ for imaginary quadratic fields with class number 1.

Protrait of Kronecker

Figure: Kronecker

Kronecker's Jugentraum

Kronecker (1853), Weber(1886) proved:

> *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field,*

i.e. a field generated by the values of of function $\exp(2\pi\sqrt{-1}x)$ at rational numbers.

Kronecker's `Jugendtraum`: special values of elliptic functions should be enough to generate all abelian extensions of imaginary quadratic fields.

General idea: `generate abelian extensions by special values of useful functions.`

For imaginary quadratic fields, carried out by

- Weber, Lehrbuch der Algebra, Bd. 3, 1906),
- Fueter, I(1924), II(1927);
- Hasse (1927, 1931), and
- Deuring (1947, 1952)

Portraits of Weber & Fueter

Figure: Weber

Figure: Fueter

Photos of Hasse & Deuring

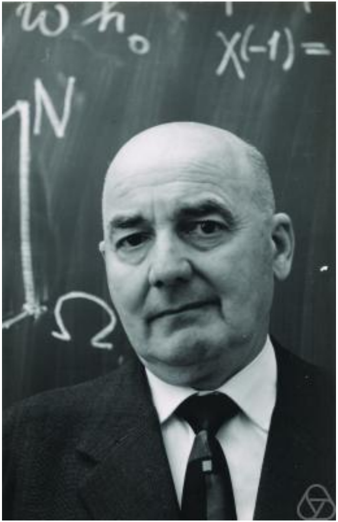

Figure: Hasse

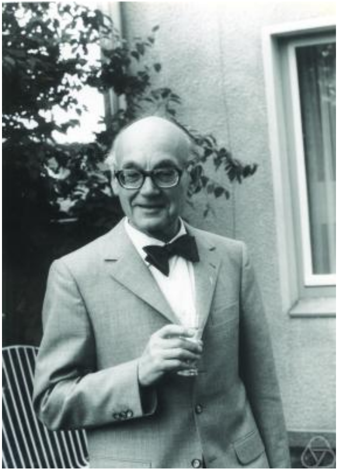

Figure: Deuring

CM curves and class fields

Let E be an elliptic curve s.t. $\mathscr{O} = \mathrm{End}(E)$ is an order $\mathscr{O}$ in an imaginary quadratic field K.

Theorem

- *$j(E)$ is an algebraic integer, and $K(j(E))$ is the* `ring class field` *of K attached to the order $\mathscr{O}$.*
- *If $\mathscr{O} = \mathscr{O}_K$ then $j(E)$ is the Hilbert class field H_K of K, i.e. the maximal unramified abelian extension of K; its Galois group is the ideal class group of K.*
- *If $\sigma \in \mathrm{Gal}(H_K/K)$ corresponds to an $\mathscr{O}_K$-ideal I, then ${}^{\sigma^{-1}}j(\mathbb{C}/J) = j(\mathbb{C}/I\cdot J)$ for every $\mathscr{O}_K$-ideal J.*
- *In particular if $h_K = 1$, then $j(\mathbb{C}/\mathscr{O}_K) \in \mathbb{Z}$; moreover $j(\mathbb{C}/\mathscr{O}_K)$ is a* `cube`*.*

Cubic root of singular j-values

For the 9 imaginary quadratic fields of class number 1

$$j(\sqrt{-1}) = 1728 = 2^6 \cdot 3^3$$
$$j(\sqrt{-2}) = 8000 = 2^6 \cdot 5^3$$

	$j(\frac{-1+\sqrt{-p}}{2})$
$p=3$	0
$p=7$	$-3^3 \cdot 5^3$
$p=11$	-2^{15}
$p=19$	$-2^{15} \cdot 3^3$
$p=43$	$-2^{18} \cdot 3^3 \cdot 5^3$
$p=67$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
$p=163$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

$$j(\tau) = \frac{1}{q} + 744 + 196884\,q + O(q)\,, \quad q = e^{2\pi\sqrt{-1}\,\tau}$$

$e^{\pi\sqrt{163}}$=262537412640768743.99999999999925007259...

$$j(\tfrac{-1+\sqrt{-163}}{2}) = -262537412640768000$$

Square root of $(j-1728)/(-p)$

	$j\left(\frac{-1+\sqrt{-p}}{2}\right)-1728$
$p=3$	$-3\cdot 2^6\cdot 3^2$
$p=7$	$-7\cdot 3^6$
$p=11$	$-11\cdot 2^6\cdot 7^2$
$p=19$	$-19\cdot 2^6\cdot 3^6$
$p=43$	$-43\cdot 2^6\cdot 3^8\cdot 7^2$
$p=67$	$-67\cdot 2^6\cdot 3^6\cdot 7^2\cdot 31^2$
$p=163$	$-163\cdot 2^6\cdot 3^6\cdot 7^2\cdot 11^2\cdot 19^2\cdot 127^2$

§4 Modern CM theory:
From Shimura/Taniyama to Deligne/Langlands.

Use moduli coordinates of abelian varieties with lots of symmetries (endomorphisms) to generate abelian extensions of CM fields.

Photos of Shimura & Taniyama

Figure: Shimura

Figure: Taniyama

Abelian varieties basics

- An `abelian variety` over a field is a complete group variety.
- Over $\mathbb{C}$ an abelian variety "is" a compact complex torus which can be embedded into a complex projective space.
- A homomorphism between abelian varieties is an `isogeny` if it is surjective with a finite kernel.
- Every abelian variety is `isogenous` to a product of simple abelian varieties.
- An abelian variety A has `sufficiently many complex multiplication` (smCM) if $\mathrm{End}^0(A) \supset$ a commutative semisimple algebra E with $\dim_{\mathbb{Q}}(E) = 2\dim(A)$.

CM fields

- A `CM field` L is a totally imaginary quadratic extension of a totally real field.
  - Then the complex conjugation ι is in the center of $\mathrm{Gal}(L^{\mathrm{nc}}/\mathbb{Q})$.
- If A is a simple abelian variety over $\mathbb{C}$ with smCM, then $\mathrm{End}^0(A)$ is a CM field.
- If A is an `isotypic` abelian variety with smCM, then $\mathrm{End}^0(A)$ contains a CM field.

CM types

- Let $(A, L \hookrightarrow \mathrm{End}^0(A))_{/\mathbb{C}}$, be an abelian variety with endomorphisms by a CM field L, $[L:\mathbb{Q}] = 2\dim(A)$.
  - $\mathrm{Lie}(A)$ corresponds to a subset $\Phi \subset \mathrm{Hom}(L,\mathbb{C})$ with $\mathrm{Hom}(L,\mathbb{C}) = \Phi \sqcup {}^{\iota}\Phi$.
  - Φ is called the `CM type` of $(A, L \hookrightarrow \mathrm{End}^0(A))$.
  - (L,Φ) determines $(A, L \hookrightarrow \mathrm{End}^0(A))$ up to L-linear isogeny.
- The `reflex field` of a CM type Φ for a CM field $L \subset \mathbb{C}$ is, equivalently,
  (a) $\mathbb{Q}\left(\sum_{\sigma\in\Phi} \sigma(x)\right)_{x\in L}$
  (b) the `field of definition` of $\Phi \subset \mathrm{Hom}(L,\mathbb{C})$, a subset of a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-set.

CM moduli towers

Let L be a CM field and let Φ be a CM type for L.

Moduli tower attached to (L, Φ)

1. For every (sufficiently small) compact open subgroup $\Lambda \subset \prod_w \mathscr{O}_{L,w} \subset \mathbb{A}_{L,f}$, let $\mathscr{X}_{L,\Phi,K}$ be the moduli space of quadruples
$$(A, L \hookrightarrow \mathrm{End}^0(A), \lambda, \bar{\psi})$$
where
   - λ is a polarization of A up to $\mathbb{Q}^\times$ s.t. L is stable under the Rosati involution Ros_λ
   - ψ is a K-coset of a L-linear polarization $\psi : L/\mathscr{O}_L \xrightarrow{\sim} A_{\mathrm{tor}}$
2. Let $\mathscr{X}_{L,\Phi} = \{\mathscr{X}_{L,\Phi,K}\}_K$ be the projective system of moduli spaces $\mathscr{X}_{L,\Phi,K}$, indexed by compact open subgroups
$$K \subseteq \prod_w \mathscr{O}_{L,w} \subset \mathbb{A}_{L,f}$$

Main CM theorem

Shimura/Taniyama

1. (significance of the reflex field) The moduli tower $\mathscr{X}_{L,\Phi}$ is defined over the reflex field $L' = \mathrm{ref}(L,\Phi)$.
2. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/L')$ on $\mathscr{X}_{L,\Phi}$ factors through $\mathrm{Gal}(L'^{\mathrm{ab}}/L')$.
3. (Shimura/Taniyama formula) Through the Artin reciprocity law $\pi_0(\mathbb{A}_{L,f}^{\times}/L^{\times}) \cong \mathrm{Gal}(L'^{\mathrm{ab}}/L')$, $\mathrm{Gal}(L'^{\mathrm{ab}}/L')$ acts on $\mathscr{X}_{L,\Phi}$ via a homomorphism

$$\mathrm{N}_{\Phi'} : \mathbb{A}_{L',f}^{\times} \longrightarrow \mathbb{A}_{L,f}^{\times}$$

Here $\mathrm{N}_{\Phi'} : \mathrm{Res}_{L/\mathbb{Q}}\mathbb{G}_m \to \mathrm{Res}_{L'/\mathbb{Q}}\mathbb{G}_m$ is a homomorphism of algebraic tori over $\mathbb{Q}$, called `reflex type norm` attached to (L,Φ).

Motivic CM theory

Skip motivic CM theory

Deligne/Langlands

- Replace L' by $\mathbb{Q}$, i.e. consider the moduli tower $\mathscr{X}_L := \{\mathscr{X}_{L,\Phi,K}\}_{\Phi,K}$ (includes `all` CM types Φ for L)
- The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\mathscr{X}_L$ is described in terms of the `Taniyama group` defined by Langland.
- Key ingredient (Deligne): Any Galois conjugate of a Hodge cycle is Hodge.

CM points on $\mathscr{A}_g$

§5 CM points on Shimura varieties: The case of $\mathscr{A}_g$

CM points on Siegel modular varieties

- Siegel modular varieties
- André/Oort conjecture
- Application: abelian varieties `not` isogenous to jacobians

CM points

Definition

A point $[(A,\lambda)]$ on $\mathscr{A}_g$ over $\mathbb{C}$ (or $\overline{\mathbb{Q}}$) is a CM point if A has smCM.

It is a Weyl CM point if $\mathrm{End}^0(A)$ is a CM field L with

$$\mathrm{Gal}(L^{\text{normal closure}}/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g\,.$$

- Among CM fields of degree $2g$, those whose with Galois group $(\mathbb{Z}/2\mathbb{Z})^g \rtimes S_g$ are (supposed to be) "`general`".
- Weyl CM points are (supposed to be) the `general CM points`.

André/Oort conjecture

André/Oort conjecture

If X is a subvariety of $\mathscr{A}_g$ over $\mathbb{C}$ with a Zariski dense subset of CM points, then X is a Shimura subvariety.

X is a Shimura subvariety of $\mathscr{A}_g$ means

- $X(\mathbb{C})$ is the quotient of a `bounded symmetric domain` attached to a semisimple subgroup $G \subset \mathrm{Sp}_{2g}$ by an arithmetic subgroup of $G(\mathbb{Q})$.
- X is "`defined`" (or, "`cut out`") by Hodge cycles.

Status

- A few low-dimensional cases known (e.g. when $X \subset (j\text{-line}) \times (j\text{-line})$)
- (Ullmo/Yafaev) True under GRH

Application: a conjecture of Katz

Abelian varieties NOT isogenous to a jacobian

Suppose $g \geq 4$. Is there a g-dimensional abelian variety over $\overline{\mathbb{Q}}$ which is not isogenous to a jacobian?

Answer, under GRH

- (group theory) If a positive dimensional Shimura subvariety X of $\mathscr{A}_g$ contains a Weyl CM point $[(A,\lambda)]$, then X is a Hilbert modular subvariety attached to the max. real subfield F of $L := \mathrm{End}^0(A)$.
- (de Jong/Zhang 2007) $\mathscr{M}_g$ does not contain any Hilbert modular subvariety attached to a totally real field F if either $g \geq 4$ or if $g = 4$ and $\mathrm{Gal}(F^{\mathrm{nc}}/\mathbb{Q}) \cong S_4$.
- Conclude by (AO). Q.E.D.

CM liftings

§6 CM lifting problems

- Review: Weil & Honda/Tate
- Known result: ∃ CM lifting after `base field extension` and `isogeny`
- (I): CM lifting up to `isogeny` (same base field)
- (NI): CM lifting over `normal` base up to `isogeny` (same base field)

Abelian varieties over finite fields

Theorem (Weil, Honda/Tate)

Let A be an abelian variety over a finite field $\mathbb{F}_q$ be a finite field with q elements.

1. $\mathrm{Fr}_A \in \mathrm{End}(A)$ *has a* `monic characteristic polynomial` *with* `integer` *coefficients, whose roots α_i are* `Weil-q-numbers`*:*

$$|\alpha_i| = q^{1/2}.$$

2. *If A is* `isotypic`*, then there exists a CM field $L \subseteq \mathrm{End}^0(A)$ with $\mathrm{Fr}_A \in L$ and $[L : \mathbb{Q}] = 2\dim(A)$.*

Theorem (Honda/Tate)

Let α be a q-Weil number. Then there exists an abelian variety A over $\mathbb{F}_q$ with $\mathrm{Fr}_A = \alpha$.

CM lifting: known result

Let $(A, L \hookrightarrow \mathrm{End}^0(A))$ be a CM abelian variety over a finite field κ.

Theorem (Honda/Tate)

There exist

- *a finite extension field* κ'/κ,
- *an abelian variety B over κ' isogenous to* $A_{/\kappa'}$,
- *a char.* $(0,p)$ *local domain (or* `dvr`*)* $(R, \mathfrak{m})$,
- *an abelian scheme $\mathcal{B}$ over R with endomorphism by an order in L*

s.t. $(\mathcal{B}, L \hookrightarrow \mathrm{End}^0(\mathcal{B}))$ *is a lifting of* $(B, L \hookrightarrow \mathrm{End}^0(B))$ *over R*

CM lifting question

Let $(A, L \hookrightarrow \mathrm{End}^0(A))$ be a CM abelian variety over a finite field $\kappa \supset \mathbb{F}_p$.

CM lifting question, optimistic version

(CML) Does there exist a CM abelian scheme over a 0 local domain $(R, \mathfrak{m})$ which lifts $(A_{\overline{\mathbb{F}}_p}, L \hookrightarrow \mathrm{End}^0(A_{\overline{\mathbb{F}}_p}))$?

Answer to (CML)

NO!

- First counter-example: F. Oort, 1992.
- Ubiquitous counter-examples: If $A[p](\overline{\mathbb{F}}_p) \cong (\mathbb{Z}/p\mathbb{Z})^f$ with $f \leq \dim(A) - 2$, then $\exists$ an isogeny $A \to B$ over $\overline{\mathbb{F}}_p$ s.t. $(B, L \hookrightarrow \mathrm{End}^0(B))_{/\overline{\mathbb{F}}_p}$ cannot be lifted to char. 0.

CM lifting up to isogeny

CM Lifting up to isogeny, same finite field κ

- **(I)** Does there exist a κ-isogeny $A \to B$ and a CM abelian scheme $(\mathcal{B}, L \hookrightarrow \mathrm{End}^0(\mathcal{B}))$ over a char. 0 local domain $(R, \mathfrak{m})$ which lifts $(B, L \hookrightarrow \mathrm{End}^0(B))$?
- **(NI)** Does there exist a κ-isogeny $A \to B$ and a CM abelian scheme $(\mathcal{B}, L \hookrightarrow \mathrm{End}^0(\mathcal{B}))$ over a char. 0 `normal` local domain $(R, \mathfrak{m})$ which lifts $(B, L \hookrightarrow \mathrm{End}^0(B))$?

Answers to (I) and (NI)

Theorem (w. B. Conrd & F. Oort)

- (I): *Yes*
- (NI): *There is an obstruction to* (NI)*, from the size of the residue fields above p of the Shimura reflex fields of all CM-types of L:*
  - *Needs:* $\exists$ *a CM-type* Φ *of L with the same slopes as A whose reflex field has a place above p whose residue field is contained in* $\mathbb{F}_q$.
  - *This* `residual reflex condition` *is the only obstruction.*

A toy model

Example

$A_{/\mathbb{F}_{p^2}}$: abelian surface with $\mathrm{Fr}_A = p\,\zeta_p$, $p \equiv 2, 3 \pmod 5$.

1. $(A_{/\overline{\mathbb{F}}_p}, \mathbb{Z}[\zeta_5] \hookrightarrow \mathrm{End}(A_{/\overline{\mathbb{F}}_p}))$ cannot be lifted to char. 0.
2. (NI) fails for $(A_{/\mathbb{F}_{p^2}}, \mathbb{Q}(\zeta_5) \hookrightarrow \mathrm{End}^0(A))$.
3. $(A, \mathbb{Q}(\zeta_5) \hookrightarrow \mathrm{End}^0(A))$ can be lifted to characteristic 0.

Skip proofs of 1 & 2

Proofs of 1 & 2

1. Complex conjugation in $\mathbb{Z}[\zeta_5]$ corresponds to Fr_{p^2}, so the action of $\mathbb{Z}[\zeta_5]$ on the tangent space of a lift corresponds to two embeddings $\sigma_1, \sigma_2 : \mathbb{Z}[\zeta_5] \hookrightarrow \mathbb{C}$ with ${}^{\iota}\sigma_1 = \sigma_2$.
2. The reflex field of any CM type of $\mathbb{Q}(\zeta_5)$ is $\mathbb{Q}(\zeta_5)$, with residue field $\mathbb{F}_{p^4}$ bigger than $\mathbb{F}_{p^2}$.

The toy model, continued

Proof of 3: CM lift for the toy model

- $\exists$ a $\mathbb{Z}[\zeta_5]$-linear isogeny over $\mathbb{F}_{p^4}$ $\xi : B \to A_{/\mathbb{F}_{p^4}}$, and $\mathrm{Ker}(\xi) \cong \alpha_p$ is the only subgroup scheme of B of order p.
- B admits an unramified lift to $R = W(\mathbb{F}_{p^4})$. (The $\mathbb{Z}[\zeta_5]$ action on $\mathrm{Lie}(B)$ corresponds to a CM type of $\mathbb{Q}(\zeta_5)$; lift the Hodge filtration.)
- Pick a point of order p in B over a (tame) extension R' of R to get lift of $(A, \mathbb{Q}(\zeta_5) \hookrightarrow \mathrm{End}^0(A))_{\mathbb{F}_{p^4}}$.
- Conclude by deformation theory.

Existence of CM lifting up to isogeny

Sketch proof of (I)

1. "Localize" and reduce to a problem on p-divisible groups: Given $(A[p^\infty], \mathscr{O}_L \otimes \mathbb{Z}_p \hookrightarrow \mathrm{End}(A[p^\infty]))$ over $\mathbb{F}_q$, need to find

- an $\mathscr{O}_L \otimes \mathbb{Z}_p$-linear isogeny $Y \to (A[p^\infty]$ over $\mathbb{F}_q$
- a lifting $(\mathcal{Y}, L \otimes \mathbb{Q}_p \hookrightarrow \mathrm{End}^0(\mathcal{Y}))$ of $(Y, L \otimes \mathbb{Q}_p \hookrightarrow \mathrm{End}^0(Y))$ to a char. 0 local ring R s.t. the L-action on $\mathrm{Lie}(\mathcal{Y})$ "`is`" a CM type for L.

2. How to find a good $\mathscr{O}_L \otimes \mathbb{Z}_p$-linear p-divisible group Y:

- $(Y, \mathscr{O}_L \otimes \mathbb{Z}_p \hookrightarrow Y)_{/\mathbb{F}_q})$ is determined by its `Lie type` $[\mathrm{Lie}(Y)]$ in a Grothdieck group $\mathrm{R}(\mathscr{O}_L \otimes \overline{\mathbb{F}}_p)$.
- Every $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_q)$-invariant effective element of $\mathrm{R}(\mathscr{O}_L \otimes \overline{\mathbb{F}}_p)$ with the same slope as $\mathrm{Lie}([A])$ is the Lie type of a p-divisible group Y $(\mathscr{O}_L \otimes \mathbb{Z}_p)$-linearly isogenous to $A[p^\infty]$ over $\mathbb{F}_q$.

Existence of CM lifting up to isogeny, continued

3. Localize at the maximal real subfield L_0 of L.

3a For every place v of L_0 above p, try to find a $\mathbb{F}_q$-rational element $\delta_v \in \mathrm{R}(\mathscr{O}_{L_v} \otimes \overline{\mathbb{F}}_p)$ with the same slopes as $[\mathrm{Lie}(A[v^\infty])]$, and satisfies

$$\delta_v +^{\iota} \delta_v = [\mathscr{O}_{L_v} \otimes \overline{\mathbb{F}}_p], \qquad \iota = \text{cpx. conjugation}$$

(Then $\exists\, Y_v$ isogenous to $A[v^\infty]$ over $\mathbb{F}_q$ which admits an L_v-linear lift to char. 0 with self-dual local CM type.)

3b The only situation when 3a fails (say v is a "bad place"):

- L_v is a field; let w be the place of L above v
- $e(L_w/\mathbb{Q}_p)$ is odd
- $f(L_w) \equiv 0 \pmod 4$
- $[\kappa_w : (\kappa_w \cap \mathbb{F}_q)]$ is even

Existence of CM lifting up to isogeny, continued

Reduction to the toy model

4. How to handle a `bad` place w/v of L/L_0 above p:

- $\exists$ an $\mathscr{O}_w$-linear isogeny $Y_w \to A[w^\infty]$ over $\mathbb{F}_q$ such that

$$(Y_w, \mathscr{O}_w \hookrightarrow \mathrm{End}(Y_w))_{/\overline{\mathbb{F}}_p} \cong \mathscr{O}_w \otimes_{W(\mathbb{F}_{p^4})} (\text{toy model})[p^\infty]$$

- The construction of the CM lift for the toy models gives a lift of $(Y_w, L_w \hookrightarrow \mathrm{End}^0(Y_w))$ with self-dual local CM type. Q.E.D.