Fields of definition of building blocks

MAGMA 2006 - Berlin

Jordi Quer
Universitat Politècnica de Catalunya
jordi.quer@upc.edu

Modular curves and modular abelian varieties

$$\Gamma_1(N) = \left\{ M \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; M \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

$$X_1(N) = \Gamma_1(N)\backslash\mathfrak{H}^*, \qquad J_1(N) = \mathrm{Jac}(X_1(N)).$$

$J_1(N)$ is an abelian variety defined over $\mathbb{Q}$.

Problem (Taniyama, 1955):

Decompose $J_1(N)$ into its simple components.

Let's call the factors (up to isogeny) of the modular jacobian $J_1(N)$ **modular abelian varieties**.

Applications of modularity:

- Solvability of certain Diophantine equations (Fermat);
- analytic continuation and functional equation for L-series;
- modular parametrization + Heegner points = partial results on Birch and Swinnerton-Dyer;
- . . .

Decomposition over $\mathbb{Q}$ of $X_1(N)$

Given a newform

$$f = \sum a_n q^n \in S_2^{\text{new}}(N, \varepsilon),$$

Shimura constructs a $\mathbb{Q}$-simple abelian variety $A_f/\mathbb{Q}$ as a quotient of $J_1(N)$. Then, one has the decomposition

$$J_1(N) \sim_{\mathbb{Q}} \prod A_f^{e_f},$$

the product ranging over all newforms of level dividing N, and the factors of multiplicity one corresponding to those of exact level N.

Important property: $E = \text{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$ is a number field of degree $[E : \mathbb{Q}] = \dim A_f$, the maximum allowed by the dimension of A_f.

Conjecturally, the modular $\mathbb{Q}$-simple varieties A_f are characterized, among all $\mathbb{Q}$-simple abelian varieties over $\mathbb{Q}$, **only by the structure of their $\mathbb{Q}$-endomorphism algebra**

Computational aspects

Magma can perform lots of explicit computations with modular forms and modular abelian varieties, thanks to several packages (`ModSym`, `ModFrm`, `ModAbVar`) written by **William Stein**.

All the computations make extensive use of the theory of **modular symbols** (Manin, Birch, Merel, ...).

Given $N \geqslant 1$, $k \geqslant 2$ and $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ there are functions computing all newforms of that level, weight and character up to reasonable bounds.
The bottleneck seems to be to do linear algebra in a vector space of dimension growing with N over the cyclotomic field generated over $\mathbb{Q}$ by the values of ε.

Decomposition over $\overline{\mathbb{Q}}$

Every A_f factors over $\overline{\mathbb{Q}}$ as a power of an absolutely simple variety B_f (only determined up to isogeny)

$$A_f \sim_{\overline{\mathbb{Q}}} B_f^n,$$

and there are three possibilities (Shimura, Ribet-Pyle):

CM B_f is an elliptic curve with **complex multiplication** ($\Leftrightarrow A_f$ has complex multiplication),

RM B_f has **real multiplication** by a totally real field F of degree $[F : \mathbb{Q}] = \dim B_f$, or

QM B_f has **quaternionic multiplication** by a (division) quaternion algebra $\mathcal{D}$ over a totally real field F of degree $[F : \mathbb{Q}] = \frac{1}{2} \dim B_f$.

The varieties B_f are known as **building blocks**, and conjecturally they are characterized **only by the structure of their endomorphism algebras**.

The Magma packages by William Stein contain a few functions giving some arithmetical information on the B_f (e.g. the "inner twists") but there is still a lot to be done compared with the case of the A_f.

Example of a computational nontrivial task: Elaborate a table "of Cremona's type" with equations and arithmetic information of all the one-dimensional B_f (known as elliptic $\mathbb{Q}$-curves) up to a certain level $N \leqslant$ bound.

Fields of definition of B_f

The variety B_f is only determined up to isogeny. One may ask about the fields of definition of the varieties in the isogeny class.

We say that a number field K is **a field of definition** for the building block B_f if there exists an abelian variety B/K, with all elements of End(B) also defined over K, and such that $B \sim_{\overline{\mathbb{Q}}} B_f$.

Example: If B_f is an elliptic curve with **complex multiplication** by an order of an imaginary quadratic field F, then there exists a smallest field of definition for B_f, namely, **the Hilbert class field** of the complex multiplication field F.

Let B_f be a **non-CM building block**. Then (Ribet-Pyle) there exists a number field K_P which is abelian of exponent 2

$$K_P = \mathbb{Q}(\sqrt{t_1}, \sqrt{t_2}, \ldots, \sqrt{t_r})$$

and an element $[c_\pm] \in \mathrm{Br}(\mathbb{Q})[2]$ such that a number field K is a field of definition for B_f if, and only if,

$$K_P \subseteq K \qquad \text{and} \qquad K \text{ splits the element } [c_\pm]$$

Theorems. If B_f is a $\mathbb{Q}$-curve (Elkies) or, more generally, it has odd dimension (Ribet) then K_P splits $[c_\pm]$, and hence K_P is the smallest field of definition for B_f.

Question. What happens for even-dimensional building blocks?

A package for building blocks

The new version 2.13 of **Magma** contains functions providing some information for building blocks. For a newform f, the following can be computed:

1. The structure of $\mathrm{End}(B_f)\otimes\mathbb{Q}$, given by the center F and the Brauer class in $\mathrm{Br}(F)[2]$.
   In particular one knows to which of the three types (CM, RM or QM) the variety B_f belongs to.

2. The field K_P and the element $\mathrm{Res}_{\mathbb{Q}}^{K_P}[c_\pm]$, giving the obstruction to K_P being a field of definition (for non-CM).

3. A function that for a given N and ε gives all the non-CM newforms $f\in S_2^{\mathrm{new}}$ having bounded degree of $[F:\mathbb{Q}]$ without needing to compute all the newforms of such type.

Using this package a table has been built containing information for all newforms $f \in S_2^{\text{new}}$ with

$$N \leqslant 500, \quad \varphi(\text{ord}(\varepsilon)) \leqslant 12, \quad [F:\mathbb{Q}] \leqslant 4$$

The table contains many examples of even-dimensional building blocks B_f that cannot be defined over the field B_f.

This are statistics on the number of non-CM varieties depending on their dimension and structure of endomorphism algebras:

$[F:\mathbb{Q}]$	total	RM cases	QM cases
1	2610	2426	184
2	1613	1555	58
3	739	695	44
4	647	619	28
total	5609	5295	314

The number of non-CM varieties B_f that cannot be defined over K_P is:

$[F : \mathbb{Q}]$	$\mathrm{End}(B_f) \otimes \mathbb{Q} = F$	$\mathrm{End}(B_f) \otimes \mathbb{Q} \neq F$
1	0	21
2	121	1
3	0	0
4	42	0

The RM example with smallest level is a surface and occurs in level 33.

The QM example with smallest level is also a surface and occurs in level 28; it is described in the Magma handbook.

Explicit computations

The field $E = \mathrm{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q} = \mathbb{Q}(\{a_n\}_{n\geqslant 1})$ comes from the computation of the newform f.

The building block B_f has CM by (an order of) the imaginary quadratic field F if, and only if,

$$a_p = \chi_F(\mathrm{Frob}_p) a_p \qquad \forall p \nmid N,$$

with $\chi_F \colon G_{\mathbb{Q}} \to \{\pm 1\}$ the quadratic character attached to F. It is enough to test the identity for $p \leqslant \frac{1}{6}\psi(N^2)$.

In the non-CM case, the field $F = Z(\mathrm{End}(B_f) \otimes \mathbb{Q})$ is

$$F = \mathbb{Q}(\{a_p^2/\varepsilon(p)\}_{p\nmid N})$$

In practice one adjoins values until obtaining an extension $F/\mathbb{Q}$ of the right degree using the fact that the degree $[E : F]$ is the number of **inner twists** of the newform f (warning: see the remarks about inner twist computations).

Let $\Psi \subset \mathrm{Hom}(G_{\mathbb{Q}}, \{\pm 1\})$ be the group of quadratic characters ψ satisfying

$$\sqrt{a_p^2/\varepsilon(p)} = \psi(\mathrm{Frob}_p)\sqrt{a_p^2/\varepsilon(p)}, \qquad \forall p \nmid N$$

(it is enough to check the identity for $p \leqslant \frac{1}{6}\psi(N^2)$). Let $\psi_1, \ldots, \psi_r$ be a basis of this group.

Let $t_i \in \mathbb{Q}^*$ be rational numbers such that $\mathbb{Q}(\sqrt{t_i}) = \overline{\mathbb{Q}}^{\ker \psi_i}$.

Let p_i be primes with $a_{p_i} \neq 0$ and $\psi_i(p_j) = (-1)^{\delta_{ij}}$ (Txebotarev).

Let $f_i = a_{p_i}^2/\varepsilon(p_i) \in F^*$.

Let $[c_\varepsilon] \in \mathrm{Br}(\mathbb{Q})[2] \simeq H^2(G_{\mathbb{Q}}, \{\pm 1\})$ be the cohomology class of the 2-cocycle

$$c_\varepsilon(\sigma, \tau) = \sqrt{\varepsilon(\sigma)}\sqrt{\varepsilon(\tau)}\sqrt{\varepsilon(\sigma\tau)}^{\,-1}$$

Then (Quer)

1. The Brauer class of $\mathrm{End}(B_f) \otimes \mathbb{Q}$ in $\mathrm{Br}(F)[2]$ is
$$\mathrm{Res}_{\mathbb{Q}}^{F}[c_\varepsilon]\left(\frac{t_1, f_1}{F}\right)\cdots\left(\frac{t_r, f_r}{F}\right)$$

2. The field K_P is $\mathbb{Q}(\sqrt{t_1}, \ldots, \sqrt{t_r})$

3. The obstruction to define B_f over K_P is
$$\mathrm{Res}_{\mathbb{Q}}^{K_P}[c_\varepsilon]$$

Remarks:

For a number field K the elements of Br$(F)[2]$ are completely determined by the (finite, even) set of ramified primes of the corresponding quaternion algebra.

The computation of elements of Br$(F)[2]$ or of Br$(K_P)[2]$ is done with functions special for the cases we consider. The new Magma version 2.13 contains John Voights's new package that does these computations in general.

The bound $\frac{1}{6}\psi(N^2)$ is replaced for $N > 100$ by the unproved (but probably true) bound $15 + N/2$. See also comments on the W. Stein's implementation of the inner twist computation.