Higher modularity of elliptic curves over function fields

Adam Logan (TIMC/CSE and Carleton University)
joint work (in progress) with Jared Weinstein
(with some help from Noam Elkies and Masato Kuwata)

June 23, 2022

Table of Contents

Introduction to modularity

Demystifying shtukas

The semistable case

Magic base changes

An example of 3-modularity

Done

Definition over $\mathbb{Q}$

For elliptic curves over $\mathbb{Q}$, we can define *modularity* in two ways:

Geometric There is a nonconstant map $X_0(N) \to E$ defined over $\mathbb{Q}$.

Analytic There is a Hecke eigenform f of weight 2 and level $\Gamma_0(N)$ such that $L(f, \chi, s) = L(E, \chi, s)$ for all Dirichlet characters χ.

The equivalence was known for several years before it was proved by Wiles et al. that all elliptic curves are modular.

Definition over function fields

Now let X be a smooth curve over a finite field $\mathbb{F}_q$, and let K be its function field. Let E be an elliptic curve over K, which gives an elliptic surface $\mathcal{E}/X$. We assume that $j(E) \notin \mathbb{F}_q$.

It is known that $L(E, \chi, s)$ is always a holomorphic function (in fact, a polynomial in q^{-s}). We can define its analytic modularity in the same way, although newforms in this context have quite a different flavour.

Likewise, Drinfeld defined modular curves $X_0^\infty(N_f)$, where ∞ is a place of K where E has split multiplicative reduction and N_f is an arbitrary divisor not containing ∞. So we can define geometric modularity (for elliptic curves with a suitable ∞).

What we are looking for

Drinfeld introduced a moduli stack of *r-legged shtukas of rank* 2, depending on an effective divisor N on X and a subset Σ_∞ of the support, which is of relative dimension r over X^r. For $r = 1$ this is closely related to a Drinfeld modular curve. So modularity of E essentially means that there is a correspondence between the space of 1-legged shtukas and $\mathcal{E}$.

A curve in correspondence with an elliptic curve admits a map to it.

More generally, we can define higher modularity in a similar way: there should be a correspondence between the space of r-legged shtukas and $\mathcal{E}^r$. (Note that $\mathcal{E}^r$ means the product over the ground field, not over $\mathbb{P}^1$.)

Higher modularity

Let $\mathrm{Sht}^r_G(\Gamma_0(N);\Sigma_\infty)$ be a suitable moduli stack of shtukas and $\mathcal{E} \to X$ an elliptic fibration of conductor N. Let $\mathcal{E}^r$ be the r-fold product over $\mathbb{F}_q$. We say that $\mathcal{E}$ is *r-modular* if there is a nontrivial correspondence between $\mathrm{Sht}^r_G(\Gamma_0(N);\Sigma_\infty)$ and $\mathcal{E}^r$.

In other words, there should be a variety Y mapping with finite degree to both $\mathrm{Sht}^r_G(\Gamma_0(N);\Sigma_\infty)$ and $\mathcal{E}^r$, commuting with the maps to X^r.

This would follow from Tate's conjecture.

Motivation for this work

This project grew out of Jared's study of a paper of Yun and Zhang in which they

> *prove an identity between (1) The r-th central derivative of the quadratic base change L-function associated to an everywhere unramified cuspidal automorphic representation π of PGL_2; (2) The self-intersection number of the π-isotypic component of the Heegner–Drinfeld cycle.*

This says something analogous to Gross-Zagier for the first nonzero coefficient of an L-series of an elliptic curve of rank r.

Our main theorem

Theorem

Let $\mathcal{E} \to \mathbb{P}^1$ be a tame rational elliptic fibration with rank 0*. Then:*

1. *If $\mathcal{E}$ is unstable, then $\mathcal{E}$ is* 2*-modular.*
2. *In some cases where $\mathcal{E}$ is semistable and $q \leq 7$, we have that $\mathcal{E}$ is* 2*-modular.*

("Tame" only matters in characteristic 2 or 3).

We certainly expect that the hypothesis on q should not be necessary. Some of the missing cases with $q \leq 7$ could be proved.

Plan for the rest of the talk

For the rest of the talk, we specialize to $X = \mathbb{P}^1$, and we consider only $\mathcal{E} \to X$ which is a rational surface of rank 0. We will do the following:

1. Explain why the shtuka moduli spaces $\mathrm{Sht}^r_G(\Gamma_0(N); \Sigma_\infty)$ can be described in terms of concrete conditions on a 2×2 matrix of polynomials.
2. Describe some of the geometry of these spaces for $r = 2$.
3. Indicate how we relate these to $\mathcal{E}^2$ in some special cases.
4. Time permitting, describe one example for $r = 3$.

Table of Contents

Introduction to modularity

Demystifying shtukas

The semistable case

Magic base changes

An example of 3-modularity

Done

Not a definition of shtukas

For our purposes, a shtuka is a map of vector bundles on a scheme which has certain special properties at some fixed or varying points.

Vector bundles on general schemes are very complicated. The easy way out of that problem is to take the base to be $\mathbb{P}^1$. Then every vector bundle is a direct sum of line bundles $\mathcal{O}(n_i)$ in a unique way.

Maps of vector bundles on general schemes are very complicated. However, maps of line bundles are not. A map from $\mathcal{O}(D)$ to $\mathcal{O}(D')$ is essentially a section of $\mathcal{O}(D' - D)$.

In particular, a map $\mathcal{O}(m) \to \mathcal{O}(n)$ on $\mathbb{P}^1$ is a homogeneous polynomial of degree $n - m$ in 2 variables, or a polynomial of degree at most $n - m$ in 1 variable.

Special properties

To simplify life even further, we consider only maps from $\mathcal{O} \oplus \mathcal{O}$ to $\mathcal{O}(k) \oplus \mathcal{O}(k)$ (usually k is 1 or 2). Then a map of vector bundles is just a 2 by 2 matrix of polynomials of degree at most k. When we specialize at a point of $\mathbb{P}^1$, we get a 2×2 matrix over the base field.

Here are some properties that such a map can have at a point:

1. It can have a kernel.
2. It can have a specified kernel.
3. It can take v to the subspace spanned by v.
4. It can take v to the subspace spanned by v^σ, where σ is the Frobenius.

By imposing these conditions at various points, we obtain a moduli space of maps which can be studied either concretely or abstractly.

Table of Contents

Introduction to modularity

Demystifying shtukas

The semistable case

Magic base changes

An example of 3-modularity

Done

Defining the moduli space

If a semistable rational elliptic surface has rank 0, it has four bad fibres. There are essentially four possibilities up to isogeny (one needs to choose a, b, c, d with $a + b + c + d = 12$ and $abcd$ a square, but $(2, 2, 4, 4)$ and $(1, 1, 2, 8)$ turn out to be the same, as do $(3, 3, 3, 3)$ and $(1, 1, 1, 9)$).

I will assume that the bad fibres are at $0, 1, -1, \infty$, though this is not essential. In this case, one shtuka moduli space over $\mathbb{F}_q$ turns out to be the space of 2×2 matrices M of polynomials over $\mathbb{F}_q(t_1, t_2)[T]$ of degree at most 1, such that:

1. for $i = 1, -1$, we have that M_i takes $(i, 1)$ into the space $\langle (i, 1) \rangle$;
2. M_{t_1}, M_{t_2} are singular;
3. M_0 is upper triangular, i.e., takes $(1, 0)$ into $\langle (1, 0) \rangle$;
4. we choose w such that M_∞ takes $(w, 1)$ into $\langle (w^q, 1) \rangle$.

(M_x means M with T set equal to x.)

What is this variety?

The first five of these are one condition each, so we have five equations in $\mathbb{P}^7$. The last one defines a cover.

More conveniently, let us consider three variables u, v, w, where $(u, 1)$ and $(v, 1)$ generate the kernels of M_{t_1}, M_{t_2} and w is as above. It is a codimension-1 condition in u, v, w for such a matrix to exist, and when it does, it is generically unique.

So we get a surface in $\mathbb{A}^3$, which we should compactify into $(\mathbb{P}^1)^3$. It then has tridegree $(2, 2, q + 1)$.

This gives it a genus-1 fibration by projecting to the last coordinate. If it isn't too singular (it isn't), we expect $h^{2,0} = q$.

How can we break it up?

Negation for the fibration acts as -1 on $H^{2,0}$.

There are also *Atkin-Lehner involutions*, which act by involutions on the base $\mathbb{P}^1$. These give us a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$.

The quotient by negation is a rational surface. But there are 4 potentially useful subgroups of order 4.

Modding out by these gives one quotient surface with $h^{2,0} = (q-3)/4$ and three with $(q+1)/4$ if $q \equiv 3 \bmod 4$, or $(q+3)/4, (q-1)/4$ if $q \equiv 1 \bmod 4$.

$q = 3$

In particular, let's look more closely at $q = 3$.

We always have the *Legendre family* $E_0 : y^2 = x(x-1)(x-\lambda^2)$, which is semistable with conductor $(0) + (1) + (-1) + (\infty)$. It has I_4 fibres at $0, \infty$ and I_2 at ± 1.

In characteristic 3, we get two more surfaces $E_{\pm 1}$ (not related by isogenies) by changing λ to $\lambda \pm 1$. We expect that the surface above is in correspondence with the Kummer surfaces of $E_{i,t_1} \times E_{i,t_2}$, where $E_{i,t}$ means substitute t for λ in E_i.

On the other hand, if we create an elliptic surface with I_2 fibres at $0, \infty$ and I_4 at ± 1, it is isogenous to the Legendre family above and does not appear separately.

Finding the correspondences

So we look at the quotients with $h^{2,0} = 1$ as above. Call them K_0, K_1, K_{-1}.

These are actually not K3 surfaces, since the fibrations have multiple fibres. (It is to a K3 as an Enriques surface is to a rational elliptic surface.)

But if we take the Jacobian it does give us a K3 in each case. And we can check that the point counts match mod 3^n when we specialize t_1, t_2 to elements of $\mathbb{F}_{3^n}$. This shows how to label the K_i.

Is that all?

Well . . . no. If we take any finite-degree map of K3 surfaces over $\mathbb{F}_q$, the source and target have the same number of points mod q.

And indeed it turns out that these two K3 surfaces are not isomorphic, even though their point counts match after specialization.

(One way to see this is to work out the Picard lattices of both, which we can do when we have elliptic fibrations.)

However, it turns out that the Picard lattices tensored with $\mathbb{Q}$ are the same. In this context that is enough to imply the existence of a map, at least after extending the base field.

Finding the correspondences

We managed to find the desired correspondences by considering a suitable chain of maps of K3 surfaces given by isogenies of elliptic fibrations.

(This is definitely harder than finding the isogeny between two elliptic curves that are known to be isogenous.)

Theorem

The elliptic curves E_i are 2-modular over $\mathbb{F}_3$.

With some further work, we found a general procedure for finding a map from a K3 to a Kummer surface of a product whenever possible. Unfortunately it only works over algebraically closed fields in general.

Digression: general remarks on finding isogenies

For me, an *isogeny* between two K3 surfaces K, L is a sequence $K = K_0, K_1, \ldots, K_n = L$ of K3 surfaces with dominant rational maps $K_i \dashrightarrow K_{i+1}$ or $K_{i+1} \dashrightarrow K_i$ for all i.

This implies that there is a nontrivial correspondence, which is what we are really interested in. But I have no understanding of correspondences that don't arise in this way.

Over finite fields, this implies that the two K3 surfaces have the same L-function up to cyclotomic factors.

Digression continued

Given two K3 surfaces where you suspect that there is an isogeny, one way to look for it is to list the elliptic fibrations on each and their torsion subgroups. Every torsion section of prime order gives a map to another K3 surface, whose Picard lattice can be determined. If the two surfaces admit maps to surfaces with isometric Picard lattices . . . well, we're not done yet, but it is progress. We can also take the Jacobian of a fibration with no section.

This might be a chance to apply Avi's techniques from yesterday.

One systematic approach to finding isogenies is to try to reduce the discriminant of $\operatorname{Pic} K$ until it is down to 1. Then there is only one family, and it is closely related to a Kummer surface.

This can always be made to work over $\mathbb{C}$.

$q = 5$ and $q = 7$

For $q = 5$, again we have three elliptic curves: the Legendre family as before, the family with $I_1 I_2 I_3 I_6$ fibres, and that one with t changed to $-t$ (which does not give an isogenous surface). The whole thing works in much the same way. The remaining factor with $h^{2,0} = 2$ appears (from consideration of a related Drinfeld modular curve and other evidence) to be connected with a curve of genus 2 with real multiplication by the order of discriminant 17.

For $q = 7$, we have one quotient with $h^{2,0} = 1$, corresponding to the Legendre family, which we therefore know to be 2-modular. The other three quotients have $h^{2,0} = 2$. One of them again seems to correspond to the $I_1 I_2 I_3 I_6$ family and its base change by $t \to -t$, but we do not have a proof. The others seem related to a curve of genus 2 with RM of discriminant 12.

Digression: reducing surfaces with $h^{2,0} = 2$

The cases of $q = 7, 8$ raise an interesting general question: let V be a surface with $h^{2,0} = 2$. Suppose we know (or suspect) that $H^2_{\mathrm{et}}(V, \mathbb{Q}_p)/\operatorname{Pic} V \otimes \mathbb{Q}_p$ is reducible. Can we find K3 surfaces with the same Galois representations? How do we find correspondences?

Even if you are given one map $V \to X$, finding the other one is by no means easy.

(The dimension-1 analogue of this is an old and important problem. For this problem as stated, there are some examples in the literature and I have a few more. But the general problem of understanding such surfaces is hard.)

Other base points

For $q = 3, 5$ there is only one orbit of sets of four points in $\mathbb{P}^1$. For $q = 7$ there are two. The other one, containing $(1, 2, 4, \infty)$, is more tractable; we only expect one elliptic curve, and that matches perfectly with the one quotient of the moduli space with $h^{2,0} = 1$.

Then again, there are also surfaces whose bad fibres are not above rational points. These are more difficult because we don't have as many Atkin-Lehner involutions, at least not over $\mathbb{F}_q$.

Table of Contents

Introduction to modularity

Demystifying shtukas

The semistable case

Magic base changes

An example of 3-modularity

Done

Magic base changes: vague

Fix an elliptic surface $\mathcal{E}/\mathbb{P}^1$ with (geometric) Mordell-Weil rank 0.

The reducible fibres contribute 8 to the Picard number 10.

If we take a generic double cover, each reducible fibre is doubled, so we get $2 \cdot 8 + 2 = 18$ for the generic Picard rank.

These double covers are isogenous to Kummer surfaces of $E \times E'$.

We would like to have a connection between $E, E', \mathcal{E}$.

Magic base changes: precise

Consider the variety $(\mathbb{P}^1)^3$ over $\mathbb{F}_q$, with function field $\mathbb{F}_q(t_1, t_2, t_3)$. Let $\mathcal{E}_{t_i}$ be $\mathcal{E}$ base changed so that the variable is t_i.

Let $\pi : D \to (\mathbb{P}^1)^3$ be a double cover. For general t_1, t_2 (i.e., over general points in the first two factors) it specializes to a double cover of $\mathbb{P}^1$, so we can pull back $\mathcal{E}_{t_3}$ by it to get a K3 elliptic surface.

If this is isogenous to the Kummer surface of $\mathcal{E}_{t_1} \times \mathcal{E}_{t_2}$, we say that π is a magic base change.

Magic is real

There is a 2-parameter family of double covers of $\mathbb{P}^1$ and a 2-parameter family of Kummer surfaces of products of elliptic curves, so we would expect magic base changes to exist.

In fact we have a way to construct them (so far not proved, but backed up by strong numerical evidence). I'll state it only for semistable fibrations (the harder case).

Pulling back the curtain

Suppose that the singularities are at P_1, P_2, P_3, ∞. Consider the 2×2 matrix

$$\begin{pmatrix} (T - P_1)(T - a) & b(T - P_2) \\ T - P_3 & T - d \end{pmatrix}.$$

There are conditions on a, b, d for this to be singular at $T = t_1, t_2, t_3$. If we eliminate b, we can solve for ad and $a + d$ and find a quadratic polynomial with coefficients in t_1, t_2, t_3 whose roots are a, d. This turns out to define the magic base change.

(Note that it is symmetric in t_1, t_2, t_3, which is not at all obvious from the previous definition.)

What is it good for?

We conjecture that there is a correspondence between the shtuka moduli space and the fibre product of the magic base change with a Drinfeld modular curve.

This would prove the 2-modularity conjecture for all rational elliptic fibrations of Mordell-Weil rank 0.

We can prove it for unstable ones, but not for semistable ones, and so for now our results for semistable fibrations are still limited to very small fields.

Coincidences

One reason the unstable case is easier is just that we don't need to worry about different locations of bad fibres, since PGL_2 is 3-transitive.

It turns out that there is not merely a correspondence but a birational equivalence.

Table of Contents

Introduction to modularity

Demystifying shtukas

The semistable case

Magic base changes

An example of 3-modularity

Done

3-modularity of the Legendre family

Since the Legendre family was the easiest for 2-modularity, we decided to try to prove its 3-modularity in the same way.

The analogue of the double cover of $(\mathbb{P}^1)^3$ in this case is a family of elliptic curves. We use it to construct a candidate threefold T over $\mathbb{Q}(t_1, t_2, t_3)$, which is the fibre product of two elliptic surfaces over $\mathbb{P}^1$.

This is supposed to match $T'(E_{t_1} \times E_{t_2} \times E_{t_3})/V$, where E_{t_i} is $y^2 = x(x-1)(x-t_i)$ and V is the four-group acting by negation on an even number of factors.

K3 fibrations on each side

I think of T' as defined by the equation $y^2 = \prod_{i=1}^{3} x_i z_i (x_i - t_i z_i)$ in a suitable toric variety. We have the fibration $(y : x_1 x_2 x_3 z_1 z_2 z_3)$.

On the other side, some straightforward (if unmotivated) computation gives a birational equivalence of T with a quintic in $\mathbb{P}^4$ that contains 9 planes.

Projection away from one of these expresses T as a family of quartic surfaces over $\mathbb{P}^1$, i.e., a K3 fibration.

What happened

Choosing the right plane on T, we found that the point counts of the fibres matched nicely after specialization.

This suggested that the generic fibres should be isogenous K3 surfaces, and we were able to prove that.

In fact they are isomorphic; it follows that T and T' are birationally equivalent.

Theorem

The Legendre family is 3*-modular over* $\mathbb{F}_q$ *for all* q*.*

Why did it happen?

I have no idea.

It seems amazingly lucky to me, since T and T' both have vast numbers of K3 fibrations. Even if there is a good reason for T, T' to be actually birational rather than just isogenous, why on earth was it so easy to find two fibrations that match?

(In fact this was the second proof of the birational equivalence that we found, but this one was more symmetrical.)

I tried to do something like this to prove 3-modularity of other rank-0 families, but got nowhere.

(For rank greater than 0 we don't know how to deal even with 2-modularity, so let's try to figure that out first.)

Table of Contents

Introduction to modularity

Demystifying shtukas

The semistable case

Magic base changes

An example of 3-modularity

Done

End

Thank you for your attention.

Are there any questions?