Shimura Degrees, New Modular Degrees, and Congruence Primes

Alyson Deines

CCR La Jolla

October 2, 2015

Elliptic Curve Parameterization

- We can parameterize modular elliptic curves by modular curves and Shimura curves.
- It's often difficult to write down the map, but the degree is accessible.
- We can usually find the optimal quotient.
- This information gives us another way to study all of these objects, and even the related modular forms by way of congruence numbers.

Modular Elliptic Curves

- $\Gamma_0(N) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \in \mathrm{GL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$
- $X_0(N)$ - the modular curve $\Gamma_0(N) \setminus \mathcal{H} \cup \text{cusps}$
- $J_0(N)$ - Jacobian of $X_0(N)$
- E - a modular elliptic curve over $\mathbb{Q}$ of conductor N, with $E = \mathbb{C}/\Lambda$
- f_E - the modular form in $S_2(N)$ associated to E with Fourier coefficients a_n.

Modular Elliptic Curves

E is modular, so we have the following surjective map:

$$\pi : X_0(N) \to E$$

given by $\tau \in X_0(N)(\mathbb{C})$

$$\pi(\tau) = -2\pi i \int_{\tau}^{i\infty} f(\tau')d\tau' = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n\tau} \in \mathbb{C}/\Lambda.$$

Modular Degree

Let $\pi : X_0(N) \to E$ be the modular parameterization. We have such map for any curve isogenous to E.

Definition

The **modular degree** of E is the minimal such degree.

Definition

The **optimal quotient** is the curve E in the isogeny class which gives the minimal degree. Alternatively, the optimal quotient is the curve E in the isogeny class such that the map $J_0(N) \to E$ has connected kernel.

Definition

If E is an optimal quotient of $J_0(N)$, $\pi : J_0(N) \to E$, $\pi^\vee : E \to J_0(N)$ $\pi \circ \pi^\vee \in \mathrm{End}(E)$ is multiplication by an integer m_E. This integer m_E is called the **modular degree** of E.

Shimura Curves

Let F be a totally real number field. Fix B an indefinite quaternion algebra over F of discriminant D and $\mathcal{O} \subset B$ an Eichler order of level M.

- Define $\Gamma_0^D(M)$ to be the group of norm-1 units in $\mathcal{O}$.
- Our Shimura curve is $X_0^D(M) = \Gamma_0^D(M) \setminus \mathcal{H}$.
- We denote its Jacobian by $J_0^D(M)$.

Quaternionic Modular Forms

Definition

A *quaternionic modular form* of weight k on $\Gamma_0^D(M)$ is a holomorphic function f on $\mathcal{H}$ such that

$$f(\gamma\tau) = (c\gamma + d)^k f(\tau) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0^D(M).$$

The space of such forms is denoted by $M_k^D(M)$, and cusp forms by $S_k^D(M)$.

New and Old spaces

Let D, M, and N be positive integers such that $N = DM$ (or ideals in a totally real number field F). Then for $f(\tau) \in S_{\bar{2}}(M)$ and $r \mid D$, $f(r\tau) \in S_{\bar{2}}(N)$. Thus we have maps $S_{\bar{2}}(M) \to S_{\bar{2}}(N)$ for each $r \mid D$. Combining these maps gives

$$\phi_M : \oplus_{r|D} S_{\bar{2}}(M) \to S_{\bar{2}}(N).$$

Definition

The image of ϕ_M is called the **D-old subspace** $S_{\bar{2}}(N)^{D\text{-old}}$. The orthogonal complement of $S_{\bar{2}}(N)^{D\text{-old}}$ in $S_{\bar{2}}(N)$ with respect to the Petersson inner product is called the **D-new subspace** $S_{\bar{2}}(N)^{D\text{-new}}$.

Jacquet-Langlands correspondance

Theorem (Eichler-Shimura-Jacquet-Langlands)

There is an injective map of Hecke modules

$$S_2^D(M) \hookrightarrow S_{\bar{2}}(N)$$

where $N = DM$, whose image consists of those cusp forms which are new at all primes $p \mid D$. In general there is a non-canonical isomorphism

$$S_2^D(M) \approx S_{\bar{2}}(N)^{D-new}.$$

Working over $\mathbb{Q}$, let $J_0^{D\text{-new}}(N)$ be the D-new part of $J_0(N)$.

Corollary

The Jacobians $J_0^{D\text{-new}}(N)$ and $J_0^D(M)$ are isogenous.

Degree of Parameterization

We have a paramterization for both J-new and Shimura Jacobians.

- E - a modular elliptic curve defined over F of conductor N.
- J - either $J_0^D(M)$ (or $J_0^{D\text{-new}}(N)$.)
- $\pi : J \to E$ where E is the optimal quotient.
- The **Shimura degree (or D-new degree)** is the degree of π.

Definition

The endomorphism $\pi \circ \pi^\vee \in \mathrm{End}(E)$ is multiplication by an integer. This integer is called the **Shimura degree (or D-new degree)**, $\delta^D(M)$ (or $\delta^{D\text{-new}}(N)$), of the elliptic curve E.

Idea for studying Shimura Degrees

- Examine character groups of E and J locally, i.e., at primes dividing $N = DM$.
- Use a short exact sequence of Grothendieck to rewrite the degree of parameterization in terms of computable invariants.
- Use dual graphs to view character groups as Hecke modules.
- Use Ribet's level-lowering sequence to compute Shimura degrees and make comparisons.

Local objects

Let A be a principally polarized abelian variety over F (either J, Shimura jacobian or new-modular jacobian, or E, elliptic curve) and $p \mid N = DM$:

- $\mathcal{A}_p$ - Néron model
- $\Phi_p(A) = \mathcal{A}_p/\mathcal{A}_p^0$ - Component Group
- $\mathcal{T}_p(A)$ - Toric part of $\mathcal{A}_p$
- $\mathcal{X}_p(A) = \mathrm{Hom}(\mathcal{T}_p(A), \mathbb{G}_m)$ - Character Group

Theorem (Grothendieck)

There is a natural exact sequence

$$0 \to \mathcal{X}_p(A) \xrightarrow{\alpha} Hom(\mathcal{X}_p(A), \mathbb{Z}) \to \Phi_p(A) \to 0$$

in which α is obtained from the monodromy pairing $u_{A,p}$ by $(\alpha(x))(y) = u_{A,p}(x, y)$.

Alternate Description of Shimura Degree

$A \mapsto \mathcal{X}_p(A)$ is functorial, so induces maps:

$$\pi^* : \mathcal{X}_p(E) \to \mathcal{X}_p(J)$$

$$\pi_* : \mathcal{X}_p(J) \to \mathcal{X}_p(E)$$

then $\pi^* \circ \pi_* : \mathcal{X}_p(E) \to \mathcal{X}_p(E)$ is multiplication by $\delta^D(M)$ on $\mathcal{X}_p(E)$.

Diagram Chasing

In particular we have

$$\begin{array}{ccccccccc} 0 & \to & \mathcal{X}_p(J) & \to & \mathrm{Hom}(\mathcal{X}_p(J),\mathbb{Z}) & \to & \phi_p(J) & \to & 0 \\ & & \downarrow\uparrow & & \downarrow & & \downarrow & & \\ 0 & \to & \mathcal{X}_p(E) & \to & \mathrm{Hom}(\mathcal{X}_p(E),\mathbb{Z}) & \to & \phi_p(E) & \to & 0 \end{array}$$

As $\mathcal{X}_p(E)$ injects into $\mathcal{X}_p(J)$, let $\mathcal{L}_p(E)$ denote the saturation of $\pi^*\mathcal{X}_p(E)$. Alternatively,

$$\mathcal{L}_p(E) = \{x \in \mathcal{X}_p(J) : T_n x = a_n(f_E)x \text{ for all } n \text{ coprime to } N\}$$

Note: $\mathcal{L}_p(E)$ depends only on the isogeny class of E and not on E itself.

Formula for Shimura Degree

Let g_p be a generator of $\mathcal{L}_p(E)$ and $\pi_* : \Phi_p(J) \to \Phi_p(E)$.
Define the following notation:

$$h_p = u_{J,p}(g_p, g_p), \bar{c}_p = \#\Phi_p(E), i_p = \#\mathrm{image}(\pi_*), j_p = \#\mathrm{coker}(\pi_*).$$

Theorem ($F = \mathbb{Q}$ due to Takahashi)

The $\#$image(π_*) divides $u_J(g_p, g_p)$ and

$$\delta^D(M) = \frac{u_{J,p}(g_p, g_p)}{\#\mathit{image}(\pi_*)} \cdot \#\mathit{coker}(\pi_*) = \frac{h_p j_p}{i_p} = \frac{h_p \bar{c}_p}{i_p^2}.$$

Hecke Modules - something we can compute

Let H be the definite quaternion algebra of discriminant D with Eichler order $\mathcal{O}(M)$ of level M.

- The **Brandt module** $\mathrm{Br}(D, M) = \mathbb{Z}[\mathrm{Cl}_R(\mathcal{O}(M))]$.
- The **Hecke module** $X(D, M) = \mathrm{Br}(D, M)^0$.
- Computable due to an algorithm of Kirschmir and Voight.
- Inner product:

  $$\langle [I], [J] \rangle = \delta_{[I],[J]} \omega_I / 2$$

  where $\delta_{[I],[J]} = 1$ if $[I] = [J]$ and 0 otherwise and $\omega_I = \#\mathcal{O}_L(I)^\times / \mathbb{Z}_F^\times$.
- Hecke operators are matrices with entries:

  $$T(p)_{i,j} = \#\left\{ x \in I_i I_j^{-1} : \mathrm{nrm}(x I_i I_j^{-1}) = (p) \right\}.$$

Level Lowering Sequence

Theorem (Buzzard over $\mathbb{Q}$)

When $N = DMp$, $\mathcal{X}_p(J_0^D(pM)) = X(Dp, M)$.

Theorem (Ribet, Buzzard over $\mathbb{Q}$)

We have the following short exact sequence of Hecke modules

$$0 \to \mathcal{X}_p(J_0^{Dpq}(M)) \to \mathcal{X}_q(J_0^D(Mpq)) \to \mathcal{X}_q(J_0^D(Mq)) \times \mathcal{X}_q(J_0^D(Mq)) \to 0.$$

Computing Character Groups of Jacobians Shimura Curves

There are two cases, p divides the level $p \mid pM$ and p divides the discriminant $p \mid pD$ with $p \mid\mid N = DMp$.

- If $p \mid Mp$: Let H be the definite quaternion algebra of discriminant pD with Eichler order $\mathcal{O}(M)$ of level M. Then $\mathcal{X}_p(J_0^D(M)) \cong X(Dp, M)$.
- If $p \mid Dp$: Let H be the quaternion algebra ramified at all infinite places of discriminant D with Eichler orders $\mathcal{O}(M)$ of level M and $\mathcal{O}(Mp)$ of level Mp. Then

$$0 \to \mathcal{X}_p(J_0^{Dpq}(M)) \to X(Dq, Mp) \to X(Dq, M) \times X(Dq, M) \to 0.$$

Let $J' = J_0^{Dpq}(M)$ and $J = J_0^D(Mpq)$. Denote invariants of J' with $'$s.

Corollary

$h'_p = h_q$ and $i_q \mid i'_p$.

Corollary

We have the following relationship between Shimura degrees:

$$\delta' = \frac{\delta}{\bar{c}'_p \bar{c}_q} i_q^2 j_p'^2.$$

Corollary

If we instead let $J' = J_0^{D\text{-new}}(N)$ and $J = J_0(N)$, then $h_p = h'_p$ and $i_p \mid i'_p$. Further, $m_E^{D\text{-new}} \mid m_E$.

How to Compute h_p and i_p

The following are now straight forward:

- h_p: compute the monodromy paring on the generator for $\mathcal{L}(f)$ using the action of Hecke operators on $\mathcal{X}_p$.
- i_p: compute the generator of the ideal I_p of $\mathbb{Z}$ by computing the monodromy pairings with h_p.

Oddly enough, in most cases this is enough to compute δ and $\bar{c}_p$'s.
Note: If you can compute the optimal quotient, there is an algorithm for finding the Shimura degree.

Data

In fact, for all semistable elliptic curves over $\mathbb{Q}$ with conductor $N < 100$ I can determine both the degree and the optimal quotient:

Isog. Class	D	M	m_E	Labels	$\delta^D(M)$	Labels
$14a$	14	1	1	$a1$	1	$a2$
$30a$	15	2	2	$a1$	2	$a2$
$30a$	6	5	2	$a1$	1	$a7$
$30a$	10	3	2	$a1$	1	$a3$
$39a$	39	1	2	$a1$	2	$a1$
$55a$	55	1	2	$a1$	2	$a1$
$65a$	65	1	2	$a1$	2	$a1$
$66b$	6	11	4	$b1$	2	$b2$
$66b$	22	3	4	$b1$	2	$b2$
$84a$	21	4	6	$a1$	6	$a1$

Question of Takahashi

Question (Takahashi)

If $p \mid D$, is the map $\Phi_p(J) \to \Phi_p(E)$ surjective?

If $p \mid M$, this is not true.

Corollary (Takahashi)

Asuming the conjecture, for $p \mid D$,

$$\delta^D(M) = \frac{u_J(g_p, g_p)}{\#image(\pi_*)} = \frac{h_p}{i_p}.$$

Note: When working over $\mathbb{Q}$ this is always enough to compute $\delta^D(M)$ and find the optimal quotient!

Definition

We say E and E' are discriminant twins if E and E' if $N(E) = N(E')$ and $\Delta(E) = \Delta(E')$, i.e., E and E' have the same conductor and the same discriminant.

Theorem (D. - Lundell)

Over $\mathbb{Q}$ there are only finitely many pairs of semistable, isogenous discriminant twins. They occur for conductors $11, 17, 19$, and 37.

Corollary

Assuming Takahashi's question, over $\mathbb{Q}$ there is an algorithm for finding the Shimura degree and the optimal quotient of $J_0^D(M)$.

Using power series expansions of quaternion modular forms

- Zagier computed the complex periods of the optimal quotient directly using the Fourier series expansion of the modular form.
- Quaternionic modular forms don't have cusps, so don't have Fourier series expansions.
- Voight and Willis use power series expansions instead!
- Compute the power series expansion of the quaternionic modular form $f_E \in S_2(\Gamma_0^D(M))$.
- Compute generators for the fundamental domain of $\Gamma_0^D(M)$.
- Use the generators to identify vertices of the fundamental domain.
- Integrate over vertices to find independent periods.
- Compute the j-invariant and match with curve in the isogeny class. This curve is the optimal quotient.

$\mathbb{Q}(\sqrt{5})$ Example

Let $F = \mathbb{Q}(\sqrt{5})$, $a = \frac{1+\sqrt{5}}{2}$ and $E : y^2 + xy + ay = x^3 + (-a-1)\,x^2$, $N = (-5a+3)$ of norm 31.

- $X_0^N(1)$ is a genus one curve, so the modular degree is trivially 1.
- There are 6 curves in the isogeny class.
- Using the method of Voight and Willis, compute the j-invariant $j(E) = (-a)(-51a+37)^3(-39a+25)^3(5a-3)^{-8}$ and find:

$$E : y^2 + xy + ay = x^3 - (a+1)x^2 - (30a+45)x - (111a+117)$$

- Only one curve in the isogeny class with $\mathrm{ord}_N(\Delta) = 8$, so we find this curve computing Hecke modules as well.

$\mathbb{Q}(\sqrt{5})$ Example

Take $N = -8a + 2$, then $\dim M_{(2,2)}(-8a+2) = 2$ and $N(-8a+2) = 76$. Let E be the elliptic curve $76a.a1$. Let $X_0^D(M)$ be the Shimura curve with $D = 2$ and $M = -4a + 1$.

Case $p \mid D$, so $p = 2$. Computing Brandt Modules: $2 = u_J(g_p, g_p)$, $i_p = 1$ so $\delta = 2\bar{c}_2$. Two choices for $\bar{c}_2$, 1 and 5, so $\delta = 2$ or 10.

Try $p \mid M$, so $p = -4a + 1$ Use the Hecke module correspondence to get again get $\bar{c}_{-4a+1} = 1$ or 5 and again $\delta = 2$ or 10.

Problem: For both curves in the isogeny class $\bar{c}_2 = \bar{c}_{-4a+1}$.

Modular Degree and Congruence Numbers

Let $S = S_2(\Gamma_0(N), \mathbb{Z})$ be the space of weight 2, level N, cuspforms with integral Fourier coefficients. Let $L = (f_E)^\perp \cap S$.

Definition

The **congruence number** r_E is the integer that satisifes the following equivalent conditions:

- r is the largest integer such that there exists $g \in L$ with $f \equiv g \pmod{r}$.
- $\{(f, h) | h \in S\} = r^{-1}(f, f)\mathbb{Z}$.
- r is the order of the finite group $S/(\mathbb{Z}f + L)$.

Theorem (Ribet)

$m_E \mid r_E$.

Modular Degree and Congruence Numbers

Zagier computed m_E for $N = p$. In all of these examples $m_E = r_E$.
This lead to Frey and Muller asking if it is always the case that $m_E = r_E$.
Stein, Agashe, investigate and found, no, not even close.
Example: The elliptic curve with Cremona label 54b1 has $m_E = 2$ and $r_E = 6$.

Theorem (Agashe,Ribet,Stein-2009)

$m_E \mid r_E$ and if $ord_p(N) \leq 1$ then $ord_p(r_E) = ord_p(m_E)$.

For $\Gamma_1(N)$ they find examples where $m_E \nmid r_E$, in particular $54b1$ and also for a curve of squarefree conductor, $N = 38$.
They also note that the analogous statment does not hold for modular abelian varieties, but get a different statement in terms of the expontents of the groups.

$\mathbb{Q}(\sqrt{5})$ Degrees and Congruence Primes

Iso.	N	gen	D	M	LMFDB Label	$\delta^D(M)$	r_E
a	$31b$	$5a-2$	$5a-2$	1	$a5$	1	1
a	$36b$	6	2	3	$a3$	1	1
a	$36b$	6	3	2	$a4$	1	1
a	$41b$	$a+6$	$a+6$	1	$a2$	1	1
a	$45a$	$-6a+3$	3	$-2a+1$	$a5$	1	1
a	$45a$	$-6a+3$	$-2a+1$	3	$a4$	1	1
a	$49a$	7	7	1	$a2$	1	1
a	$55a$	$-a+8$	$-2a+1$	$-3a+2$	$a5$	1	1
a	$55a$	$-a+8$	$-3a+2$	$-2a+1$	$a5$	1	1
a	$71b$	$a+8$	$a+8$	1	$a4$	1	1
a	$76a$	$-8a+2$	2	$-4a+1$	$a1^*$	2^*	2
a	$76a$	$-8a+2$	$-4a+1$	2	$a2$	2	2

D-new parts

Let $S = S_2(\Gamma_0(N), \mathbb{Z})^{D-\text{new}}$ and $L = (f)^{\perp} \cap S$.

Definition

The D-**new congruence number** $r_E^{D\text{-new}}$ is the integer that satisifes the following equivalent conditions:

- r is the largest integer such that their exists $g \in L$ with $f \equiv g \pmod{r}$.
- $\{(f, h) | h \in S\} = r^{-1}(f, f)\mathbb{Z}$.
- r is the exponent of the finite group $S/(\mathbb{Z}f + L)$.

Isogeny Class	D	M	Cremona Label	$\delta^D(M)$	$m_E^{D\text{-new}}$	$r_E^{D\text{-new}}$
$14a$	1	14	$a1$	1	—	—
$14a$	14	1	$a2$	1	1	1
$15a$	1	15	$a1$	1	—	—
$15a$	15	1	$a1$	1	1	1
$21a$	1	21	$a1$	1	—	—
$21a$	21	1	$a2$	1	1	1
$26a$	1	26	$a1$	2	—	—
$26a$	26	1	$a1$	2	2	2
$26b$	1	26	$b1$	2	—	—
$26b$	26	1	$b2$	2	2	2
$30a$	1	30	$a1$	2	—	—
$30a$	15	2	$a2$	2	2	2
$30a$	6	5	$a7$	1	1	1
$30a$	10	3	$a3$	1	1	1

Conjectures

Computing $m_E^{D\text{-new}}$ is just a few lines using modular symbols and is **very** fast compared to computing Brandt modules.

Conjecture

For semistable elliptic curves the following invariants are equal:

$$\delta^D(M) = m_E^{D\text{-new}} = r_E^{D\text{-new}}.$$

If this is true, it gives more evidence of Takahashi's conjecture:

Conjecture

When $p \mid D$, $\phi_p(J) \to \phi_p(E)$ is surjective.

And, as $m_E^{D\text{-new}} \mid m_E$:

Conjecture

$\delta^D(M) \mid m_E$.

Open Questions

- We can use the work of Voight and Willis to find the j-invariant of the optimal quotient of the Shimura curve parameterization up to some precision. Is there an algebraic way to find the optimal quotient? This would give a provable agorithm for computing the Shimura degree.

- For totally real number fields, do we get the same analogues? Does $\delta^D(M) \mid r_E$? When $p \mid D$ is the map on component groups surjective?

- Are there only finitely many semistable, isogenous discriminant twins over totally real number fields? Data indicates yes, but the proof over $\mathbb{Q}$ does not generalize.

Thank you!