Modular Degrees of Elliptic Curves and Discriminants of Hecke Algebras

William Stein*

`http://modular.fas.harvard.edu`

ANTS VI, June 18, 2004

*This is joint work with F. Calegari.

Goal

Let p be a prime. My goal is to explain and justify the following Calegari-Stein conjectures (note: 3 implies 2 implies 1):

Conjecture 1: If $E/\mathbf{Q}$ is an elliptic curve of conductor p, then the modular degree m_E of E is not divisible by p.

Conjecture 2: If $\mathbf{T}_2(p)$ is the Hecke algebra associated to $S_2(p)$, then p does not divide the index of $\mathbf{T}_2(p)$ in its normalization.

Conjecture 3: If $p \geq k-1$, then there is an explicit formula for the p-part of the index of $\mathbf{T}_k(p)$ in its normalization.

Conj 1: If E of conductor p_E, then

$$p_E \nmid m_E.$$

A Motivation:  Conjecture 1 looks like Vandiver's conjecture, which asserts that $p \nmid h_p^-$. Flach proved the modular degree annihilates $Ш(\mathrm{Sym}^2(E))$, which is an analogue of a class group.

Conj 1: If E of conductor p_E, then

$$p_E \nmid m_E.$$

Watkins Data:  For $p_E < 10^7$ there are 52878 curves of prime conductor whose modular degree Watkins computed. No counterexamples to Conjecture 1 in the data. There are 23 curves such that m_E is divisible by a prime $\ell > p_E$. For example the curve $y^2 + xy = x^3 - x^2 - 391648x - 94241311$ of prime conductor $p_E = 4\,847\,093$ has modular degree $2 \cdot 21\,695\,761$. Smallest p_E with some $\ell > p_E$ is $p_E = 1\,194\,923$.

More Data

- The **maximum** known ratio $\dfrac{m_E}{p_E}$ is ~ 23.2, attained for $p_E =$ 7 944 197.

- **First** curve with $\dfrac{m_E}{p_E} > 1$ has $p_E = 13723$ and $m_E = 16176 = 2^4 \cdot 3 \cdot 337$.

- **Smallest** known $\dfrac{m_E}{p_E} > 1$ is $1.0004067\ldots$ for $p_E = 1\,757\,963$ where $m_E = p_E + 715$.

Modular Forms

Congruence Subgroup:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \text{ such that } N \mid c \right\}.$$

Cusp Forms: $S_k(N) = \Big\{ f : \mathfrak{h} \to \mathbf{C}$ such that

$$f(\gamma(z)) = (cz+d)^{-k} f(z) \text{ all } \gamma \in \Gamma_0(N),$$

and f is holomorphic at the cusps$\Big\}$

Fourier Expansion:

$$f = \sum_{n\geq 1} a_n e^{2\pi i z n} = \sum_{n\geq 1} a_n q^n \in \mathbf{C}[[q]].$$

Computing Modular Forms

$S_k(N) = 0$ if k is odd, so we will not consider odd k further.

For $k \geq 2$, a basis of $S_k(N)$ can be computed to any given precision using **modular symbols**. Appears that no formal analysis of complexity has been done. Certainly polynomial time in N and required precision. Is polynomial factorization over $\mathbf{Z}$ the theoretical bottleneck?

Implemented in MAGMA

```
> S := CuspForms(37,2);
> Basis(S);
    q + q^3 - 2*q^4 - q^7 + O(q^8),
    q^2 + 2*q^3 - 2*q^4 + q^5 - 3*q^6 + O(q^8)
```

See also `http://modular.fas.harvard.edu/mfd`

Basis for $S_{14}(11)$:

```
> S := CuspForms(11,14); SetPrecision(S,17);
> Basis(S);
    q   - 74*q^13 - 38*q^14 + 441*q^15 + 140*q^16 + O(q^17),
    q^2 - 2*q^13 + 78*q^14 + 24*q^15 - 338*q^16 + O(q^17),
    q^3 + 18*q^13 - 72*q^14 + 89*q^15 + 492*q^16 + O(q^17),
    q^4 + 12*q^13 + 31*q^14 - 18*q^15 - 193*q^16 + O(q^17),
    q^5 - 10*q^13 + 46*q^14 - 63*q^15 - 52*q^16 + O(q^17),
    q^6 + 11*q^13 - 18*q^14 - 74*q^15 - 4*q^16 + O(q^17),
    q^7 - 7*q^13 - 16*q^14 + 42*q^15 - 84*q^16 + O(q^17),
    q^8 - q^13 - 16*q^14 - 18*q^15 - 34*q^16 + O(q^17),
    q^9 - 8*q^13 - 2*q^14 - 3*q^15 + 16*q^16 + O(q^17),
    q^10 - 5*q^13 - 2*q^14 - 6*q^15 + 14*q^16 + O(q^17),
    q^11 + 12*q^13 + 12*q^14 + 12*q^15 + 12*q^16 + O(q^17),
    q^12 - 2*q^13 - q^14 + 2*q^15 + q^16 + O(q^17)
```

Hecke Algebras 

Hecke Operators: Let p be a prime.

$$T_p\left(\sum_{n\geq 1} a_n \cdot q^n\right) = \sum_{n\geq 1} a_{np}\cdot q^n + p^{k-1}\sum_{n\geq 1} a_n \cdot q^{np}$$

(If $p \mid N$, drop the second summand.) This preserves $S_k(N)$, so defines a linear map

$$T_p : S_k(N) \to S_k(N).$$

Similar definition of T_n for any integer n.

Hecke Algebra: A *commutative ring*:

$$\mathbf{T}_k(N) = \mathbf{Z}[T_1, T_2, T_3, T_4, T_5, \ldots] \subset \mathrm{End}_{\mathbf{C}}(S_k(N))$$

Computing Hecke Algebras

Fact: $\mathbf{T}_k(N) = \mathbf{Z}[T_1, T_2, T_3, T_4, T_5, \ldots]$ is free as a $\mathbf{Z}$-**module** of rank equal to $\dim S_k(N)$.

Sturm Bound: $\mathbf{T}_k(N)$ is generated as a $\mathbf{Z}$-module by $T_1, T_2, \ldots, T_b$, where

$$b = \left\lceil \frac{k}{12} \cdot N \cdot \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \right\rceil.$$

Example: For $N = 37$ and $k = 2$, the bound is 7. In fact, $\mathbf{T}_2(37)$ has $\mathbf{Z}$-basis $T_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $T_2 = \begin{pmatrix} -2 & 0 \\ 1 & 0 \end{pmatrix}$.

There are several other $\mathbf{T}_k(N)$-modules isomorphic to $S_2(N)$, and I use these instead to compute $\mathbf{T}_k(N)$ as a ring.

Discriminants

The discriminant of $\mathbf{T}_k(N)$ is an integer. It measures ramification, or what's the same, congruences between simultaneous eigenvectors for $\mathbf{T}_k(N)$, hence is related to the modular degree.

Discriminant:

$$\mathrm{Disc}(\mathbf{T}_k(N)) = \mathrm{Det}(\mathrm{Tr}(t_i \cdot t_j)),$$

where $t_1, \ldots, t_n$ are a basis for $\mathbf{T}_k(N)$ as a free $\mathbf{Z}$-module.

Examples:

$$\mathrm{Disc}(\mathbf{T}_2(37)) = \mathrm{Det}\begin{pmatrix} 2 & -2 \\ -2 & 4 \end{pmatrix} = 4$$

$$\mathrm{Disc}(\mathbf{T}_{14}(11)) = 2^{46} \cdot 3^{14} \cdot 5^{2} \cdot 11^{42} \cdot 79 \cdot 241 \cdot 1163 \cdot 40163 \cdot 901181111 \cdot 47552569849 \cdot 124180041087631 \cdot 205629726345973.$$

Ribet's Question

I became interested in computing with modular forms when I was a grad student and Ken Ribet started asking:

Question: (Ribet, 1997) Is there a prime p so that $p \mid \mathrm{Disc}(\mathbf{T}_2(p))$?

Ribet proved a theorem about $X_0(p) \cap J_0(p)_{\mathrm{tor}}$ under the hypothesis that $p \nmid \mathrm{Disc}(\mathbf{T}_2(p))$, and wanted to know how restrictive his hypothesis was. Note: When $k > 2$, usually $p \mid \mathrm{Disc}(\mathbf{T}_k(p))$.

Computations

Using a PARI/GP script of Joe Wetherell, I set up a computation on my laptop and found exactly one example in which $p \mid \mathrm{Disc}(\mathbf{T}_2(p))$. It was $p = 389$, now my favorite number.

Last year I checked that for $p < 50000$ there are no other examples in which $p \mid \mathrm{Disc}(\mathbf{T}_2(p))$. For this I used the Mestre method of graphs, which involves computing with the free abelian group on the supersingular j-invariants in $\mathbf{F}_{p^2}$ of elliptic curves.

Index in the Normalization

Let $\tilde{\mathbf{T}}_k(p)$ be the **normalization** of $\mathbf{T}_k(p)$. Since $\mathbf{T}_k(p)$ is an order in a product of number fields, $\tilde{\mathbf{T}}_k(p)$ is the product of the rings of integers of those number fields.

It turned out that Ribet could prove his theorem under the weaker hypothesis that $p \nmid [\tilde{\mathbf{T}}_2(p) : \mathbf{T}_2(p)]$. I was unable to find a counterexample to this divisibility. (Note: Matt Baker's Ph.D. was a complete proof of the result Ribet was trying to prove, but used different methods.)

[[Picture on blackboard of Spec($\mathbf{T}_k(p)$)]]

? Conjecture 2 ?

Conjecture 2. $(-)$. If $\mathbf{T}_2(p)$ is the Hecke algebra associated to $S_2(\Gamma_0(p))$, then p does not divide the index of $\mathbf{T}_2(p)$ in its normalization.

The primes that divide $[\tilde{\mathbf{T}}_2(p) : \mathbf{T}_2(p)]$ are called **congruence primes**. They are the primes of congruence between non-Gal$(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugate eigenvectors for $\mathbf{T}_2(p)$. Using this observation and another theorem of Ribet (and Wiles's theorem), we see that Conjecture 2 implies that p does not divide the modular degree of any elliptic curve of conductor p. This is why Conjecture 2 implies Conjecture 1.

But is there any reason to believe Conjecture 2, beyond knowing that it is true for $p < 50000$?

Example of Weight $k = 14$

Totally stuck on Conjecture 2, so look at weight $k > 2$. We have

$$\mathrm{Disc}(\mathbf{T}_{14}(11)) = 2^{46} \cdot 3^{14} \cdot 5^{2} \cdot \mathbf{11}^{42} \cdot 79 \cdot 241 \cdot 1163 \cdot 40163 \cdot 901181111 \cdot 47552569849 \cdot 124180041087631 \cdot 205629726345973.$$

Notice the large power of 11. Upon computing the p-maximal order in $\mathbf{T}_{14}(11) \otimes_{\mathbf{Z}} \mathbf{Q}$, we find that $11 \nmid \mathrm{Disc}(\tilde{\mathbf{T}}_{14}(11))$, so all the 11 is in the index of $\mathbf{T}_{14}(11)$ in $\tilde{\mathbf{T}}_{14}(11)$. Thus

$$\mathrm{ord}_{11}([\tilde{\mathbf{T}}_{14}(11) : \mathbf{T}_{14}(11)]) = 21.$$

Data for $k = 4$

For inspiration, consider weight > 2.

Each row contains pairs p and $\mathrm{ord}_p(\mathrm{Disc}(\mathbf{T}_4(p)))$.

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59
0	0	0	0	0	2	2	2	2	4	4	6	6	6	6	8	8
61	67	71	73	79	83	89	97	101	103	107	109	113	127	131	137	139
10	10	10	12	12	12	14	16	16	16	16	18	18	20	20	22	**24**
149	151	157	163	167	173	179	181	191	193	197	199	211	223	227	229	233
24	24	26	26	26	28	28	30	30	32	32	32	34	36	36	38	38
239	241	251	257	263	269	271	277	281	283	293	307	311	313	317	331	337
38	40	40	42	42	44	44	46	46	46	48	50	50	52	52	54	56
347	349	353	359	367	373	379	383	389	397	401	409	419	421	431	433	439
56	58	58	58	60	62	62	62	**65**	66	66	68	68	70	70	72	72
443	449	457	461	463	467	479	487	491	499							
72	74	76	76	76	76	78	80	80	82							

A Pattern?

F. Calegari (during a talk I gave): There is **almost** a pattern!!! Frank, Romyar Sharifi and I computed $2 \cdot [\tilde{\mathbf{T}}_4(p) : \mathbf{T}_4(p)]$ and obtained the numbers as in the table, except for $p = 389$ (which gives 64) and 139 (which gives 22). We also considered many other examples... and found a pattern!

Conjecture 3

In all cases, we found the following **amazing** pattern:

Conjecture 3. Suppose $p \geq k-1$. Then

$$\mathrm{ord}_p([\tilde{\mathbf{T}}_k(p) : \mathbf{T}_k(p)]) = \left\lfloor \frac{p}{12} \right\rfloor \cdot \binom{k/2}{2} + a(p,k),$$

where

$$a(p,k) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod{12}, \\ 3 \cdot \binom{\lceil \frac{k}{6} \rceil}{2} & \text{if } p \equiv 5 \pmod{12}, \\ 2 \cdot \binom{\lceil \frac{k}{4} \rceil}{2} & \text{if } p \equiv 7 \pmod{12}, \\ a(5,k) + a(7,k) & \text{if } p \equiv 11 \pmod{12}. \end{cases}$$

Warning

The conjecture is false without the constraint that $p \geq k-1$.

For example, if $p = 5$ and $k = 12$, then the conjecture predicts that the index is $0+3\cdot 1 = 3$, but in fact $\mathrm{ord}_p([\tilde{\mathbf{T}}_k(p) : \mathbf{T}_k(p)]) = 5$.

In our data when $k > p+1$, then the conjectural ord_p is often less than the actual ord_p.

Summary

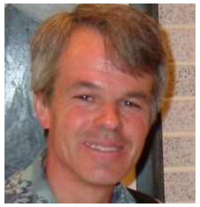
For many years I had no idea whether there should or shouldn't be mod p congruence between nonconjugate eigenforms. (I.e., whether p divides modular degrees at prime level.) By considering weight $k \geq 4$, and computing examples, a simple conjectural formula emerged. When specialized to weight 2 this formula is the conjecture that there are no mod p congruences.

Future Direction. Explain why there are so many mod p congruences at level p, when $k \geq 4$. See paper for a strategy.

Connection with Vandiver's Conjecture? Investigate the connection between Conjecture 1 and Flach's results on modular degrees annihilating Selmer groups.

This Concludes ANTS VI: THANKS!

Many thanks to the organizers (Sands, Kelly, Buell):

, , and Duncan Buell