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

**Conjecture 2:** If $T_2(p)$ is the Hecke algebra associated to $S_2(p)$, then $p$ does not divide the index of $T_2(p)$ in its normalization.

**Conjecture 3:** If $p \geq k - 1$, then there is an explicit formula for the $p$-part of the index of $T_k(p)$ 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 $\text{III}(\text{Sym}^2(E))$, 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 $p_E = 4847093$ has modular degree $2 \cdot 21695761$. Smallest $p_E$ with some $\ell > p_E$ is $p_E = 1194923$. 


More Data

- The **maximum** known ratio $\frac{m_E}{p_E}$ is $\sim 23.2$, attained for $p_E = 7944197$.

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

- **Smallest** known $\frac{m_E}{p_E} > 1$ is $1.0004067 \ldots$ for $p_E = 1757963$ where $m_E = p_E + 715$. 
Modular Forms

Congruence Subgroup:

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

Cusp Forms: \( S_k(N) = \left\{ f : \mathfrak{h} \rightarrow \mathbb{C} \text{ such that } \right. \\
\left. f(\gamma(z)) = (cz + d)^{-k}f(z) \text{ all } \gamma \in \Gamma_0(N), \right. \\
\left. \text{and } f \text{ is holomorphic at the cusps} \right\} \]

Fourier Expansion:

\[ f = \sum_{n \geq 1} a_n e^{2\pi i nz} = \sum_{n \geq 1} a_n q^n \in \mathbb{C}[[q]]. \]
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 \( \mathbb{Z} \) 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);

\[
\begin{align*}
q & - 74q^{13} - 38q^{14} + 441q^{15} + 140q^{16} + O(q^{17}), \\
q^2 & - 2q^{13} + 78q^{14} + 24q^{15} - 338q^{16} + O(q^{17}), \\
q^3 & + 18q^{13} - 72q^{14} + 89q^{15} + 492q^{16} + O(q^{17}), \\
q^4 & + 12q^{13} + 31q^{14} - 18q^{15} - 193q^{16} + O(q^{17}), \\
q^5 & - 10q^{13} + 46q^{14} - 63q^{15} - 52q^{16} + O(q^{17}), \\
q^6 & + 11q^{13} - 18q^{14} - 74q^{15} - 4q^{16} + O(q^{17}), \\
q^7 & - 7q^{13} - 16q^{14} + 42q^{15} - 84q^{16} + O(q^{17}), \\
q^8 & - q^{13} - 16q^{14} - 18q^{15} - 34q^{16} + O(q^{17}), \\
q^9 & - 8q^{13} - 2q^{14} - 3q^{15} + 16q^{16} + O(q^{17}), \\
q^{10} & - 5q^{13} - 2q^{14} - 6q^{15} + 14q^{16} + O(q^{17}), \\
q^{11} & + 12q^{13} + 12q^{14} + 12q^{15} + 12q^{16} + O(q^{17}), \\
q^{12} & - 2q^{13} - q^{14} + 2q^{15} + q^{16} + O(q^{17})
\end{align*}
\]
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

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

Similar definition of $T_n$ for any integer $n$.

Hecke Algebra: A commutative ring:

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

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

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

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

**Example:** For $N = 37$ and $k = 2$, the bound is 7. In fact, $T_2(37)$ has $\mathbb{Z}$-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 $T_k(N)$-modules isomorphic to $S_2(N)$, and I use these instead to compute $T_k(N)$ as a ring.
Discriminants

The discriminant of $T_k(N)$ is an integer. It measures ramification, or what's the same, congruences between simultaneous eigenvectors for $T_k(N)$, hence is related to the modular degree.

**Discriminant:**

$$\text{Disc}(T_k(N)) = \text{Det}(\text{Tr}(t_i \cdot t_j)),$$

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

**Examples:**

$$\text{Disc}(T_2(37)) = \text{Det} \begin{pmatrix} 2 & -2 \\ -2 & 4 \end{pmatrix} = 4$$

$$\text{Disc}(T_{14}(11)) = 2^{46} \cdot 3^{14} \cdot 5^2 \cdot 11^{42} \cdot 79 \cdot 241 \cdot 1163 \cdot 40163 \cdot 901181111 \cdot 47552569849 \cdot 124180041087631 \cdot 205629726345973.$$
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 $p \mid \text{Disc}(T_2(p))$?

Ribet proved a theorem about $X_0(p) \cap J_0(p)_{\text{tor}}$ under the hypothesis that $p \nmid \text{Disc}(T_2(p))$, and wanted to know how restrictive his hypothesis was. Note: When $k > 2$, usually $p \mid \text{Disc}(T_k(p))$. 

12
Computations

Using a script of Joe Wetherell, I set up a computation on my laptop and found exactly one example in which $p \mid \text{Disc}(T_2(p))$. It was $p = 389$, now my favorite number.

Last year I checked that for $p < 50000$ there are no other examples in which $p \mid \text{Disc}(T_2(p))$. 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 $\tilde{T}_k(p)$ be the normalization of $T_k(p)$. Since $T_k(p)$ is an order in a product of number fields, $\tilde{T}_k(p)$ 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 $p \nmid [\tilde{T}_2(p) : T_2(p)]$. 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.)
Conjecture 2. \((-\).

If $T_2(p)$ is the Hecke algebra associated to $S_2(\Gamma_0(p))$, then $p$ does not divide the index of $T_2(p)$ in its normalization.

The primes that divide $[\bar{T}_2(p) : T_2(p)]$ are called **congruence primes**. They are the primes of congruence between non-$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-conjugate eigenvectors for $T_2(p)$. 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 $k = 14$

Let’s look at higher weight. We have

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

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

$$\text{ord}_{11}([\tilde{T}_{14}(11) : T_{14}(11)]) = 21.$$
Data for $k = 4$

For inspiration, consider weight $> 2$.

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

<table>
<thead>
<tr>
<th></th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
<th>43</th>
<th>47</th>
<th>53</th>
<th>59</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>67</td>
<td>71</td>
<td>73</td>
<td>79</td>
<td>83</td>
<td>89</td>
<td>97</td>
<td>101</td>
<td>103</td>
<td>107</td>
<td>109</td>
<td>113</td>
<td>127</td>
<td>131</td>
<td>137</td>
<td>139</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>14</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>16</td>
<td>18</td>
<td>18</td>
<td>18</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>24</td>
<td>26</td>
<td>26</td>
<td>26</td>
<td>28</td>
<td>28</td>
<td>30</td>
<td>30</td>
<td>32</td>
<td>32</td>
<td>32</td>
<td>34</td>
<td>36</td>
<td>36</td>
<td>38</td>
<td>38</td>
</tr>
<tr>
<td>4</td>
<td>241</td>
<td>251</td>
<td>257</td>
<td>263</td>
<td>269</td>
<td>271</td>
<td>277</td>
<td>281</td>
<td>283</td>
<td>293</td>
<td>307</td>
<td>311</td>
<td>313</td>
<td>317</td>
<td>331</td>
<td>337</td>
</tr>
<tr>
<td>5</td>
<td>40</td>
<td>40</td>
<td>42</td>
<td>42</td>
<td>44</td>
<td>44</td>
<td>46</td>
<td>46</td>
<td>46</td>
<td>48</td>
<td>50</td>
<td>50</td>
<td>50</td>
<td>52</td>
<td>52</td>
<td>54</td>
</tr>
<tr>
<td>6</td>
<td>349</td>
<td>353</td>
<td>359</td>
<td>367</td>
<td>373</td>
<td>379</td>
<td>383</td>
<td>389</td>
<td>397</td>
<td>401</td>
<td>409</td>
<td>419</td>
<td>421</td>
<td>431</td>
<td>433</td>
<td>439</td>
</tr>
<tr>
<td>7</td>
<td>58</td>
<td>58</td>
<td>58</td>
<td>60</td>
<td>62</td>
<td>62</td>
<td>62</td>
<td>65</td>
<td>66</td>
<td>66</td>
<td>68</td>
<td>68</td>
<td>70</td>
<td>70</td>
<td>72</td>
<td>72</td>
</tr>
<tr>
<td>8</td>
<td>449</td>
<td>457</td>
<td>461</td>
<td>463</td>
<td>467</td>
<td>479</td>
<td>487</td>
<td>491</td>
<td>499</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>74</td>
<td>76</td>
<td>76</td>
<td>76</td>
<td>76</td>
<td>78</td>
<td>80</td>
<td>80</td>
<td>82</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A Pattern?

F. Calegari (during a talk I gave): There is almost a pattern!!! Frank, Romyar Sharifi and I computed $2 \cdot [\bar{T}_4(p) : T_4(p)]$ 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

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

where

$$a(p, k) = \begin{cases} 
0 & \text{if } p \equiv 1 \pmod{12}, \\
3 \cdot \binom{\left\lfloor \frac{k}{6} \right\rfloor}{2} & \text{if } p \equiv 5 \pmod{12}, \\
2 \cdot \binom{\left\lfloor \frac{k}{4} \right\rfloor}{2} & \text{if } p \equiv 7 \pmod{12}, \\
a(5, k) + a(7, k) & \text{if } p \equiv 11 \pmod{12}.
\end{cases}$$
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 $\text{ord}_p([\tilde{T}_k(p) : T_k(p)]) = 5$.

In our data when $k > p + 1$, then the conjectural $\text{ord}_p$ is often less than the actual $\text{ord}_p$. 
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