Modular Degrees of Elliptic Cu
and
Discriminants of Hecke Algeb

William Stein*

http://modular.fas.harvard.edu

ANTS VI, June 18, 2004

*Joint with F. Calegari

Goal

Let p be a prime. The goal of this talk is to explain
the following *increasingly general* Calegari-Stein conje

Conjecture 1. (−). If $E/\mathbf{Q}$ is an elliptic
conductor p, then the modular degree m_E of
divisible by p.

Conjecture 2. (−). If $\mathbf{T}_2(p)$ is the H
gebra associated to $S_2(\Gamma_0(p))$, then p does n
the index of $\mathbf{T}_2(p)$ in its normalization.

Conjecture 3. (−). If $p > k-1$, then th
explicit formula for the p-part of the index of
its normalization.

Conj 1: If E of conductor p, then

Vandiver: Conjecture 1 looks like Vandiver's conject
asserts that $p \nmid h_p^-$. (Note Flach's Selmer group conne

Data: (Watkins) For $p < 10^7$ there are 52878 curve
Watkins table. No counterexamples to conjecture
are 23 curves such that m_E is divisible by a prime ℓ
example the curve $y^2 + xy = x^3 - x^2 - 391648x - 94$
prime conductor $p = 4847093$ has modular degree $2 \cdot$
Smallest p with $\ell > p$ is $p = 1194923$.

Ratio: Max ratio m_E/p is ~ 23.2, attained for $p =$
First curve with $m_E/p > 1$ has level 13723, where m_E
$2^4 \cdot 3 \cdot 337$. Smallest $m_E/p > 1$ is $p = 1757963$; $m_E =$

Conjecture is consistent with ABC-conjecture (m_E is

Cuspidal Modular Form

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

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

and f is holomorphic at the cus

Fourier Expansion:

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

Modular Forms Example

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

For $k \geq 2$, a basis of $S_k(N)$ can be computed to
precision using modular symbols (e.g., my MAGMA
Appears that no formal analysis of complexity has b
Certainly polynomial time in N and required precision

```
MAGMA CODE
> 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)
]
```

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 +
    q^2 - 2*q^13 + 78*q^14 + 24*q^15 - 338*q^16 + O
    q^3 + 18*q^13 - 72*q^14 + 89*q^15 + 492*q^16 + O
    q^4 + 12*q^13 + 31*q^14 - 18*q^15 - 193*q^16 + O
    q^5 - 10*q^13 + 46*q^14 - 63*q^15 - 52*q^16 + O
    q^6 + 11*q^13 - 18*q^14 - 74*q^15 - 4*q^16 + O(q
    q^7 - 7*q^13 - 16*q^14 + 42*q^15 - 84*q^16 + O(q
    q^8 - q^13 - 16*q^14 - 18*q^15 - 34*q^16 + O(q^1
    q^9 - 8*q^13 - 2*q^14 - 3*q^15 + 16*q^16 + O(q^1
    q^10 - 5*q^13 - 2*q^14 - 6*q^15 + 14*q^16 + O(q
    q^11 + 12*q^13 + 12*q^14 + 12*q^15 + 12*q^16 + O
    q^12 - 2*q^13 - q^14 + 2*q^15 + q^16 + O(q^17)
```

Hecke algebras

Hecke Operators: Let p be a prime.

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

(If $p \mid N$, drop the second summand.) This preserves
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 Algeb

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

Sturm Bound: $\mathbf{T}_k(N)$ is generated as a $\mathbf{Z}$-module by T
where b is the ceiling of

$$\frac{k}{12} \cdot N \cdot \prod_{p \mid N} \left(1 - \frac{1}{p}\right).$$

Example: For $N = 37$, bound is 7, and $\mathbf{T}_2(37)$ h
$T_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $T_2 = \begin{pmatrix} -2 & 1 \\ 0 & 0 \end{pmatrix}$.

There are several other $\mathbf{T}_k(N)$-modules isomorphic
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 measu
cation, or what's the same, congruences between sin
eigenvectors for $\mathbf{T}_k(N)$, hence is related to the modu

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 $\mathbf{Z}$-mod

Examples:

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

$$\mathrm{Disc}(\mathbf{T}_{14}(11)) = 2^{46} \cdot 3^{14} \cdot 5^{2} \cdot 11^{42} \cdot 79 \cdot 241 \cdot 1163 \cdot 40163 \cdot$$
$$47552569849 \cdot 124180041087631 \cdot 20562$$

Ribet's Question

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

Question: (Ribet, 1997) Is there a prime p so that $p \mid$ I

Ribet had proved a theorem about $X_0(p) \cap J_0(p)_{\mathrm{tor}}$
hypothesis that $p \nmid \mathbf{T}_2(p)$, and wanted to know how res
hypothesis was. Note that when $k > 2$, usually $p \mid$ Dis

Using a PARI script of Joe Wetherell, I set up a comp
my laptop and found exactly one example: $p = 389$.

Index in the Normalizatio

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

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

It turned out that Ribet could prove his theorem weaker hypothesis that $p \nmid [\tilde{\mathbf{T}}_k(p) : \mathbf{T}_k(p)]$. I was una a counterexample to this divisibility. (Note: Matt Bak was a proof of the full theorem using different metho

Conjecture 2

Conjecture 2. (−). If $\mathbf{T}_2(p)$ is the H
gebra associated to $S_2(\Gamma_0(p))$, then p does n
the index of $\mathbf{T}_2(p)$ in its normalization.

The primes that divide $[\tilde{\mathbf{T}}_k(p) : \mathbf{T}_k(p)]$ are called *c*
primes. They are the primes of congruence between no
conjugate eigenvectors for $\mathbf{T}_k(p)$. Using this observati
other theorem of Ribet (and Wiles et al. modularity
that a "no" answer to the above question implies that
divide the modular degree of any elliptic curve of co
This is why Conjecture 2 implies Conjecture 1.

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

Higher Weight

Recall that

$$\mathrm{Disc}(\mathbf{T}_{14}(11)) = 2^{46} \cdot 3^{14} \cdot 5^{2} \cdot \mathbf{11}^{42} \cdot 79 \cdot 241 \cdot 1163 \cdot 40163 \cdot$$
$$47552569849 \cdot 124180041087631 \cdot 20562$$

Notice the large power of 11. Upon computing the p-maxi
$\mathbf{T}_{14}(11) \otimes_{\mathbf{Z}} \mathbf{Q}$, we find that $11 \nmid \mathrm{Disc}(\tilde{\mathbf{T}}_{14}(11))$, so all the 11
dex 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 $k = 4$

Each row contains p and $\mathrm{ord}_p(\mathrm{Disc}(\mathbf{T}_4(17)))$. E.g., $\mathrm{ord}_{17}(\mathrm{Disc}(\mathbf{T}$

2	3	5	7	11	13	17	19	23	29	31	37	41
0	0	0	0	0	2	2	2	2	4	4	6	6
61	67	71	73	79	83	89	97	101	103	107	109	113
10	10	10	12	12	12	14	16	16	16	16	18	18
149	151	157	163	167	173	179	181	191	193	197	199	211
24	24	26	26	26	28	28	30	30	32	32	32	34
239	241	251	257	263	269	271	277	281	283	293	307	311
38	40	40	42	42	44	44	46	46	46	48	50	50
347	349	353	359	367	373	379	383	389	397	401	409	419
56	58	58	58	60	62	62	62	65	66	66	68	68
443	449	457	461	463	467	479	487	491	499			
72	74	76	76	76	76	78	80	80	82			

F. Calegari (during a talk I gave): Except for 389, there is clear
Calegari and I computed $2 \cdot [\tilde{\mathbf{T}}_4(p) : \mathbf{T}_4(p)]$ and obtained the sa
as above, except for $p = 389$ which now gives 64. We also cons
examples where

$$2 \cdot [\tilde{\mathbf{T}}_4(p) : \mathbf{T}_4(p)] \neq \mathrm{Disc}(\mathbf{T}_k(p)).$$

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
pared to k. Though it works for our running example $p = 11$, k
the formula yields $0 + 3 \cdot \binom{3}{2} + 2 \cdot \binom{4}{2} = 9 + 12 = 21$, which is co

Summary

For a long time I had no idea whether to conjecture that the
shouldn't be mod p congruence between nonconjugate eigenfor
alently, whether p divides modular degrees at prime level. By
higher weight and *computing*, a simple conjectural formula em
when specialized to 2 is the conjecture that there are no mod p

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

Computational Question. Push computation of $\mathrm{ord}_p(\mathrm{Disc}(\mathbf{T}_2(p$
using Wiedemann's minimal polynomial algorithm.

Vandiver-ish Question. Investigate the connection between
and Flach's results on modular degrees annihilating Selmer grou