Discriminants of Hecke Algebras at Prime Level

William A. Stein*

September 24, 2002

Abstract

We study p-divisibility of discriminant of Hecke algebras associated to spaces of cusp forms of prime level. By considering cusp forms of weight bigger than 2, we are are led to make a conjecture about indexes of Hecke algebras in their normalization which, if true, implies that there are no mod p congruences between non-conjugate newforms in $S_2(\Gamma_0(p))$.

1 Introduction

I started working in modular forms when Ken Ribet asked about discriminants of Hecke algebras at prime level. I've recently revisited this question and, with the help of Frank Calegari, have made some interesting discoveries.

2 Discriminants of Hecke Algebras

Let R be a ring and let A be an R algebra that is free as an R module. The trace of an element of A is the trace, in the sense of linear algebra, of left multiplication by that element on A.

Definition 2.1 (Discriminant). Let $\omega_1, \ldots, \omega_n$ is a R-basis for A. Then the *discriminant* of A, denoted $\mathrm{disc}(A)$, is the determinant of the $n \times n$ matrix $(\mathrm{tr}(\omega_i \omega_j))$, which is well defined modulo squares of units in A.

When $R = \mathbb{Z}$ the discriminant is well defined, since the only units are ± 1.

Proposition 2.2. *Suppose R is a field. Then A has discriminant* 0 *if and only if A is separable over R, i.e., for every extension R' of R, the ring $A \otimes R'$ contains no nilpotents.*

The following proof is summarized from Section 26 of Matsumura. If A contains a nilpotent then that nilpotent is in the kernel of the trace pairing. If A is separable then we may assume that R is algebraically closed. Then A is an Artinian reduced ring, hence isomorphic as a ring to a finite product of copies of R, since R is algebraically closed. Thus the trace form on A is nondegenerate.

[*] This will eventually be a joint paper with Frank Calegari.

2.1 The Discriminant Valuation

Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, e.g., $\Gamma = \Gamma_0(p)$ or $\Gamma_1(p)$. For any integer $k \geq 1$, let $S_k(\Gamma)$ denote the space of holomorphic weight-k cusp forms for Γ. Let

$$\mathbb{T} = \mathbb{Z}[\ldots, T_n, \ldots] \subset \mathrm{End}(S_k(\Gamma))$$

be the associated Hecke algebra. Then $\mathbb{T}$ is a commutative ring that is free and of finite rank as a $\mathbb{Z}$-module. Also of interest is the image $\mathbb{T}^{\mathrm{new}}$ of $\mathbb{T}$ in $\mathrm{End}(S_k(\Gamma)^{\mathrm{new}})$.

Example 2.3. Let $\Gamma = \Gamma_0(243)$, which is illustrated on my T-shirt. Since $243 = 3^5$, experts will immediately deduce that $\mathrm{disc}(\mathbb{T}) = 0$. A computation shows that

$$\mathrm{disc}(\mathbb{T}^{\mathrm{new}}) = 2^{13} \cdot 3^{40},$$

which reflects the mod-2 and mod-3 intersections all over my shirt.

Definition 2.4 (Discriminant Valuation). Let p be a prime and suppose that $\Gamma = \Gamma_0(p)$ or $\Gamma_1(p)$. The *discriminant valuation* is

$$d_k(\Gamma) = \mathrm{ord}_p(\text{the discriminant of } \mathbb{T}).$$

3 Motivation and Applications

Let p be a prime and suppose that $\Gamma = \Gamma_0(p)$ or $\Gamma_1(p)$. The quantity $d_k(\Gamma)$ is of interest because it measures mod p congruences between eigenforms in $S_k(\Gamma)$.

Proposition 3.1. *Suppose that $d_k(\Gamma)$ is finite. Then the discriminant valuation $d_k(\Gamma)$ is nonzero if and only if there is a mod-p congruence between two Hecke eigenforms in $S_k(\Gamma)$ (note that the two congruent eigenforms might be Galois conjugate).*

Proof. It follows from Proposition 2.2 that $d_k(\Gamma) > 0$ if and only if $\mathbb{T} \otimes \overline{\mathbb{F}}_p$ is not separable. The Artinian ring $\mathbb{T} \otimes \overline{\mathbb{F}}_p$ is not separable if and only if the number of ring homomorphisms $\mathbb{T} \otimes \overline{\mathbb{F}}_p \to \overline{\mathbb{F}}_p$ is less than

$$\dim_{\overline{\mathbb{F}}_p} \mathbb{T} \otimes \overline{\mathbb{F}}_p = \dim_{\mathbb{C}} S_k(\Gamma).$$

Since $d_k(\Gamma)$ is finite, the number of ring homomorphisms $\mathbb{T} \otimes \overline{\mathbb{Q}}_p \to \overline{\mathbb{Q}}_p$ equals $\dim_{\mathbb{C}} S_k(\Gamma)$. Using the standard bijection between congruences and normalized eigenforms, we see that $\mathbb{T}\otimes\overline{\mathbb{F}}_p$ is not separable if and only if there is a mod-p congruence between two eigenforms. □

Example 3.2. If $\Gamma = \Gamma_0(389)$ and $k = 2$, then $\dim_{\mathbb{C}} S_2(\Gamma) = 32$. Let f be the characteristic polynomial of T_2. One can check that f is square free and 389 exactly divides the discriminant of f, so T_2 generated $\mathbb{T} \otimes \mathbb{Z}_{389}$ as a ring. (If it generated a subring of $\mathbb{T} \otimes \mathbb{Z}_{389}$ of finite index, then the discriminant of f would be divisible by 389^2.)

Modulo 389 the polynomial f is congruent to

$$\begin{aligned}&(x+2)(x+56)(x+135)(x+158)(x+175)^2(x+315)(x+342)(x^2+387)\\&(x^2+97x+164)(x^2+231x+64)(x^2+286x+63)(x^5+88x^4+196x^3+\\&113x^2+168x+349)(x^{11}+276x^{10}+182x^9+13x^8+298x^7+316x^6+\\&213x^5+248x^4+108x^3+283x^2+x+101)\end{aligned}$$

The factor $(x+175)^2$ indicates that $\mathbb{T}\otimes\overline{\mathbb{F}}_{389}$ is not separable since the image of T_2+175 is nilpotent (its square is 0). There are 32 eigenforms over $\mathbb{Q}_2$ but only 31 mod-389 eigenforms, so there must be a congruence. Let F be the 389-adic newform whose a_2 term is a root of

$$x^2+(-39+190\cdot 389+96\cdot 389^2+\cdots)x+(-106+43\cdot 389+19\cdot 389^2+\cdots).$$

Then the congruence is between F and its $\mathrm{Gal}(\overline{\mathbb{Q}}_{389}/\mathbb{Q}_{389})$-conjugate.

Example 3.3. The discriminant of the Hecke algebra $\mathbb{T}$ associated to $S_2(\Gamma_0(389))$ is

$$2^{53}\cdot 3^4\cdot 5^6\cdot 31^2\cdot 37\cdot 389\cdot 3881\cdot 215517113148241\cdot 477439237737571441$$

I computed this using the following algorithm, which was suggested by Hendrik Lenstra. Using the Sturm bound I found a b such that $T_1,\ldots,T_b$ generate $\mathbb{T}$ as a $\mathbb{Z}$-module. I then found a subset B of the T_i that form a $\mathbb{Q}$-basis for $\mathbb{T}\otimes_{\mathbb{Z}}\mathbb{Q}$. Next, viewing $\mathbb{T}$ as a ring of matrices acting on $\mathbb{Q}^{32}$, I found a random vector $v\in\mathbb{Q}^{32}$ such that the set of vectors $C=\{T(v):T\in B\}$ is linearly independent. Then I wrote each of $T_1(v),\ldots,T_b(v)$ as $\mathbb{Q}$-linear combinations of the elements of C. Next I found a $\mathbb{Z}$-basis D for the $\mathbb{Z}$-span of these $\mathbb{Q}$-linear combinations of elements of C. Tracing everything back, I find the trace pairing on the elements of D, and deduce the discriminant by computing the determinant of the trace pairing matrix. The most difficult step is computing D from $T_1(v),\ldots,T_b(v)$ expressed in terms of C, and this explains why we embed $\mathbb{T}$ in $\mathbb{Q}^{32}$ instead of viewing the elements of $\mathbb{T}$ as vectors in $\mathbb{Q}^{32^2}$. This whole computation takes one second on an Athlon 2000 processor.

3.1 Literature

I've seen a version of Theorem 4.1 referred to in the following papers:

1. Ribet: *Torsion points on $J_0(N)$ and Galois representations*
2. Loïc Merel and William Stein: *The field generated by the points of small prime order on an elliptic curve*
3. Ken Ono and William McGraw: *Modular form Congruences and Selmer groups* (McGraw will speak about this next week in this seminar!)
4. Momose and Ozawa: *Rational points of modular curves $X_{\text{split}}(p)$*

4 Data About Discriminant Valuations

4.1 Weight Two

Theorem 4.1. *The only prime $p<60000$ such that $d_2(\Gamma_0(p))>0$ is $p=389$. (Except possibly* 50923 *and* 51437*, which I haven't finished checking yet.)*

Proof. This is the result of a large computer computation, and perhaps couldn't be verified any other way, since I know of no general theorems about $d_2(\Gamma_0(p))$. The rest of this proof describes how I did the computation, so you can be convinced that there is valid mathematics behind my computation, and that you could verify the computation given sufficient time. The computation described below took about one week using 12 Athlon 2000MP processors. In 1999 I had checked the result stated above but only for $p<14000$ using a completely different implementation of the algorithm and a 200Mhz Pentium computer. These computations are nontrivial; we compute spaces of modular symbols, supersingular points, and Hecke operators on spaces of dimensions up to 5000.

The aim is to determine whether or not p divides the discriminant of the Hecke algegra of level p for each $p < 60000$. If T is an operator with integral characteristic polynomial, we write $\operatorname{disc}(T)$ for $\operatorname{disc}(\operatorname{charpoly}(T))$, which also equals $\operatorname{disc}(\mathbb{Z}[T])$. We will often use that

$$\operatorname{disc}(T) \bmod p = \operatorname{disc}(\operatorname{charpoly}(T) \bmod p).$$

Most levels $p < 60000$ were ruled out by computing characteristic polynomials of Hecke operators using an algorithm that David Kohel and I implemented in MAGMA, which is based on the Mestre-Oesterle method of graphs (our implementation is "The Modular of Supersingular Points" package that comes with MAGMA). I computed $\operatorname{disc}(T_q)$ modulo p for several primes q, and in most cases found a q such that this discriminant is nonzero. The following table summarizes how often we used each prime q (note that there are 6057 primes up to 60000):

q	number of $p < 60000$ where q smallest s.t. $\operatorname{disc}(T_q) \neq 0 \bmod p$
2	5809 times
3	161 (largest: 59471)
5	43 (largest: 57793)
7	15 (largest: 58699)
11	15 (the smallest is 307; the largest 50971)
13	2 (they are 577 and 5417)
17	3 (they are 17209, 24533, and 47387)
19	1 (it is 15661)

The numbers in the right column sum to 6049, so 8 levels are missing. These are

$$389, 487, 2341, 7057, 15641, 28279, 50923, \text{ and } 51437.$$

(The last two are still being processed. 51437 has the property that $\operatorname{disc}(T_q) = 0$ for $q = 2, 3, \ldots, 17$.) We determined the situation with the remaining 6 levels using Hecke operators T_n with n composite.

p	How we rule level p out, if possible
389	p does divide discriminant
487	using $\operatorname{charpoly}(T_{12})$
2341	using $\operatorname{charpoly}(T_6)$
7057	using $\operatorname{charpoly}(T_{18})$
15641	using $\operatorname{charpoly}(T_6)$
28279	using $\operatorname{charpoly}(T_{34})$

Computing T_n with n composite is very time consuming when p is large, so it is important to choose the right T_n quickly. For $p = 28279$, here is the trick I used to quickly find an n such that $\operatorname{disc}(T_n)$ is not divisible by p. This trick might be used to speed up the computation for some other levels. The key idea is to efficiently discover which T_n to compute. Though computing T_n on the full space of modular symbols is quite hard, it turns out that there is an algorithm that quickly computes T_n on subspaces of modular symbols with small dimension (see §3.5.2 of my Ph.D. thesis). Let M be the space of mod p modular symbols of level $p = 28279$, and let $f = \gcd(\operatorname{charpoly}(T_2), \operatorname{deriv}(\operatorname{charpoly}(T_2)))$. Let V be the kernel of $f(T_2)$ (this takes 7 minutes to compute). If $V = 0$, we would be done, since then $\mathrm{disc}(T_2) \neq 0 \in \mathbb{F}_p$. In fact, V has dimension 7. We find the first few integers n so that the charpoly of T_n on V_1 has distinct roots, and they are $n = 34$, 47, 53, and 89. I then computed charpoly(T_{34}) directly on the whole space and found that it has distinct roots modulo p. □

4.2 Higher Weight Data

1. The following are the valuations $d = d_4(\Gamma_0(p))$ at p of the discriminant of the Hecke algebras associated to $S_4(\Gamma_0(p))$ for $p < 500$.

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

5 The Conjecture

Let $k = 2m$ be an even integer and p a prime. Let $\mathbb{T}$ be the Hecke algebra associated to $S_k(\Gamma_0(p))$ and let $\tilde{\mathbb{T}}$ be the normalization of $\tilde{\mathbb{T}}$ in $\mathbb{T} \otimes \mathbb{Q}$.

Conjecture 5.1.

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

where

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

In particular, when $k = 2$ we conjecture that $[\tilde{\mathbb{T}} : \mathbb{T}]$ is not divisible by p.

Here $\binom{x}{y}$ is the binomial coefficient "x choose y", and floor and ceiling are as usual. We have checked this conjecture against significant numerical data. (Will describe here.)

6 Conjectures

Conjecture 6.1. *Suppose p is a prime and $k \geq 4$ is an even integer. If*

$$\begin{aligned}(p,k) \notin \{&(2,4),(2,6),(2,8),(2,10),\\ &(3,4),(3,6),(3,8),\\ &(5,4),(5,6),(7,4),(11,4)\}\end{aligned}$$

then $d_k(\Gamma_0(p)) > 0$.

Frank Calegari outlined a possible strategy for proving this conjecture.

Conjecture 6.2. *Suppose $p > 2$ is a prime and $k \geq 3$ is an integer. If*

$$\begin{aligned}(p,k) \notin \{&(3,3),(3,4),(3,5),(3,6),(3,7),(3,8),\\ &(5,3),(5,4),(5,5),(5,6),(5,7)\\ &(7,3),(7,4),(7,5),(11,3),(11,4),(11,5),\\ &(13,3),(17,3),(19,3)\}\end{aligned}$$

then $d_k(\Gamma_1(p)) > 0$.