Some computations with Hecke rings and deformation rings

Joan-C. Lario and René Schoof

(with an appendix by Amod Agashe and William Stein)

Abstract. In the proof by Wiles, completed by Taylor-Wiles, of the fact that all semi-stable elliptic curves over $\mathbf{Q}$ are modular, certain deformation rings play an important role. In this note we explicitly compute these rings for the elliptic curve $Y^2+XY=X^3-X^2-X-3$ of conductor 142.

1. Introduction.

In order to prove that semi-stable elliptic curves E over $\mathbf{Q}$ are modular, A. Wiles [17] considers the Galois representation $\overline{\rho}:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\longrightarrow\mathrm{GL}_2(\mathbf{F}_3)$ provided by the 3-torsion points $E[3]$ of a semi-stable elliptic curve E. He proves that certain rather restricted deformations of $\overline{\rho}$ are modular. It follows then that, in particular, the deformation provided by the Galois representation $\rho_E:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\longrightarrow\mathrm{GL}_2(\mathbf{Z}_3)$ associated to the 3-adic Tate module of E is modular. This implies that the curve E is modular.

Wiles proceeds in two steps. First he considers certain *minimal* deformations of $\overline{\rho}$. Using the Langlands-Tunnell Theorem [9, Thm.1.3] and some so-called 'level lowering theorems' [8], he constructs a normalized eigenform of weight 2 and minimal level N whose associated Galois representation

$$\rho_{\min}:\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\longrightarrow\mathrm{GL}_2(R)$$

is a *minimal* deformation of $\overline{\rho}$. Here the ring R is a finite extension of $\mathbf{Z}_3$. R. Taylor and Wiles [15] then show that the *universal* minimal deformation ring is isomorphic to a ring $\mathbf{T}$ of Hecke operators of level N. It follows that the minimal deformations are all modular.

It may happen that the representation ρ_E associated to the 3-adic Tate module of E is itself *not* minimal. Therefore Wiles's second step is to consider deformations of $\overline{\rho}$ that are not necessarily minimal, but satisfy more relaxed conditions at the primes that divide the conductor of E. From the fact that the minimal deformation ring is a Hecke ring, Wiles then deduces that the corresponding universal deformation rings are also isomorphic to certain Hecke rings. It follows then that the representation ρ_E is modular.

In this short note we explicitly compute the relevant universal deformation rings for a specific elliptic curve E. The main result is Theorem 3.2. Our example is the elliptic curve E of conductor 142 which is denoted by "142A" in the Antwerp Tables [1] (it is the curve 142C1 in J. Cremona's Tables [2]). A Weierstrass equation for E is given by

$$Y^2 + XY = X^3 - X^2 - X - 3.$$

As we explain below, the representation

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_3)$$

provided by the 3-torsion points $E[3]$ is unramified outside 3 and 71. Since 2 divides the conductor of E, but $\overline{\rho}$ is not ramified at the prime 2, the representation ρ_E associated to the 3-adic Tate module of E is *not* a minimal deformation of $\overline{\rho}$. Indeed, the minimal universal deformation ring is isomorphic to a ring $\mathbf{T}_{\min}$ of Hecke operators of level 71 rather than $142 = 2 \cdot 71$. We compute it in section 2. It has two $\mathbf{Z}_3$-valued points, one of which we call $\rho_{\min}$ and take it as the "origin" of the deformation space $\mathrm{Spec}(\mathbf{T}_{\min})$. In section 3 we study deformations ρ of $\overline{\rho}$ that need not be unramified at 2. In this case the universal deformation ring considered by Wiles is isomorphic to a ring of Hecke operators of level $284 = 4 \cdot 71$. We show that it is a complete intersection algebra of rank 8 over $\mathbf{Z}_3$. Since the elliptic curve E has conductor 142, one might have expected the universal deformation ring to be isomorphic to a Hecke ring of level $2 \cdot 71$ rather than $4 \cdot 71$. Therefore we also determine the two natural Hecke algebras of level 142 in section 4. These have $\mathbf{Z}_3$-ranks equal to 3 and 4 respectively. Both rings are complete intersections.

For the Hecke rings $\mathbf{T}$ of levels 71, 142 and 284, we also compute two invariants associated to the $\mathbf{Z}_3$-algebras $\mathbf{T}$ and the morphisms $\pi : \mathbf{T} \longrightarrow \mathbf{Z}_3$ provided by $\rho_{\min}$. Writing $I = \ker(\pi)$, we determine the *congruence ideal* $\eta = \pi(\mathrm{Ann}(I))$ and the *cotangent space* I/I^2 of $\mathbf{T}$. We have that $\#(I/I^2) = [\mathbf{Z}_3 : \eta]$ if and only if $\mathbf{T}$ is a complete intersection [5, Crit.I].

We conclude this introduction by giving some relevant information concerning the curve 142A. Counting points on E modulo the primes p with $3 \leq p \leq 67$ one finds that $\#E(\mathbf{F}_p) = p + 1 - a_p$ with a_p as in Table 1.1.

Table 1.1 *Fourier coefficients a_p.*

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67
a_p	0	2	0	6	4	6	-8	-4	-2	-8	10	-2	-8	-4	0	10	-8	2

For $p \neq 2, 3, 71$ the characteristic polynomial of a Frobenius automorphism φ_p acting on $E[3]$ is given by $T^2 - a_p T + p \in \mathbf{F}_3[T]$. As in [13, sect.5.5] one deduces from Table 1.1 that $\overline{\rho}$ is surjective and hence irreducible. Alternatively, the X-coordinates of the 3-torsion points are the zeroes of the polynomial $3X^4 - 3X^3 - 6X^2 - 36X + 8$. It is not difficult to show directly that the Galois group of this polynomial is isomorphic to S_4, and deduce that the representation $\overline{\rho}$ is surjective.

We briefly discuss the behavior of the critical primes 2, 3 and 71 with respect to the representation $\overline{\rho}$. The discriminant of the curve 142A is equal to $-2^6 71$.

- Since E has good reduction modulo 3, the representation $\overline{\rho}$ is "flat at 3", i.e. the Zariski closure of the 3-torsion points in the Néron model of E over $\mathbf{Z}_3$ is a finite flat group scheme. Since $a_3 = 0$, the elliptic curve E is supersingular modulo 3 and the representation $\overline{\rho}$ is non-ordinary.
- The curve E has multiplicative reduction modulo 71. Since the 71-adic valuation of the discriminant is not divisible by 3, the theory of the Tate curve implies that the representation $\overline{\rho}$ is ramified at 71. Moreover, $\overline{\rho}$ is of type (A) at 71. This means that the image $\overline{\rho}(I_{71})$ of the inertia group I_{71} at any prime over 71 is contained in a subgroup conjugate to $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$.
- The curve E has non-split multiplicative reduction at 2. Since the 2-adic valuation of Δ is divisible by 3, the representation $\overline{\rho}$ is unramified and hence flat at 2. Alternatively, one can show directly that the number field generated by a zero of the quartic polynomial above is only ramified at 3 and 71. Because of this, the Galois representation ρ_E associated to the 3-adic Tate module of E is not a minimal deformation of $\overline{\rho}$ in the sense of Wiles. See [11] for similar octahedral calculations.

We would like to thank the referee for his very useful suggestions.

2. The Hecke ring of level 71.

In this section we consider *minimal* deformations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(R)$ of the representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_3)$ associated to the 3-torsion points of the elliptic curve 142A mentioned in the introduction. Here R is a local Noetherian $\mathbf{Z}_3$-algebra with residue field $\mathbf{F}_3$ and the diagram

$$\begin{tikzcd}
 & \mathrm{GL}_2(R) \arrow[d] \\
\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \arrow[ur, "\rho"] \arrow[r, "\overline{\rho}"] & \mathrm{GL}_2(\mathbf{F}_3)
\end{tikzcd}$$

is commutative. We consider deformations ρ of the following type:

- ρ is unramified outside $\{3, 71\}$;
- ρ is flat at 3;
- ρ is of type (A) at 71;
- the determinant of ρ is the cyclotomic character.

The first condition ensures that ρ is minimal. See [10, section 29]. Since the representation $\overline{\rho}$ is irreducible, there exists by [10, sections 26, 29 and 31] a universal deformation of this type:

$$\rho_{\mathrm{univ}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(R_{\mathrm{univ}}).$$

Wiles shows [4, Thm 8] that the universal deformation ring R_{univ} is isomorphic to a certain local 3-adic ring $\mathbf{T}_{\mathrm{min}}$ of Hecke operators T_n. The ring $\mathbf{T}_{\mathrm{min}}$ is the $\mathbf{Z}_3$-subalgebra

$$\mathbf{T}_{\mathrm{min}} \quad \subset \quad \tilde{\mathbf{T}} = \prod_f O_f$$

generated by the vectors $T_n = (a_n(f))_f$. Here f runs over the normalized 3-adic eigenforms of level 71 whose Fourier coefficients $a_p(f)$ are congruent to the coefficients a_p associated to the curve 142A. The rings O_f denote the rings of integers of the extension of $\mathbf{Q}_3$ generated by the Fourier coefficients $a_p(f)$ of f. By the Theorem of the appendix, $\mathbf{T}_{\min}$ is generated as a $\mathbf{Z}_3$-module by the operators T_n with $n \leq 2 \cdot 72/12 = 12$. Note that by [7, Lemma 3.2] the Hecke operators T_p with $p \neq 3$ generate $\mathbf{T}_{\min}$ as a $\mathbf{Z}_3$-algebra. Therefore our definition of $\mathbf{T}_{\min}$ agrees with the one in [7, section 3].

The space $S_2(\Gamma_0(71))$ of weight 2 cusp forms of level 71 has dimension 6 and a basis can be found in [3] or can be computed with W. A. Stein's package [14]. The Hecke action decomposes $S_2(\Gamma_0(71))$ over $\mathbf{Q}$ into a product of two subspaces of dimension 3 corresponding to a pair of newforms f_{71} and f'_{71}. The Fourier coefficients $a_n(f_{71})$ of f_{71} or $a_n(f'_{71})$ of f'_{71} are contained in the same totally real cubic field of discriminant 257, generated by u where $u^3 - 5\,u + 3 = 0$. For $n \leq 12$ they are listed in Table 2.1.

Table 2.1 *Hecke operators T_n.*

n	$a_n(f_{71})$	$a_n(f'_{71})$	mod 81
1	1	1	(1,1)
2	u	$3 - u - u^2$	(60,69)
3	$3 - u^2$	$-3 + u + u^2$	(48,12)
4	$-2 + u^2$	$1 + u$	$(34, 61)$
5	$-1 - u$	$5 - 2u - u^2$	$(20, 11)$
6	$3 - 2u$	$-3 - u$	$(45, 18)$
7	$-6 + 2u + 2u^2$	$-6 + 2u + 2u^2$	(24,24)
8	$-3 + u$	$-u$	$(57, 21)$
9	$6 - 3u - u^2$	u	(33,60)
10	$-u - u^2$	$6 + u - u^2$	$(66, 30)$
11	$6 - 2u - 2u^2$	$2u$	(57,39)
12	$-6 + 3u$	$-6 + 3u + 2u^2$	$(12, 3)$

The polynomial $X^3 - 5X + 3 \in \mathbf{Z}_3[X]$ factors as a product of a linear and an irreducible quadratic factor. Mapping u to the unique root u_0 of $X^3 - 5X + 3$ in $\mathbf{Z}_3$, we obtain a 3-adic eigenform which we also denote by f_{71} and whose Fourier coefficients $a_p(f_{71})$ are congruent to the coefficients a_p associated to the curve 142A. See Table 1.1. On the other hand, mapping u to a root of the irreducible quadratic divisor of $X^3 - 5X + 3$, gives rise to a 3-adic eigenform whose Fourier coefficients are *not* congruent to the coefficients a_p. The same happens with the other eigenform f'_{71}.

Using the approximation $u_0 \equiv 60 \pmod{3^4}$, we list the vectors $T_n = (a_n(f_{71}), (a_n(f'_{71}))$ in the rightmost column of Table 2.1 with a precision of $O(3^4)$. The Hecke ring $\mathbf{T}_{\min}$ is the $\mathbf{Z}_3$-submodule of $\tilde{\mathbf{T}} = \mathbf{Z}_3 \times \mathbf{Z}_3$ generated by the vectors T_n for $n \leq 12$.

The following Lemma enables us to do the 3-adic computations with finite precision.

Lemma 2.2. *Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and let M be a finitely generated R-module. Let M_1 and M_2 be two submodules of M and suppose there is an integer $k > 0$ for which*

- $M_1 + \mathfrak{m}^k M = M_2 + \mathfrak{m}^k M$,
- $\mathfrak{m}^{k-1} M \subset M_2$;

then $M_1 = M_2$.

Proof. Since $\mathfrak{m}^{k-1}M \subset M_2 \subset M_1 + \mathfrak{m}^k M$, Nakayama's Lemma implies that $\mathfrak{m}^{k-1}M \subset M_1$. This implies that $\mathfrak{m}^k M$ is contained in M_1 as well as M_2 so that $M_1 = M_2$ as required.

Theorem 2.3. *There is an isomorphism between complete intersections*

$$\mathbf{T}_{\mathrm{min}} \cong \mathbf{Z}_3[[X]]/(X^2 - 9X).$$

Proof. We apply Lemma 2.2 to the $\mathbf{Z}_3$-module $M = \tilde{\mathbf{T}}$ and to the submodules $M_1 = \mathbf{T}$ and M_2, the $\mathbf{Z}_3$-submodule generated by any lifts of the row vectors in the rightmost column of Table 2.1. It is easy to see that M_2 has $\mathbf{Z}_3$-basis $(1, 1)$ and $(0, 9)$ so that $3^2\tilde{\mathbf{T}} \subset M_2$. Now Let $k = 3$. Then $3^{k-1}\tilde{\mathbf{T}} \subset M_2$. Since the computations were done with an accuracy of $O(3^4)$ we have that $M_1 = M_2$ modulo $3^k\tilde{\mathbf{T}}$. It follows that $\mathbf{T}_{\mathrm{min}}$ is the $\mathbf{Z}_3$-module generated by $1 = (1, 1)$ and $x = (0, 9)$. As a $\mathbf{Z}_3$-algebra $\mathbf{T}_{\mathrm{min}}$ is therefore generated by x. Since $x^2 = 9x$, the homomorphism $\mathbf{Z}_3[X]/(X^2 - 9X) \longrightarrow \mathbf{T}_{\mathrm{min}}$ given by $X \mapsto x$ is an isomorphism. Since the natural map $\mathbf{Z}_3[X]/(X^2 - 9X) \longrightarrow \mathbf{Z}_3[[X]]/(X^2 - 9X)$ is an isomorphism, the theorem follows.

The two $\mathbf{Z}_3$-valued points $\pi, \pi' : \mathbf{Z}_3[[X]]/(X^2 - 9X) \longrightarrow \mathbf{Z}_3$ given by $\pi(X) = 0$ and $\pi'(X) = 9$, are precisely the algebra homomorphisms given by, say, $T_n \mapsto a_n(f_{71})$ and $T_n \mapsto a_n(f'_{71})$ respectively. The η-invariant with respect to the first point is the $\mathbf{Z}_3$-ideal $\eta = \pi(\mathrm{Ann}_{\mathbf{T}}(I))$ where $I = \ker(\pi) = (X)$. Since $\mathbf{T}$ is a complete intersection, η is also the ideal for which $\#\mathbf{Z}_3/\eta = \#(X)/(X^2)$. Using either description one easily checks that η is the $\mathbf{Z}_3$-ideal generated by 3^2. See [5, Crit.I].

3. The Hecke ring of level 284.

In this section we consider deformations $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(R)$ of the representation $\overline{\rho}$ that are not necessarily minimal at the prime 2. As in Wiles's paper [17], these representations are supposed to satisfy the following more relaxed conditions:

- ρ is unramified outside $\{2,\ 3,\ 71\}$;
- ρ is flat at 3;
- ρ is of type (A) at 71;
- the determinant of ρ is the cyclotomic character.

It follows from the theory of the Tate curve that the deformation given by the 3-adic Tate module of the curve 142A is of this type. According to Wiles, the universal deformation ring is isomorphic to a certain 3-adic Hecke ring $\mathbf{T}$ of level $284 = 4 \cdot 71$ rather than $142 = 2 \cdot 71$. See the remarks in [7, p. 361].

The Hecke operators T_n in the algebra $\mathbf{T}$ of level 284 can be represented as row vectors $(a_n(f))_f$ with $f = f(z)$ running through the normalized 3-adic eigenforms of level 284 whose Fourier coefficients $a_p(f)$ are, for prime $p \neq 2, 3$, congruent to the coefficients a_p associated to the elliptic curve 142A, while $a_2(f) = 0$. The forms f are of the form $g(z)$, $g(z) - b_2 g(2z)$ or $g(z) - b_2 g(2z) + 2g(4z)$ where $g(z) = \sum_{n \geq 1} b_n q^n$ is a newform of level 284, 142 or 71 respectively. Since $T_2 = 0$, the vectors T_n are zero whenever n is even. The newforms of level 71 have already been described in the previous section. The new part of the space of weight 2 cusp forms $S_2(\Gamma_0(142))$ is a product of 1-dimensional eigenspaces for the action of the Hecke algebra. The Fourier coefficients of the eigenforms can be found in the Antwerp Tables [1]. The Fourier coefficients of three of these, viz. 142A, 142F and 142G, are for $p \neq 2$, congruent to the coefficients a_p of the curve 142A. Finally, there is up to conjugacy only one newform of level 284 whose Fourier coefficients $a_p(f_{284})$ are for $p \neq 2$, congruent to the coefficients a_p of the curve 142A. Its coefficients are contained in the cubic field $\mathbf{Q}_3(t)$ where $t^3 + 3t^2 - 3 = 0$. This totally ramified extension of $\mathbf{Q}_3$ has discriminant 81. Its ring of integers is $\mathbf{Z}_3[t]$.

In this way the Hecke ring $\mathbf{T}$ becomes the $\mathbf{Z}_3$-subalgebra of $\tilde{\mathbf{T}}$

$$\mathbf{T} \quad \subset \quad \tilde{\mathbf{T}} = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3[t]$$

generated as a $\mathbf{Z}_3$-module by the Hecke operators T_n with n odd. Here T_n is identified with the row vector consisting of the n-th Fourier coefficients of the eigenforms f_{71}, f'_{71}, $142A$, $142F$, $142G$ and f_{284} as displayed in the n-th row of Table 3.1. The q-expansion of the newform of level 284 was computed using modular symbols as in [14].

By Theorem 1 of the appendix, $\mathbf{T}$ is generated as a $\mathbf{Z}_3$-module by the operators T_n with $n \leq 2 \cdot 6 \cdot 72/12 = 72$. Since T_n is zero when n is even, it suffices to consider only the T_n for n odd. We remark that by [7, Lemma 3.2] one does not need T_3 to generate $\mathbf{T}$. Therefore our Hecke algebra agrees with the one in [7, sect.3].

The additive group of $\tilde{\mathbf{T}}$ is a free $\mathbf{Z}_3$-module of rank 8. Choosing the $\mathbf{Z}_3$-basis $\{1, t, t^2\}$ for $\mathbf{Z}_3[t]$, we view the Hecke operators T_p as vectors in $\mathbf{Z}_3^8$. For example, the Hecke operator T_{25} in Table 3.1 becomes the vector

$$(-4 + 2u + u^2,\ 8 - 3u - u^2\ , -1\ , 11\ , -1\ , 5\ , 9\ , 2).$$

We do the computations modulo 3^7. As in section 2, let u denote the unique root in $\mathbf{Z}_3$ of the polynomial $X^3 - 5X + 3$. We have that

$$u = 2\cdot 3 + 2\cdot 3^3 + 3^4 + 2\cdot 3^5 + 2\cdot 3^6 + O(3^7).$$

Table 3.1 *Hecke operators T_n.*

n	$a_n(f_{71})$	$a_n(f'_{71})$	142A	142F	142G	$a_n(f_{284})$
1	1	1	1	1	1	1
3	$3 - u^2$	$-3 + u + u^2$	0	-3	3	t
5	$-1 - u$	$5 - 2u - u^2$	2	-4	2	$-1 - 3t - t^2$
7	$-6 + 2u + 2u^2$	$-6 + 2u + 2u^2$	0	-3	-3	$-6 + 2t + 2t^2$
9	$6 - 3u - u^2$	u	-3	6	6	$-3 + t^2$
11	$6 - 2u - 2u^2$	$2u$	6	0	-6	$2t$
13	4	$-2 - 2u$	4	1	-5	$4 - 6t - 4t^2$
15	$-6 + 2u + u^2$	$-6 - u + u^2$	0	12	6	$-3 - t$
17	$-6 + 2u + 2u^2$	$6 - 2u^2$	6	0	6	$-6 + 6t + 4t^2$
19	$7 - u - u^2$	$7 - u - 2u^2$	-8	-5	1	$-2 - t^2$
21	$-12 + 2u + 2u^2$	$6 + 2u$	0	9	-9	$3 - 6t - t^2$
23	$-4 + 2u^2$	-4	-4	-7	5	$8 - 2t^2$
25	$-4 + 2u + u^2$	$8 - 3u - u^2$	-1	11	-1	$5 + 9t + 2t^2$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
67	$-4 + 4u$	$-4 - 2u$	2	-4	2	$-4 + 2t^2$
69	$-12 + 6u$	$12 - 4u - 4u^2$	0	21	15	$-6 + 8t + 6t^2$
71	1	1	1	1	1	1

Applying Hermite reduction to the row vectors, we find the matrix below. Let M_2 the $\mathbf{Z}_3$-submodule of $\tilde{\mathbf{T}}$ spanned by its rows. Incidentally, we find the same matrix using only the rows $n = 1, 3, \ldots, 17$. This means that the module M_2 is already generated by the T_n with n odd and $n \leq 17$. Now we apply Lemma 2.2 with $M = \tilde{\mathbf{T}}$, $M_1 = \mathbf{T}$ and M_2. It is easy to see that $3^5\tilde{\mathbf{T}} \subset M_2$. We take $k = 6$. Then $3^{k-1}\tilde{\mathbf{T}} \subset M_2$ and, since we did the computations with an accuracy of $O(3^7)$, we certainly have $M_1 + 3^k\tilde{\mathbf{T}} = M_2 + 3^k\tilde{\mathbf{T}}$. It follows that $\mathbf{T} = M_2$. Thus, as a $\mathbf{Z}_3$-module, $\mathbf{T}$ is generated by the rows of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 9 & 0 & 6 & 18 & 0 & 0 & 1 \\ 0 & 0 & 3 & 0 & 54 & 0 & -1 & -1 \\ 0 & 0 & 0 & 9 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 81 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

For later use we observe that the determinant of the matrix and hence the index $[\tilde{\mathbf{T}} : \mathbf{T}]$ are equal to 3^{12}. The first row of the matrix is the unit element $1 \in \mathbf{T}$. We let $x = (0,\ 9,\ 0,\ 6,\ 18\ ,t^2)$ be the element corresponding to the second row and $y = (0,\ 0,\ 3,\ 54,\ -t-t^2)$ be the one corresponding to the third row. The morphism $\varphi : \mathbf{Z}_3[X,Y] \longrightarrow \mathbf{T}$ given by $f(X,Y) \mapsto f(x,y)$ extends to a $\mathbf{Z}_3$-algebra morphism

$$\widehat{\varphi} : \mathbf{Z}_3[[X,Y]] \longrightarrow \mathbf{T}.$$

This follows from the fact that $x^n, y^n \to 0$ in $\tilde{\mathbf{T}}$ as $n \to \infty$.

Theorem 3.2. *The ring homomorphism $\widehat{\varphi}$ induces an isomorphism of $\mathbf{Z}_3$-algebras*

$$\mathbf{Z}_3[[X,Y]]/(F_1,F_2) \xrightarrow{\cong} \mathbf{T},$$

where

$$F_1 = 29412Y - 9804Y^2 - 91158XY - 1641XY^2 + 11618X^2Y - 787(X^3 - 15X^2 + 54X),$$
$$F_2 = 8514Y - 477Y^2 - 8204XY + 1741XY^2 + 2369X^2Y - 787Y^3.$$

Proof. We compute a few monomials in x and y of low degree in the subring $\mathbf{T}$ of $\tilde{\mathbf{T}}$:

$$\begin{array}{rl}
\mathbf{1} = (1, & 1,\ 1,\ 1,\ \ 1,\ \ 1\ ),\\
x = (0, & 9,\ 0,\ 6,\ \ 18,\ \ t^2\ ),\\
y = (0, & 0,\ 3,\ 0,\ \ 54,\ \ -t-t^2\ ),\\
x^2 = (0, & 81,\ 0,\ 36,\ \ 324,\ \ -9+3t+9t^2\ ),\\
xy = (0, & 0,\ 0,\ 0,\ \ 972,\ \ 6-3t-6t^2\ ),\\
y^2 = (0, & 0,\ 9,\ 0,\ \ 2916,\ \ -3+3t+4t^2\ ),\\
x^2y = (0, & 0,\ 0,\ 0,\ \ 17496,\ \ 45-18t-39t^2\ ),\\
xy^2 = (0, & 0,\ 0,\ 0,\ \ 52488,\ \ -27+12t+24t^2\ ).
\end{array}$$

Using the $\mathbf{Z}_3$-basis $\{1,t,t^2\}$ for the ring $\mathbf{Z}_3[t]$, we write these eight vectors as row vectors in $\mathbf{Z}_3^8$. The determinant of the resulting 8×8 matrix is equal to $-2^2 3^{12} 787$. Since the index $[\tilde{\mathbf{T}} : \mathbf{T}]$ is equal to 3^{12}, this implies that the Hecke ring $\mathbf{T}$ is equal to the $\mathbf{Z}_3$-span of the eight monomials above. It follows that φ and hence $\widehat{\varphi}$ are surjective. In order to determine the kernels of φ and $\widehat{\varphi}$, we express x^3, y^3 and x^2y^2 as $\mathbf{Z}_3$-linear combinations of the eight monomials above. Solving the corresponding linear systems of eight equations in eight unknowns one finds that

$$\begin{aligned}
787x^3 &= 29412y - 9804y^2 - 91158xy - 1641xy^2 + 11618x^2y - 787(54x - 15x^2),\\
787y^3 &= 8514y - 477y^2 - 8204xy + 1741xy^2 + 2369x^2y,\\
787x^2y^2 &= 15444y - 5148y^2 - 15870xy + 12657xy^2 + 6219x^2y.
\end{aligned}$$

In other words, $F_1(x,y) = F_2(x,y) = F_3(x,y) = 0$ where F_1 and F_2 are as above and

$$F_3 = 15444Y - 5148Y^2 - 15870XY + 12657XY^2 + 6219X^2Y - 787X^2Y^2.$$

Therefore $J = (F_1, F_2, F_3) \subset \ker(\varphi)$. Since $\mathbf{Z}_3[X,Y]/J$ has $\mathbf{Z}_3$-rank at most 8, it follows that $\ker(\varphi) = J$. Writing J' for the $\mathbf{Z}_3[[X,Y]]$-ideal (F_1, F_2, F_3), there is a commutative diagram

$$\begin{tikzcd}
\mathbf{Z}_3[X,Y]/J \arrow[r, "\cong"] \arrow[d] & \mathbf{T}. \\
\mathbf{Z}_3[[X,Y]]/J' \arrow[ur] &
\end{tikzcd}$$

Here the diagonal arrow is the morphism induced by $\widehat{\varphi}$. It is surjective. Reducing everything modulo 3, we obtain the diagram

$$\begin{tikzcd}
\mathbf{F}_3[X,Y]/\overline{J} \arrow[r, "\cong"] \arrow[d] & \mathbf{T}/3\mathbf{T}, \\
\mathbf{F}_3[[X,Y]]/\overline{J}' \arrow[ur, "\overline{\varphi}"'] &
\end{tikzcd}$$

where $\overline{J}$ and $\overline{J}'$ denote the ideals generated by the reduced polynomials $\overline{F}_1$, $\overline{F}_2$ and $\overline{F}_3$ in the rings $\mathbf{F}_3[X,Y]$ and $\mathbf{F}_3[[X,Y]]$ respectively and $\overline{\varphi} : \mathbf{F}_3[[X,Y]]/\overline{J}' \longrightarrow \mathbf{T}/3\mathbf{T}$ denotes the surjective morphism induced by $\widehat{\varphi}$. Since $\mathbf{F}_3[X,Y]/\overline{J}$ is an Artin ring, the natural map to the product of the completions at its maximal ideals is an isomorphism. Since the vertical map is the natural map from $\mathbf{F}_3[X,Y]/\overline{J}$ to its completion at the maximal ideal (X,Y), it is surjective. We conclude that $\overline{\varphi}$ is an isomorphism

$$\mathbf{F}_3[[X,Y]]/\overline{J}' \xrightarrow{\cong} \mathbf{T}/3\mathbf{T}.$$

From

$$\begin{aligned}
\overline{F}_1 &= -X^3 - X^2Y, \\
\overline{F}_2 &= -Y^3 + XY + XY^2 - X^2Y, \\
\overline{F}_3 &= -X^2Y^2,
\end{aligned}$$

we obtain the relation

$$-Y(X-1)\overline{F}_1 + X^2\overline{F}_2 = (1 + X + Y)\overline{F}_3$$

in $\mathbf{F}_3[[X,Y]]$. Since $1 + X + Y$ is a unit in $\mathbf{F}_3[[X,Y]]$, the monomial $\overline{F}_3$ belongs to the ideal $(\overline{F}_1, \overline{F}_2)$ so that $\overline{J}' = (\overline{F}_1, \overline{F}_2)$. We claim that the ideal $\widehat{J} = \ker(\widehat{\varphi}) \subset \mathbf{Z}_3[[X,Y]]$ is generated by F_1 and F_2. Indeed, since the Hecke algebra $\mathbf{T}$ is free over $\mathbf{Z}_3$, the exact sequence

$$0 \longrightarrow \widehat{J} \longrightarrow \mathbf{Z}_3[[X,Y]] \longrightarrow \mathbf{T} \longrightarrow 0.$$

remains exact after tensoring with $\mathbf{F}_3$. It follows that $\widehat{J}/3\widehat{J} = \overline{J}' = (\overline{F}_1, \overline{F}_2)$. Therefore

$$\widehat{J} \subset (F_1, F_2) + 3\,\widehat{J} \subset (F_1, F_2) + \mathfrak{m}\,\widehat{J}$$

where $\mathfrak{m} = (3, X, Y)$ denotes the maximal ideal of the local ring $\mathbf{Z}_3[[X,Y]]$. Nakayama's Lemma implies then that $\widehat{J} = (F_1, F_2)$. This proves the Theorem.

The "points" of the Hecke algebra $\mathbf{T}$ are $(X,Y) = (0,0)$, $(9,0)$, $(0,3)$, $(6,0)$, $(18,54)$ and the three conjugates of $(t^2, -t-t^2)$. The first two points correspond to the newforms of level 71, the next three to eigenforms of level 142 and the three conjugates of $(t^2, -t-t^2)$ to an eigenform of level 284. The point $(0,3)$ corresponds to the elliptic curve 142A of the introduction. The point $(0,0)$ is our origin. The canonical morphism from $\mathbf{T}$ to the minimal universal deformation ring of section 2 is given by $X \mapsto X$ and $Y \mapsto 0$. Since $\mathbf{T}$ is a complete intersection, the η-invariant associated to it is equal to the $\mathbf{Z}_3$-ideal generated by $\#I/I^2$ where I is the ideal (X,Y). The order of I/I^2 is given by the determinant of the matrix of the coefficients of the linear terms of F_1 and F_2. Since

$$\begin{aligned} F_1 &= -787{\cdot}54X + 29412Y &&+ \text{terms of deg} \geq 2,\\ F_2 &= \phantom{-787{\cdot}54X + 2}8514Y &&+ \text{terms of deg} \geq 2, \end{aligned}$$

it is the $\mathbf{Z}_3$-ideal generated by

$$\eta = \det\begin{pmatrix} -787{\cdot}54 & 29412 \\ 0 & 8514 \end{pmatrix} = 3^5 \cdot (\text{unit}).$$

This is 3^3 times the η-invariant of the minimal deformation ring computed in section 2. This agrees with [7, Lemma 4.4] because the contribution there of the Euler factors at 2 is equal to $(1-2)((1+2)^2 - a_2(f_{71})^2) = -3^2 + u^2$ and has 3-adic valuation equal to 3.

4. The Hecke rings of level 142.

In this section we study 3-adic Hecke rings $\mathbf{T}$ of level 142. In contrast to the Hecke rings of levels 71 and 284, there are *two* natural Hecke algebras of level 142 to consider. One is the completion $\mathbf{T}_{\mathfrak{m}}$ of the Hecke algebra at the maximal ideal $\mathfrak{m}$ corresponding to the representation $\overline{\rho}$ on the 3-torsion points of the elliptic curve 142A. Since E has non-split multiplicative reduction modulo 2, the ideal $\mathfrak{m}$ is generated by 3, by $T_p - a_p$ for p odd and by $T_2 + 1$. The other is the completion $\mathbf{T}_{\mathfrak{m}'}$ at the maximal ideal $\mathfrak{m}'$ generated by 3, by $T_p - a_p$ for p odd and by $T_2 - 1$.

In order to describe these two Hecke rings, we recall that f_{71} and f'_{71} denote the two 3-adic newforms of level 71 and let $\alpha, \beta \in \mathbf{Z}_3$ denote the zeroes of the characteristic polynomial $T^2 - a_2(f_{71})T + 2$. Similarly, $\alpha', \beta' \in \mathbf{Z}_3$ denote the zeroes of the polynomial $T^2 - a_2(f'_{71})T + 2$. We choose $\alpha, \alpha' \equiv 1 \pmod 3$ so that $\beta, \beta' \equiv -1 \pmod 3$. Then

$$\begin{aligned} f_\alpha(z) &= f_{71}(z) - \beta f_{71}(2z),\\ f_\beta(z) &= f_{71}(z) - \alpha f_{71}(2z), \end{aligned}$$

are eigenforms of level 142. We have that $T_2(f_\alpha) = \alpha f_\alpha$ and $T_2(f_\beta) = \beta f_\beta$. Similarly,

$$\begin{aligned} f_{\alpha'}(z) &= f'_{71}(z) - \beta' f'_{71}(2z),\\ f_{\beta'}(z) &= f'_{71}(z) - \alpha' f'_{71}(2z), \end{aligned}$$

are eigenforms with T_2-eigenvalues equal to α' and β' respectively. The forms f_α, f_β, $f_{\alpha'}$ and $f_{\beta'}$ are also eigenforms of the Hecke operators T_n with n odd with eigenvalues equal to the ones of level 71.

The elliptic curve 142G has equation $Y^2 + XY = X^3 - X^2 - 2626X + 52244$. Like 142A, it has non-split multiplicative reduction at 2. On the other hand, the curve 142F given by $Y^2 + XY + Y = X^3 - X^2 - 12X + 15$ has split multiplicative reduction. Therefore the Hecke algebra $\mathbf{T}_\mathfrak{m}$ is isomorphic to the $\mathbf{Z}_3$-subalgebra of $\tilde{\mathbf{T}} = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$ of the row vectors consisting of the n-th Fourier coeffients of f_β, $f_{\beta'}$, 142A and 142G, while the Hecke algebra $\mathbf{T}_{\mathfrak{m}'}$ is isomorphic to the $\mathbf{Z}_3$-subalgebra of $\tilde{\mathbf{T}}' = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$ consisting of the row vectors consisting of the n-th Fourier coeffients of f_α, $f_{\alpha'}$ and 142F.

Consider the Hecke algebra $\mathbf{T}_\mathfrak{m}$ first. The operators T_n with odd $n \leq 71$ generate the $\mathbf{Z}_3$-submodule spanned by the rows of the 8 by 8 matrix of section 3, omitting the colums corresponding to the curve 142F and the newforms of level 284, i.e., omitting columns 4, 6, 7 and 8. In other words, the Hecke operators T_n with odd $n \leq 71$ generate the $\mathbf{Z}_3$-submodule M of $\tilde{\mathbf{T}} = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$ spanned by the rows of the matrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 9 & 0 & 18 \\ 0 & 0 & 3 & 54 \\ 0 & 0 & 0 & 81 \end{pmatrix}.$$

Since $a_2(f_{71}) = u \equiv 627 \pmod{3^6}$, the zeroes α and β of the characteristic polynomial $T^2 - a_2(f_{71})T + 2$ satisfy $\alpha \equiv 448 \pmod{3^6}$ and $\beta \equiv 179 \pmod{3^6}$ respectively. Similarly, $a_2(f'_{71}) = 3 - u - u^2 \equiv 636 \pmod{3^6}$ and hence $\alpha' \equiv 709 \pmod{3^6}$ and $\beta \equiv 656 \pmod{3^6}$. Therefore the Hecke operator T_2 corresponds to the row vector $(179, 656, -1, -1)$. It is not difficult to check that $T_2 \cdot M \subset M$ so that M is actually equal to the $\mathbf{Z}_3$-submodule generated by *all* Hecke operators T_n with $n \leq 71$. Therefore, by the appendix, $M = \mathbf{T}_\mathfrak{m}$.

In order to calculate the algebra structure of $\mathbf{T}_\mathfrak{m}$, we let x and $y \in \mathbf{T}_\mathfrak{m}$ be the elements corresponding to the second and third row of the matrix above. The matrix with row vectors corresponding to 1, x, x^2 and y is equal to

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 9 & 0 & 18 \\ 0 & 81 & 0 & 324 \\ 0 & 0 & 3 & 54 \end{pmatrix}.$$

It has determinant $-2 \cdot 3^6$ which, up to a unit, is equal to the determinant of the 4×4 matrix we started with. Therefore the elements $1, x, x^2$ and y form a $\mathbf{Z}_3$-basis for $\mathbf{T}_\mathfrak{m}$. One checks that $y^2 - 3y - 17(x^2 - 9x)$, $xy - 6(x^2 - 9x)$ and $(x - 18)(x^2 - 9x)$ are all zero. The last polynomial is a linear combination of the first two in the ring $\mathbf{T}_\mathfrak{m}/3\mathbf{T}_\mathfrak{m}$ and hence in the Hecke ring $\mathbf{T}_\mathfrak{m}$ itself. Nakayama's Lemma and the arguments of the proof of Theorem 3.2 imply therefore that there is an isomorphism of $\mathbf{Z}_3$-algebras

$$\mathbf{T}_\mathfrak{m} \cong \mathbf{Z}_3[[X, Y]]/(Y^2 - 3Y - 17(X^2 - 9X), XY - 6(X^2 - 9X)),$$

mapping x, y to X, Y respectively. As predicted by [16, Theorem 3.4], the ring $\mathbf{T}_\mathfrak{m}$ is a Gorenstein ring. It is even a complete intersection. The four 'points' of $\mathbf{T}_\mathfrak{m}$ are $(X, Y) = (0, 0)$, $(0, 3)$, $(9, 0)$ and $(18, 54)$. The point $(0, 3)$ corresponds to the elliptic curve 142A. The point $(0,0)$ corresponds to the form f_β of level 71. It is the 'origin' of the deformation space. It follows that Wiles's η-invariant is generated by the order of I/I^2, where $I = (X, Y)$. One easily checks that it is equal to 3^4.

For the sake of completeness we also determine the structure of the $\mathbf{Z}_3$-algebra $\mathbf{T}_{\mathfrak{m}'}$. Note however that the associated modular representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\mathbf{T}_{\mathfrak{m}'})$ is *not* a deformation of the representation ρ_E we started with. The operators T_n with odd $n \leq 71$ generate the $\mathbf{Z}_3$-submodule spanned by the rows of the 8 by 8 matrix of section 3, omitting columns 3, 5, 6, 7 and 8. In other words, they generate the $\mathbf{Z}_3$-submodule M' of $\tilde{\mathbf{T}}'_{\mathfrak{m}} = \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$ spanned by the rows of the matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 9 & 6 \\ 0 & 0 & 9 \end{pmatrix}.$$

The Hecke operator T_2 corresponds to the row vector $(448, 709, 1)$. It is not difficult to check that $T_2 \cdot M' \subset M'$ so that M' is actually equal to the $\mathbf{Z}_3$-submodule generated by *all* Hecke operators T_n with $n \leq 71$. Therefore, by the appendix, $M' = \mathbf{T}_{\mathfrak{m}'}$.

In order to calculate the algebra structure of $\mathbf{T}_{\mathfrak{m}'}$, we let x be the element corresponding to the second row of the matrix. The matrix with row vectors corresponding to 1, x and x^2 has determinant $2 \cdot 3^4$ which, up to a unit, is equal to the determinant of the 3×3 matrix above. Therefore the elements $1, x$ and x^2 form a $\mathbf{Z}_3$-basis for $\mathbf{T}_{\mathfrak{m}'}$. One checks that $(x-6)(x^2-9x) = 0$. It follows that there is an isomorphism of $\mathbf{Z}_3$-algebras

$$\mathbf{T}_{\mathfrak{m}'} \cong \mathbf{Z}_3[[X]]/(X(X-6)(X-9)),$$

mapping x to X. As predicted by [16, Theorem 3.4], the ring $\mathbf{T}_{\mathfrak{m}'}$ is a Gorenstein ring. It is even a complete intersection. The three 'points' of $\mathbf{T}_{\mathfrak{m}'}$ are $X = 0$, 6 and 9 respectively. None of these points corresponds to the elliptic curve 142A. The point $(0,0)$ corresponds to the form f_α of level 71. If we take it as the origin of the deformation space, the η-invariant is equal to the ideal generated by 3^3.

Bibliography

[CSS] G. Cornell, J.H. Silverman and G. Stevens, Eds., *Modular forms and Fermat's Last Theorem*, Springer-Verlag, New York 1997.

[1] Birch, B.J. and Kuyk, W., *Modular Functions of One Variable IV*, Lecture Notes in Mathematics **476**, Springer-Verlag, 1975.

[2] Cremona, J., *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge 1992.

[3] Darmon, H., *Serre's conjectures*, in Seminar on Fermat's Last Theorem 1993-1994, Kumar Murty ed. Canadian Mathematical Society, CMS Conference Proceedings **17**, 1995, pages 135–153.

[4] De Shalit, E., *Hecke rings and universal deformation rings*, Chapter XIV in [CSS].

[5] De Smit, B., Rubin, K., Schoof, R. , *Criteria for Complete Intersections*, Chapter XI in [CSS].

[6] Diamond, F., *The refined conjecture of Serre*, in Elliptic Curves, Modular Forms and Fermat's Last Theorem, J. Coates, S. Yau, eds. International Press, Cambridge, 1995, pages 22–37.

[7] Diamond, F., Ribet, K., *ℓ-adic Modular Deformations and Wiles's "Main Conjecture"*, Chapter XII in [CSS].

[8] Edixhoven, S.J., *Serre's conjecture*, Chapter VII in [CSS].

[9] Gelbart, S., *Three lectures on the modularity of $\overline{\rho}_{E,3}$ and the Langlands reciprocity conjecture*, Chapter VI in [CSS].

[10] Mazur, B., *Deformation theory of Galois representations*, in Galois groups over $\mathbf{Q}$, Chapter VIII in [CSS].

[11] Rio, A., *Representacions de Galois octaèdriques*, Tesi Doctoral, Universitat de Barcelona (1995).

[12] Serre, J.-P., *Sur les représentations de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. Journal **54** (1987), 179–230.

[13] Serre, J.-P., *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[14] Stein, W.A., HECKE package, Magma V2.7 or higher, 2000.

[15] Taylor, R. and Wiles, A., *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141** (1995) 553–572.

[16] Tilouine, J., *Hecke algebras and the Gorenstein property*, Chapter X in [CSS].

[17] Wiles, A., *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Appendix by A. Agashe and W. Stein.

In this appendix, we apply a result of J. Sturm* to obtain a bound on the number of Hecke operators needed to generate the Hecke algebra as an abelian group. This bound was suggested to the authors of this appendix by Loïc Merel and Ken Ribet.

Theorem. *The ring* $\mathbf{T}$ *of Hecke operators acting on the space of cusp forms of weight* k *and level* N *is generated as an abelian group by the Hecke operators* T_n *with*

$$n \leq \frac{kN}{12} \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

Proof. For any ring R, let $S_k(N;R) = S_k(N;\mathbf{Z}) \otimes R$, where $S_k(N;\mathbf{Z})$ is the subgroup of cusp forms with integer Fourier expansion at the cusp ∞, and let $\mathbf{T}_R = \mathbf{T} \otimes_{\mathbf{Z}} R$. There is a perfect pairing $S_k(N;R) \otimes_R \mathbf{T}_R \to R$ given by $\langle f, T \rangle \mapsto a_1(T(f))$.

Let M be the submodule of $\mathbf{T}$ generated by $T_1, T_2, \ldots, T_r$, where r is the largest integer $\leq \frac{kN}{12} \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$. Consider the exact sequence of additive abelian groups

$$0 \to M \xrightarrow{i} \mathbf{T} \to \mathbf{T}/M \to 0.$$

Let p be a prime and use that tensor product is right exact to obtain an exact sequence

$$M \otimes \mathbf{F}_p \xrightarrow{\bar{i}} \mathbf{T} \otimes \mathbf{F}_p \to (\mathbf{T}/M) \otimes \mathbf{F}_p \to 0.$$

Suppose that $f \in S_k(N;\mathbf{F}_p)$ pairs to 0 with each of $T_1, \ldots, T_r$. Then $a_m(f) = a_1(T_m f) = \langle f, T_m \rangle = 0$ in $\mathbf{F}_p$ for each $m \leq r$. By Theorem 1 of Sturm's paper, it follows that $f = 0$. Thus the pairing restricted to the image of $M \otimes \mathbf{F}_p$ in $\mathbf{T} \otimes \mathbf{F}_p$ is nondegenerate, so

$$\dim_{\mathbf{F}_p} \bar{i}(M \otimes \mathbf{F}_p) = \dim_{\mathbf{F}_p} S_k(N, \mathbf{F}_p) = \dim_{\mathbf{F}_p} \mathbf{T} \otimes \mathbf{F}_p.$$

It follows that $(\mathbf{T}/M) \otimes \mathbf{F}_p = 0$; repeating the argument for all primes p shows that $\mathbf{T}/M = 0$, as claimed.

Remark. In general, the theorem is not true if one considers only T_n where n runs over the *primes* less than the bound. Consider, for example, $S_2(11)$, where the bound is 2 and T_2 is the 1×1 matrix [2], which does not generate the full Hecke algebra as a $\mathbf{Z}$-submodule of $\mathrm{End}(S_2(\Gamma_0(N), \mathbf{Z}))$. One needs, in addition, the matrix [1].

* J. Sturm, *On the Congruence of Modular Forms.* Number theory (New York, 1984–1985), 275–280, Lecture Notes in Math., 1240, Springer, Berlin-New York, 1987.