Honours Research Project: Modular forms and Galois representations mod p, and the nilpotent action of Hecke operators mod 2

Mathilde Gerbelli-Gauthier[*]

May 20, 2014

Abstract

We study Hecke operators acting on the space of modular forms mod 2, with a view towards the relation between modular forms and Galois representations. We first give background on modular forms and Galois representations mod p, and state the theorem of Khare-Wintenberger long known as Serre's conjecture. We then focus on the case $p = 2$, where the Hecke algebra acts nilpotently, and give an exposition of recent work of Nicolas and Serre. In their article [6], two proposition describing the action of the operators T_3 and T_5 respectively are left unproved. These propositions state that the action of the Hecke operator on a modular form of the form Δ^k depends on an invariant computed from the dyadic expansion of k. The final sections of this article give original proofs of these two results using recurrences suggested by the authors.

[*] Some of this research was conducted when the author was supported by an NSERC SURA scholarship.

Contents

1 Introduction **3**

2 Modular forms and Galois representations mod p **5**

2.1 Modular forms . . . 5

2.2 Hecke operators . . . 7

2.3 Modular forms mod p . . . 7

2.4 Galois representations mod p . . . 8

2.5 Frobenius elements . . . 9

2.6 Serre's conjecture . . . 10

3 Modular forms mod 2 **12**

3.1 The order of nilpotency of a modular form . . . 13

3.2 Nilpotency of Hecke operators: a new proof. . . . 14

3.3 Structure of the Hecke algebra . . . 15

4 The code of an integer **16**

4.1 Definitions . . . 16

4.2 Properties . . . 17

4.3 The code of a polynomial . . . 20

5 The action of T_3 **21**

5.1 The recurrences . . . 21

5.2 Proof of proposition 4.3 . . . 21

6 The action of T_5 **27**

6.1 More recurrences . . . 27

6.2 Proposition 4.4 and integers such that $n_3(\ell) = 0$ . . . 28

6.3 Proof of proposition 4.4 . . . 31

7 Possibilities or further research **39**

1 Introduction

The first part of this article is an introduction to modular forms and Galois representations mod p. First, modular forms in characteristics 0 and p are introduced, as well as Hecke operators and their eigenforms. We then introduce Galois representations mod p. We discuss Frobenius elements in Galois groups of extensions of $\mathbb{Q}$ and their images under representations

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\bar{\mathbb{F}}_p).$$

We conclude the section by giving the idea for the invariants (N, k, ε) attached to a representation, and stating Serre's conjecture on modular forms and Galois representations mod p.

The next part focuses on modular forms mod 2 and presents recent results of Nicolas and Serre, [6], [7]. In level 1, the ring of modular foms modulo 2 is the polynomial ring $\mathbb{F}_2[\Delta]$, where Δ is the reduction of the modular discriminant. The action of the Hecke operators on this ring is nilpotent, as there are no non-trivial systems of eigenvalues mod 2. In [6], the authors give a precise description of this action on the subspace $\mathcal{F}$ spanned by odd powers of Δ. They define the order of nilpotency of a modular form Δ^k as the minimal integer n such that for any collection of primes p_i,

$$T_{p_1}^{n_1} \cdot \ldots \cdot T_{p_i}^{n_i}(\Delta^k) = 0, \quad n = \sum n_i.$$

The upper bound on $n-1$ is achieved when applying only the operators T_3 and T_5. The multiplicities appearing in this maximal application are denoted $n_3(k)$ and $n_5(k)$. The authors find that this pair of integers, which they call the code of k, can be computed from the dyadic expansion of k, where the $\beta_i(k)$ is the coefficient of 2^i in this expansion. The code is given by

$$n_3(k) = \sum_{i=0}^{\infty} \beta_{2i+1}(k)2^i, \quad n_5(k) = \sum_{i=0}^{\infty} \beta_{2i+2}(k)2^i, \quad h(k) = n_3(k) + n_5(k).$$

The code defines a bijection between the positive odd integers and $\mathbb{N}^2$ and an associated total ordering of the odd integers. The order relation is denoted by $\prec$ and for two odd integers k, k', we write that $k \prec k'$ if $h(k) < h(k')$ or $h(k) = h(k')$ and $n_5(k) < n_5(k')$. Given a polynomial $f \in \mathcal{F}$, the highest exponent of f is the greatest in this ordering, and f inherits the code of this exponent. The precise descriptions of the action of T_3 and T_5 in are given in the following propositions.

Proposition 1 (Proposition 4.3 [6]). *Let $f \in \mathcal{F}$, $f \neq 0$, and let k be its highest exponent.*
(i) We have $h(T_3(f)) \leq h(f) - 1 = h(k) - 1$, where the second equality is by definition.
(ii) When $n_3(k) > 0$, we have $h(T_3(f)) = h(k) - 1$ and the code of the highest exponent of $T_3(f)$ is $[n_3(k) - 1, n_5(k)]$.

Proposition 2 (Proposition 4.4 [6]). *Let $f \in \mathcal{F}$, $f \neq 0$, and let k be its highest exponent.*
(i) We have $h(T_5(f)) \leq h(f) - 1 = h(k) - 1$.
(ii) When $n_5(k) > 0$, we have $h(T_5(f)) = h(k) - 1$ and the code of the highest exponent of $T_5(f)$ is $[n_3(k), n_5(k) - 1]$.

The proof of these propositions is said to be "long and technical" and is left unpublished. The authors do indicate that the proof is obtained by induction via linear recurrences which they developed:

$$T_3(\Delta^k) = \Delta T_3(\Delta^{k-3}) + \Delta^4 T_3(\Delta^{k-4}) \tag{1.1}$$

$$T_5(\Delta^k) = \Delta^2 T_5(\Delta^{k-2}) + \Delta^4 T_5(\Delta^{k-4}) + \Delta^6 T_5(\Delta^{k-6}) + \Delta T_5(\Delta^{k-5}). \tag{1.2}$$

In [7], the authors uncover structural properties of the algebra $\mathcal{F}$ using the results from [6]. They show that the algebra $\mathcal{A}$ of Hecke operators can be identified with dual $\mathcal{F}^*$. Furthermore, $\mathcal{A}$ is isomorphic to the ring $\mathbb{F}_2[[x, y]]$ where $x = T_3$ and $y = T_5$.

Sections 5-7 present original proofs of propositions 4.3 and 4.4. We first show that the recurrence relations (1.1) and (1.2) can be respectively composed with themselves to obtain similar recurrence relations involving arbitrarily large powers of 2:

$$T_3(\Delta^k) = \Delta^{2^i} T_3(\Delta^{k-3\cdot 2^i}) + \Delta^{4\cdot 2^i} T_3(\Delta^{k-4\cdot 2^i}), \tag{1.3}$$

$$T_5(\Delta^k) = \Delta^{2\cdot 2^i} T_5(\Delta^{k-2\cdot 2^i}) + \Delta^{4\cdot 2^i} T_5(\Delta^{k-4\cdot 2^i}) + \Delta^{6\cdot 2^i} T_5(\Delta^{k-6\cdot 2^i}) + \Delta^{2^i} T_5(\Delta^{k-5\cdot 2^i}). \tag{1.4}$$

These new recurrences can be used to circumvent the incompatibility of subtraction with the $\prec$ ordering of the odd integers. To illustrate this, we arrange the odd integers in a grid using $[n_3(k), n_5(k)]$ as coordinates for k. In terms of the grid, the statement of propositions 4.3 and 4.4 is that T_3 acts by translation to the left by one unit, and T_5 by downwards translation.

Δ^{85}	Δ^{87}	Δ^{93}	Δ^{95}	Δ^{117}	Δ^{119}	Δ^{125}	Δ^{127}		
Δ^{81}	Δ^{83}	Δ^{89}	Δ^{91}	Δ^{113}	Δ^{115}	Δ^{121}	Δ^{123}		
Δ^{69}	Δ^{71}	Δ^{77}	Δ^{79}	Δ^{101}	Δ^{103}	Δ^{109}	Δ^{111}		
Δ^{65}	Δ^{67}	Δ^{73}	Δ^{75}	Δ^{97}	Δ^{99}	Δ^{105}	Δ^{107}		
Δ^{21}	Δ^{23}	Δ^{29}	Δ^{31}	Δ^{53}	Δ^{55}	Δ^{61}	Δ^{63}		
Δ^{17}	Δ^{19}	Δ^{25}	Δ^{27}	Δ^{49}	Δ^{51}	Δ^{57}	Δ^{59}		
Δ^{5}	Δ^{7}	Δ^{13}	Δ^{15}	Δ^{37}	Δ^{39}	Δ^{45}	Δ^{47}	Δ^{133}	Δ^{135}
Δ	Δ^{3}	Δ^{9}	Δ^{11}	Δ^{33}	Δ^{35}	Δ^{41}	Δ^{43}	Δ^{129}	$\Delta^{131}\ldots$

A look at this table shows that the code does not behave well under arithmetic operations in general, but it does under subtraction of single powers of 2. For example, the square containing odd integers in the range $(33, 63)$ is a right translate by 4 units of the square containing the integers $(1, 31)$. This translation corresponds to adding 32 and the ordering inside the square is preserved.

This is the strategy for the proof of proposition 4.3: the recurrences allow us induct on numbers that have exactly the same binary expansion, up to the greatest power of 2. Visually, we could say that we induct on the left-translate of a box of size $4 \cdot 2^i$ ($4 \cdot 2^3$ in the example above). In this case, since the image under T_3 of Δ^k is the translate of the image under T_3 of $\Delta^{k-4\cdot 2^i}$, we like to think of subtraction (translation) and applying T_3 as two operation that commute. This operation of left-translation corresponds to the $\Delta^{4\cdot 2^i} T_3(\Delta^{k-4\cdot 2^i})$ term of the recurrence, and we bound the highest exponent first term to get our result.

For proposition 4.4, which describes the action of T_5, the recurrence has more terms, which can cancel each other in various ways. This lead to a multiplication of the number of subcases to consider if one wishes to replicate the proof used for T_3. In some cases, this technique appears to simply not work, since the cancellation leaves the second exponent in one of the four terms as the leading exponent. As proposition 4.4 says nothing about lower order exponents, this appears to be a dead end and we adopt a different technique. It is based on the idea that the operator T_3 is almost invertible despite being nilpotent. Indeed, if one considers a polynomial $f \in \mathcal{F}$ with leading term Δ^j, the question "what would be the leading exponent of a polynomial g such that $T_3(g) = f$?" has a very limited number of possible answers. If the leading exponent of g is an integer ℓ such that $n_3(\ell) \neq 0$, then it is almost certain that $\ell \simeq [n_3(j) + 1, n_5(j)]$. The only other possibility is that the $n_3(\ell) = 0$, in which case proposition 4.3 only tells us that $h(\ell) \geq h(j)$.

We use this observations and the commutativity of Hecke operators to regard T_5 as $T_3^{-1} T_5 T_3$. Concretely, given a monomial Δ^k, we first apply T_3 to get a new $f \in \mathcal{F}$ whose degrees are smaller than k. We then use induction to determine the leading exponent of $T_5(f) = T_5 T_3(\Delta^k)$. We then ask the question "what could be the preimage under T_3 of $T_5 T_3(\Delta^k)$?" In well-behaved cases, the answer is the integer ℓ such that $n_3(\ell) = n_3(T_5 T_3(\Delta^k)) + 1$. There are a limited number of k such that the second possibility arises: $n_3(\ell) = 0$ and $\ell < k$. However, there are strict restrictions on the dyadic expansion of an integer k for which this could occur. We take of these special cases by using the recurrence formula to explicitly compute $T_5(\Delta^k)$ in the same way as for T_3.

Acknowledgements. The author is grateful for the patience, excellent advice and constant support provided throughout this project by her research supervisor Henri Darmon. Her gratitude goes to Jean-Louis Nicolas and Jean-Pierre Serre for their attention and for providing their version of the proofs. She is also thankful to Paul Monsky for important suggestions in the presentation of the proof. Finally, she would like to thank Olivier Martin for his inestimable friendship, the quality of their mathematical exchanges, and for being a constant source of inspiration.

2 Modular forms and Galois representations mod p

This section introduces modular forms mod p and Galois representations mod p. It gives the definition of the invariants (N, k, ε) for both objects, and ends with the statement of Serre's modularity conjecture. References for this section are Serre's article stating the conjectures [10], as well as [9] and [4] for modular forms, and [12] for Galois representations.

2.1 Modular forms

Let $\mathbb{H}$ be the complex upper half-plane. The group $PSL_2(\mathbb{Z})$ acts isometrically on $\mathbb{H}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}, \quad a, b, c, d \in \mathbb{Z}, ad - bc = 1, z \in \mathbb{H}.$$

Definition 1. *Let N ba a positive integer. The congruence subgroup $\Gamma_0(N)$ of $PSL_2(\mathbb{Z})$ is*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in PSL_2(\mathbb{Z}) \; ; \; c \equiv 0 \mod N \right\}.$$

Modular forms are complex-valued functions on $\mathbb{H}$ satisfying a certain functional equation with respect to the action of a congruence subgroup.

Definition 2. *Let k and N be positive integers, and $\varepsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$ be a character. A modular form of level N, weight k and character ε is a holomorphic function*

$$f : \mathbb{H} \to \mathbb{C}$$

such that

(i) for any $\gamma \in \Gamma_0(N)$, the function f satisfies the equation

$$f(\gamma \cdot z) = \varepsilon_0(d)(cz+d)^k f(z), \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

(ii) the function f is holomorphic at ∞, i.e. the value of $f(z)$ is bounded as $im(z) \to \infty$.

Considering the definition in the case of the element

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$$

shows that $f(z) = f(z+1)$. Thus every modular form is periodic and has a Fourier series expansion of the form

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i z}.$$

Definition 3. *A modular form f is called a cusp form if $a_0(f) = 0$.*

Example Classical examples in level 1 and with trivial character are the Eisenstein series E_{2k} for $k \geq 2$:

$$E_{2k} = 1 + \frac{(-1)^k 4k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \qquad \sigma_k(n) = \sum_{d|n} d^k$$

where B_k is the k^{th} Bernouilli number, see [9]. In particular, we have

$$E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n, \qquad E_6 = 1 - 506 \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{2.1}$$

For level 1, the cusp form of smallest weight is the Δ function. It has weight 12 and the following q-series expansion

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

Modular forms of each weight, level and character from a vector space denoted $M(N, k, \varepsilon_0)$. Likewise $S(N, k, \varepsilon_0)$ denotes the subspace of cusp forms. Both these vector spaces are finite dimensional and have a basis f_i such that $a_n(f_i) \in \mathbb{Z}[\varepsilon]$ for all n. For a given level, modular forms of all weights and characters form a graded ring. For a detailed treatment of this, see [4], chapter 3.

Example For level 1 and trivial character, the ring of modular forms is isomorphic to the polynomial ring $\mathbb{C}[x, y]$ where $x = E_4$ and $y = E_6$. Moreover, all modular forms with integer coefficients can be obtained as elements of the polynomial ring $\mathbb{Z}[E_4, E_6, \Delta]$.

2.2 Hecke operators

For a prime ℓ, the Hecke operator T_ℓ acts on the ring of modular forms of all weights in the following way:

$$T_\ell \left(\sum_{n=1}^{\infty} a_n(f) q^n \right) = \sum_{n=1}^{\infty} a_{\ell n}(f) q^n + \varepsilon(\ell) \ell^{k-1} a_n q^{\ell n}.$$

If f is a modular form (resp. a cusp form) of weight k, then so is $T_\ell(f)$. Furthermore, Hecke operators commute with each other.

The space $S(N, k, \varepsilon)$ can be equipped with the *Petersson inner product*, defined roughly as an integral over the fundamental domain for the action of $\Gamma_0(N)$. The Hecke operators are self-adjoint with respect to this inner product.[1] Hence they are diagonalizable, and the space $S(N, k, \varepsilon_0)$ has a basis of elements that are simultaneous eigenvectors for all the T_ℓ. If such an eigenform f is normalized so that $a_1(f) = 1$, then for all primes ℓ, $a_\ell(f)$ is the eigenvalue of T_ℓ attached to f. All these eigenvalues are algebraic integers, and the field $K = \mathbb{Q}(a_n(f))$ generated by these eigenvalues is a number field. Again, this is covered in detail in [4], chapter 5.

2.3 Modular forms mod p

We use Serre's definition of modular forms mod p from his Duke article [10]. Fix a prime p, let $\bar{\mathbb{Q}}$ be the algebraic closure of the rationals and $\bar{\mathbb{Q}}_p$ the algebraic closure of the p-adics. There are many possible $\mathbb{Q}$-embeddings of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_p$, and the choice of one of these corresponds to the choice of a place above p in $\bar{\mathbb{Q}}$. The choice of such a place determines a specific maximal ideal of $\bar{\mathbb{Z}}_p$, and the quotient by this ideal is a morphism $\bar{\mathbb{Z}}_p \to \bar{\mathbb{F}}_p$. Following Serre, we denote this map $z \to \tilde{z}$. Given a character

$$\varepsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \bar{\mathbb{Z}}$$

[1] true

one can define a character ε with values in $\bar{\mathbb{F}}_p$ as the composition with the above map. Conversely, given a character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \bar{\mathbb{F}}_p$, there is a unique lift to a character ε_0 which takes its values in the roots of unity of $\bar{\mathbb{Z}}$.

Definition 4. *Let*

$$\tilde{f} = \sum_{n=1}^{\infty} a_n(\tilde{f}) q^n$$

be a formal power series in $\bar{\mathbb{F}}_p[[q]]$. The function $\tilde{f}$ is said to be a modular form modulo p of weight k, level N, and character ε if there exists a cusp form f of level N, weight k and character ε_0 with $a_n(f) \in \bar{\mathbb{Z}}$ and such that

$$a_n(\tilde{f}) = \tilde{a}_n(f).$$

Let $S(N, k, \varepsilon)$ be the space of such modular forms. This space is independent of the choice of a place above p in $\bar{\mathbb{Q}}$, and its dimension is equal to the dimension of the corresponding $\mathbb{C}$-vector space $S(N, k, \varepsilon_0)$. The action of the Hecke operators descends to $S(N, k, \varepsilon)$:

$$T_\ell \left(\sum_{n=1}^{\infty} a_n(\tilde{f}) \right) = \sum_{n=1}^{\infty} a_{\ell n}(\tilde{f}) q^n + \varepsilon(\ell) \ell^{k-1} a_n(\tilde{f}) q^{\ell n} \qquad \ell \nmid pN$$

$$U_\ell \left(\sum_{n=1}^{\infty} a_n(\tilde{f}) \right) = \sum_{n=1}^{\infty} a_{\ell n}(\tilde{f}) q^n \qquad \ell \mid pN.$$

This action preserves $S(N, k, \varepsilon)$. If $\tilde{f}$ is a simultaneous eigenform for all Hecke operators, then it is the reduction mod p of an eigenform f in characteristic 0. However, this eigenform f might not be unique.

Example Consider the algebra of modular forms of level 1, and let $p = 2$. In this case, (2.1) implies that

$$E_4 = E_6 = 1 \mod 2$$

so that $\mathbb{Z}[E_4, E_6, \Delta]$ reduces to $\mathbb{F}_2[\tilde{\Delta}]$. The coefficient $a_n(\Delta)$ is equal to 1 mod 2 precisely when $n = (2m+1)^2$ for $m \geq 0$, so $\tilde{\Delta} = \sum_{m=1}^{\infty} q^{2m+1}$.

2.4 Galois representations mod p

One of the main reasons why modular forms have been studied is their connection with Galois representations, and we now define these. There are theories of p-adic and complex Galois representations, but we restrict our attention to Galois representations mod p. Let $G_{\mathbb{Q}}$ be the absolute Galois group of $\mathbb{Q}$, $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Definition 5. *A two-dimensional Galois representation is a homomorphism*

$$\rho : G_{\mathbb{Q}} \to GL(V)$$

for some two-dimensional vector space V. It is irreducible if there is no non-trivial stable $\rho(G_{\mathbb{Q}})$ subspace.

Here we will be concerned with Galois representations modulo p so we will always have

$$GL(V) \simeq GL_2(\bar{\mathbb{F}}_p)$$

where $\bar{\mathbb{F}}_p$ is the algebraic closure of the field with p elements. The group $G_{\mathbb{Q}}$ is profinite and equipped with the corresponding topology, and $GL_2(\bar{\mathbb{F}}_p)$ is a discrete topological space. The representations ρ which we consider are continuous, which implies that they have finite image. Hence the matrices in the image of ρ take entries in a finite extension $\mathbb{F}_q/\mathbb{F}_p$.

2.5 Frobenius elements

We recall the algebraic number theory needed to define conjugacy classes of Frobenius elements. Since we are concerned with Galois representations with finite image, we only consider Frobenius elements of the Galois group of extensions of $\mathbb{Q}$ of finite degree. We follow Wiese's notes [12] on Galois representations.

Let $K/\mathbb{Q}$ be a Galois extension, $\mathcal{O}_K$ its ring of integers. Any rational prime p has a factorization into ideals of $\mathcal{O}_K$:

$$p = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_n^{e_n}.$$

The group $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on this set of ideals, which implies that all the exponents e_i are equal.

Definition 6. *The extension K is said to be ramified at p if the e_i are greater than 1. Otherwise, it is said to be unramified.*

Fix an ideal $\mathfrak{p}$ in the factorization; it is said to lie above p. This ideal induces a valuation $v_\mathfrak{p}$ and a norm $|\cdot|_\mathfrak{p}$ on K. The field K can be completed with respect to this norm to get an extension $K_\mathfrak{p}/\mathbb{Q}_p$ of finite degree. This field $K_\mathfrak{p}$ has a discrete valuation ring

$$\mathcal{O}_{K_\mathfrak{p}} = \{x \subset K;\ |x|_\mathfrak{p} \leq 1\}.$$

The ring $\mathcal{O}_{K_\mathfrak{p}}$ is local with maximal ideal

$$\mathfrak{p} = \{x \in K;\ |x|_\mathfrak{p} < 1\}.$$

We use the same notation for the ideal $\mathfrak{p} \in K$ and $\mathfrak{p} \subset K_\mathfrak{p}$; one is the completion of the other. Let $\mathbb{F}(\mathfrak{p})$ be the residue field of K with respect to $\mathfrak{p}$; it is isomorphic to $\mathbb{F}_q$ for some $q = p^n$. The field $\mathbb{F}(\mathfrak{p})$ can be viewed as the quotient $\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K$ or equivalently as $\mathcal{O}_{K_\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{K_\mathfrak{p}}$.

Definition 7. *The subgroup*

$$D_\mathfrak{p} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\} \subset \mathrm{Gal}(K/\mathbb{Q})$$

is called the decomposition subgroup at $\mathfrak{p}$.

Since $D_\mathfrak{p}$ fixes $\mathfrak{p}$, it preserves the completion with respect to the induced norm, and so it is isomorphic to $\mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p)$. Moreover, since it fixes the maximal ideal $\mathfrak{p} \subset K_\mathfrak{p}$, it acts on the quotient $\mathbb{F}(\mathfrak{p})$. This induces a natural surjective mapping

$$\pi(\mathfrak{p}/p) : \mathrm{Gal}(K_\mathfrak{p}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}(\mathfrak{p})/\mathbb{F}_p)$$

which fits into a short exact sequence

$$0 \to I(K_{\mathfrak{p}}/\mathbb{Q}_p) \to \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p) \xrightarrow{\pi(\mathfrak{p}/p)} \mathrm{Gal}(\mathbb{F}(\mathfrak{p})/\mathbb{F}_p) \to 0.$$

Definition 8. *The group $I(K_{\mathfrak{p}}/\mathbb{Q}_p)$ is called the inertia group of $\mathfrak{p}$.*

The extension K is unramified at p if and only if the inertia group is trivial, i.e. if $D_{\mathfrak{p}} \simeq \mathrm{Gal}(\mathbb{F}(\mathfrak{p})/\mathbb{F}_p)$. The group $\mathrm{Gal}(\mathbb{F}(\mathfrak{p})/\mathbb{F}_p)$ is generated by the Frobenius map which takes x to x^p. If K is unramified at p, this is used to define the Frobenius in $\mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$.

Definition 9. *If $\mathfrak{p}$ is unramified,* $\mathrm{Frob}(\mathfrak{p}/p) \in \mathrm{Gal}(K_{\mathfrak{p}}/\mathbb{Q}_p)$ *is the the preimage of the Frobenius under $\pi(\mathfrak{p}/p)$.*

As an element of $\mathrm{Gal}(K/\mathbb{Q})$, the Frobenius depends on to the choice of an ideal above p. However, since all these ideals are conjugate under the action of $\mathrm{Gal}(K/\mathbb{Q})$, their decomposition groups are also conjugate and for two primes $\mathfrak{p}$ and $\mathfrak{p}' = \sigma(\mathfrak{p})$,

$$\mathrm{Frob}(\mathfrak{p}/p) = \sigma \, \mathrm{Frob}(\mathfrak{p}'/p)\sigma^{-1}.$$

It follows that the Frobenius at p is a well-defined conjugacy class of elements in $\mathrm{Gal}(K/\mathbb{Q})$. The following theorem states that Frobenius elements for all p are evenly distributed among conjugacy classes of $\mathrm{Gal}(K/\mathbb{Q})$.

Theorem 1 (Chebotarev's Density Theorem)**.** *Let K be a Galois extension of $\mathbb{Q}$. Let $\sigma \in Gal(K/\mathbb{Q})$ and denote its conjugacy class by $[\sigma]$. For an ideal $\mathfrak{p} \subset K$, let $N(\mathfrak{p})$ be the cardinality of the residue field $\mathbb{F}(\mathfrak{p})$. Then*

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} | [\mathrm{Frob}(\mathfrak{p}/p)] = [\sigma],\, N(\mathfrak{p}) < x\}}{\#\{\mathfrak{p} | N(\mathfrak{p}) < x\}} = \frac{\#[\sigma]}{\# Gal(K/\mathbb{Q})}.$$

Any Galois representation ρ with finite image factors through $\mathrm{Gal}(K/\mathbb{Q})$ for some Galois extension K. The representation ρ is said to be unramified ℓ if K is unramified at ℓ. A representation can only be ramified at finitely many primes. If ρ is unramified at ℓ, one can talk about the image of $\mathrm{Frob}(\ell)$ under ρ, but only up to conjugacy. As a consequence of Chebotarev's density theorem, the images of these Frobenius elements constitute the entire image of ρ and thus completely determine it. Furthermore, the minimal polynomial and in particular the trace of a matrix are defined on an entire conjugacy class. Consequently, for each ℓ, $\mathrm{tr}\rho(\mathrm{Frob}(\ell))$ is well-defined.

2.6 Serre's conjecture

Serre's conjecture relates the two objects introduced above; it states that any odd irreducible Galois representation mod p corresponds to a modular form mod p which is an eigenvector for the Hecke operators. More precisely, let ρ be an irreducible Galois representation

$$\rho : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p).$$

Serre attaches three invariants (N, k, ε) to this representation; these should correspond to the level, trace and character of the associated modular form. See [10] or [12] for a more detailed treatment.

- The integer N is the Artin conductor of ρ. The representation ρ is ramified at a finite number of primes $\ell \neq p$, and N is a weighted product of these. It is a measure of the ramification of ρ away from p.

- The integer k is a measure of the ramification of ρ at p. Its value depends on the value of ρ on the inertia group at p.

- Taking the determinant of ρ, one obtains a morphism

  $$\det \rho : G_{\mathbb{Q}} \to \bar{\mathbb{F}}_p^{\times}$$

  that factors through $(\mathbb{Z}/pN\mathbb{Z})^{\times}$. Since $p \nmid N$, this can be split in two morphisms. The first factor

  $$\varepsilon : (\mathbb{Z}/N\mathbb{Z})^{\times} \to \bar{\mathbb{F}}_p^{\times}$$

  is the character used in the conjecture. The second factor is a morphism

  $$\varphi : \mathbb{Z}/p\mathbb{Z} \to \bar{\mathbb{F}}_p.$$

  Since $(\mathbb{Z}/p\mathbb{Z})^{\times}$ is cyclic, it is in fact a cyclotomic character taking $x \mapsto x^n$ with $n \in \mathbb{Z}/p-1\mathbb{Z}$. This exponent n will be the residue class mod $p-1$ of the integer k.

Finally, for the definition of odd, note that each possible an embedding of $\bar{\mathbb{Q}}$ into $\mathbb{C}$ determines an element $c \in G_{\mathbb{Q}}$ that acts as complex conjugation. The representation ρ is said to be odd if $\det \rho(c) = -1$ for one, and hence all possible choices of c.

Before Serre's conjecture, one direction of the correspondence between modular forms and Galois representations mod p was known. Results of Eichler and Shimura for weight 2, and Deligne for larger weights, state that for each eigenform of the Hecke operators mod p there is an associated Galois representation mod p. This representation is unramified outside of pN, and for every prime $\ell \nmid pN$, the eigenvalue of T_ℓ is equal to the trace of the image of $\mathrm{Frob}(\ell)$.

Serre's conjecture goes in the opposite direction: it states that every odd irreducible Galois representation of type (N, k, ε) has an associated modular form of the same type, where the invariants have the appropriate interpretation. This statement is now a theorem: it was proved for level 1 by Khare in 2005, and for all levels by Khare and Wintenberger in 2008.

Theorem 2 (Khare-Wintenberger). *Let*

$$\rho : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_p)$$

be an odd irreducible Galois representation. Let the integers N, k and the character ε be as above. Then there exists $\tilde{f}$, a modular form mod p of level N, weight k and character ε with the property that for all primes ℓ at which ρ is unramified,

$$a_\ell(\tilde{f}) = \operatorname{tr} \rho(\mathrm{Frob}(\ell)).$$

3 Modular forms mod 2

From now on, we will focus on the ring of modular forms of all weights modulo 2, of level $N = 1$ and trivial character. Recall that this ring is isomorphic to $\mathbb{F}_2[\Delta]$ where Δ is the reduction mod 2 of the modular discriminant, with q-expansion

$$\Delta = \sum_{m=1}^{\infty} q^{(2m+1)^2} \in \mathbb{F}_2[[q]].$$

Here the discussion of the previous section is applicable, with $(N, k, \varepsilon) = (1, k, \chi_0)$, where χ_0 is the trivial character. Serre's conjecture then states that any irreducible odd two-dimensional Galois representation

$$\rho : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_2)$$

which is unramified away from 2 should correspond to a Hecke eigenform in $\mathbb{F}_2[\Delta]$. The ramification can only occur at 2 since $N = 1$.

However, for this particular ring, there is no irreducible two-dimensional Galois representation, and the only Hecke eigenform is the 0 function. The absence of Galois representations was first demonstrated by Tate [11] using bounds on the discriminant of Galois extensions of $\mathbb{Q}$ unramified outside of 2. For modular forms, Hatada [5] proved that the eigenvalues of Hecke operators are all divisible by 2, showing that the Hecke operators act nilpotently on the ring of modular forms mod 2. These two results predate the announcement of Serre's conjecture but likely served as evidence.

The absence of Galois representations and nilpotency of Hecke operators are now equivalent results. To go from representations to forms, note that the trace of the identity matrix in $GL_2(\bar{\mathbb{F}}_2)$ is 0. So if the only admissible Galois representation is the trivial one, and if, by Deligne's result, each Hecke eigenform corresponds to a representation, then the only possible eigenform is the 0 function.

In the other direction, assume that the Hecke operators act nilpotently, and suppose that there exists an irreducible two-dimensional Galois representation

$$\rho : G_{\mathbb{Q}} \to GL_2(\bar{\mathbb{F}}_2)$$

of type $(1, k, \chi_0)$. Then by Serre's conjecture, the images under ρ of Frobenius elements all have trace 0. Chebotarev's density theorem then implies that all elements of the image have trace 0. Moreover, since $N = 1$, the determinant of ρ is a character of $(\mathbb{Z}/2\mathbb{Z})^\times$ and therefore trivial. It follows that the characteristic polynomial of all the matrices in the image of ρ is x^2+1. This implies in particular that all elements of the image have order 2. Thus the image of ρ is an abelian subgroup of $GL_2(\bar{\mathbb{F}}_2)$ so its elements stabilize a non-trivial $\bar{\mathbb{F}}_2$-subspace. This contradicts the fact that ρ is irreducible.

The action of the Hecke operators, despite being nilpotent, has interesting structural properties which were studied by Nicolas and Serre in [6] and [7]. The following will be an overview of their results, with section 3.2 presenting a new proof due to Nicolas and Serre that the Hecke operators are nilpotent mod 2. Finally, sections 5-7 contain alternate proofs of two central propositions of [6].

3.1 The order of nilpotency of a modular form

As we have seen in the above examples, the Eisenstein series E_4 and E_6 reduce modulo 2 to their constant term 1. Thus the reduction modulo 2 of the graded algebra of modular forms is a polynomial ring in one variable:

$$\mathbb{F}_2[\Delta], \quad \Delta = \sum_{m=1}^{\infty} q^{(2m+1)^2} \in \mathbb{F}_2[[q]].$$

Note that the coefficient of q^n is 0 whenever n is not congruent to 1 mod 8. Following Nicolas and Serre's notation, we let

$$\Delta^k = \sum_{n=1}^{\infty} \tau_k(n) q^n$$

so that

$$\tau_k(n) \neq 0 \Rightarrow n \equiv k \mod 8. \tag{3.1}$$

In [6], "L'ordre de nilpotence des opérateurs de Hecke", the authors wish to describe precisely the action of the Hecke operators acting on $\mathbb{F}_2[\Delta]$. They first observe that in characteristic 2,

$$\tau_{2k}(n) = \tau_k(2n).$$

Recall that the action of the Hecke operators T_p for odd p on modular forms mod 2 is

$$T_p\left(\sum_{n=1}^{\infty} a_n q^n\right) = \sum_{n=1}^{\infty} a_{pn} q^n + a_n q^{pn}.$$

Since we are working in characteristic 2, this implies that

$$T_p(\Delta^{2k}) = \Big(T_p(\Delta^k)\Big)^2.$$

The authors thus restrict their attention to the space $\mathcal{F} \subset \mathbb{F}_2[\Delta]$ spanned by the odd powers of Δ. This space can be divided in

$$\mathcal{F} = \mathcal{F}_1 \oplus \mathcal{F}_3 \oplus \mathcal{F}_5 \oplus \mathcal{F}_7$$

where $\Delta^k \in \mathcal{F}_n$ if $k \equiv n$ mod 8. In particular, this implies by 3.1 that if $\Delta^k \in \mathcal{F}_n$, then $\tau_k(m) \neq 0$ only if $m \equiv n \mod 8$. Furthermore, by 3.1 the coefficient of q^n in $T_p(\Delta^k)$ is non-zero only if $n \equiv pk \mod 8$. In short,

$$T_p(\mathcal{F}_n) = \mathcal{F}_{pn \bmod 8}.$$

Nicolas and Serre then find that the image of $T_p(\Delta^k)$ can be determined by recursion on k. For each p, there exists a symmetric polynomial

$$F_p(X,Y) = Y^{p+1} + s_1(X)Y^p + ... + s_p(X)Y + s_{p+1}(X)$$

such that for any $k > p+1$,

$$T_p(\Delta^k) = \sum_{i=1}^{p+1} s_i(\Delta)T_p(\Delta^{k-i}).$$

In the particular cases of $p = 3, 5$, the formulas are

$$T_3(\Delta^k) = \Delta T_3(\Delta^{k-3}) + \Delta^4 T_3(\Delta^{k-4}) \tag{3.2}$$
$$T_5(\Delta^k) = \Delta T_5(\Delta^{k-5}) + \Delta^2 T_5(\Delta^{k-2}) + \Delta^4 T_4(\Delta^{k-4}) + T_6(\Delta^{k-6}). \tag{3.3}$$

Nicolas and Serre use these to describe the action of T_3 and T_5 on the space $\mathcal{F}$. For each integer k, the action of these operators on Δ^k is encoded in a pair of integers $[n_3(k), n_5(k)]$ called the code of k. The code has the property that

$$T_5^{n_5(k)} T_3^{n_3(k)}(\Delta^k) = \Delta, \quad k \in \mathbb{Z}_{\text{odd}}.$$

In particular, the only $f \in \mathcal{F}$ such that $T_3(f) = T_5(f) = 0$ is $f = \Delta$. These facts rely on a pair of propositions, the proof of which is the subject of sections 5-7 of this article. Furthermore, Nicolas and Serre show that the integers $n_3(k)$ and $n_5(k)$ are minimal in the sense that for any collection of primes $p_1, ..., p_r$,

$$T_{p_1}^{n_1} ... T_{p_r}^{n_r}(\Delta^k) = 0 \quad \text{if} \quad \sum_{i=1}^{r} n_i \geq n_3(k) + n_5(k) + 1.$$

Nicolas and Serre call the integer $n_3(k) + n_5(k) + 1$ the order of nilpotency of Δ^k.

3.2 Nilpotency of Hecke operators: a new proof.

In [8], which is an expanded note detailing the results of [6], Nicolas and Serre give a new proof of the nilpotency of Hecke operators, using the results about T_3 and T_5. We present their argument.

Theorem 3. *Let T_p be a Hecke operator with $p \neq 2$. Then*

$$T_p(\Delta^k) = \sum_{i<k} a_i \Delta^i, \qquad a_i \in \mathbb{F}_2.$$

Proof. The function Δ^k is the reduction modulo 2 of a modular form of weight $12k$, and the same is true of $T_p(\Delta^k)$. Hence the degree of $T_p(\Delta^k)$ is bounded above by k. From the previous section, we know that $T_p(\Delta^k) \in \mathcal{F}_{pk}$, which implies that in fact

$$T_p(\Delta^k) = \sum_{\substack{i \le k \\ i \equiv pk \mod 8}} a_i \Delta^i.$$

If $p \equiv 3, 5, 7 \mod 8$, this directly implies that the degree of $T_p(\Delta^k)$ is strictly smaller than k.

Now suppose that $p \equiv 1 \mod 8$. If $T_p(\Delta) = \Delta$, then $\tau_1(p) = 1$, which contradicts the fact that $\tau_1(n) \neq 0$ only for odd squares. Now suppose for contradiction that there exists k such that $T_p(\Delta^k)$ is a polynomial of degree k, and let k_0 be the smallest such k. By the above, $k_0 \neq 1$. By the minimality of k_0, we have that for any $j < k_0$,

$$T_p(\Delta^j) = \sum_{i<j} a_i \Delta^i, \qquad a_i \in \mathbb{F}_2.$$

Since $k_0 \neq 1$, then the code of k_0 is not $[0, 0]$. It follows that there is T_ℓ, with $\ell \in \{3, 5\}$ such that $T_\ell(\Delta^{k_0}) \neq 0$. Consider

$$(T_p)^{k_0+1} T_\ell(\Delta^{k_0}) = T_\ell (T_p)^{k_0+1}(\Delta^{k_0}).$$

On one hand, by either proposition 4.3 or 4.4 (cf. sections 5-7 of this article),

$$T_\ell(\Delta^{k_0}) = \sum_{i \le k_0 - 2} a_i \Delta^i \quad \Rightarrow \quad (T_p)^{k_0+1} T_\ell(\Delta^{k_0}) = 0.$$

However, since the largest exponent of $T_p(\Delta^{k_0})$ is k_0, it is also the largest exponent of $(T_p)^{k_0+1}(\Delta^{k_0})$, which implies by the choice of T_ℓ that

$$T_\ell (T_p)^{k_0+1}(\Delta^{k_0}) = T_\ell \left(\Delta^{k_0} + \sum_{i<k_0} a_i \Delta^i \right) \neq 0.$$

This is a contradiction, so T_p is nilpotent. □

3.3 Structure of the Hecke algebra

In the sequel [7], Nicolas and Serre use the results about the action of T_3 and T_5 to determine the structure of the Hecke algebra $\mathbb{T}$ acting on $\mathcal{F}$. For each n, let $\mathcal{F}(n)$ be the space spanned $\Delta, \Delta^3, ..., \Delta^{2n+1}$. Let $\mathcal{A}(n)$ be the subalgebra of $\mathrm{End}(\mathcal{F}(n))$ generated by the T_p. Let e be the element of the dual $\mathcal{A}(n)^*$ that maps a polynomial $f(\Delta)$ to the coefficient of q in its Fourier expansion. The authors show $\mathcal{F}(n)$ can be identified with $\mathcal{A}(n)^*$ by way of the map

$$T_p \to e \circ T_p.$$

Furthermore, they show that there is a surjective morphism

$$\psi : \mathbb{F}_2[x, y] \to \mathcal{A}(n), \qquad \psi(x) = T_3, \quad \psi(y) = T_5.$$

The maps $\mathcal{A}(n) \to \mathcal{A}(n-1)$ given by restriction of the action make the $\mathcal{A}(n)$ into a projective system; its inverse limit is the algebra $\mathcal{A}$ of Hecke operators acting of $\mathcal{F}$. In the limit, the morphism ψ becomes injective, since given a polynomial $p(x,y)$, there is a k such that the order of nilpotency of Δ^k is larger than the degree of $p(x,y)$. It follows that $\mathcal{A}$ is isomorphic to $\mathbb{F}_2[[x,y]]$. Thus for any p,

$$T_p = \psi(f), \quad f = \sum_{i,j=1^\infty} a_{i,j}(p)x^i y^j.$$

The values of $a_{i,j}(p)$ have been computed by Nicolas up to fairly large values of p. They can be obtained by calculating the value of $T_p(\Delta^{[i,j]})$. According to the authors, the assignment $p \to a_{ij}(p)$ is *Frobenian.* It only depends on the value of the Frobenius at p in a certain Galois extension of $\mathbb{Q}$ unramified outside of 2 and whose Galois group is a 2-group. This led Serre to ask whether or not this could be used to construct an irreducible representation of $G_\mathbb{Q}$ in $GL_2(\mathcal{A})$ with the property that the traces of Frobenius elements at p would be the T_p. In [1], Bellaiche constructs this representation.

4 The code of an integer

We now give proofs of propositions 4.3 and 4.4 from “L'ordre de nilpotence” [6]. We begin by introducing Nicolas and Serre's definition of the code of an integer.

4.1 Definitions

Let k be an integer, and let

$$k = \sum_{i=0}^{\infty} \beta_i(k)2^i, \quad \beta_i(k) \in \{0,1\}$$

be the dyadic expansion of k, where the $\beta_i(k)$ are of course all 0 for i large enough.

Definition 10. *[6] The* support *of k, denoted $\mathcal{S}(k)$, is the set of 2^i such that $\beta_i(k) = 1$.*

Definition 11. *[6]*

(i) The code of k is the pair of integers $[n_3(k), n_5(k)]$ defined as follows:

$$n_3(k) = \sum_{i=0}^{\infty} \beta_{2i+1}(k)2^i = \sum_{\substack{i=1 \\ i \text{ odd}}}^{\infty} \beta_i(k)2^{\frac{i-1}{2}} \tag{4.1}$$

$$n_5(k) = \sum_{i=0}^{\infty} \beta_{2i+2}(k)2^i = \sum_{\substack{i=2 \\ i \text{ even}}}^{\infty} \beta_i(k)2^{\frac{i-2}{2}}. \tag{4.2}$$

Following [6] we will denote this by $k \simeq [n_3(k), n_5(k)]$.

(ii) The height of k is the integer $h(k) = n_3(k) + n_5(k)$.

Remark

- If $\mathcal{S}(k)$ only contains odd powers of 2, $n_3(k) = h(k)$. Likewise if $\mathcal{S}(k)$ only contains even powers of 2, $n_5(k) = h(k)$.
- If k is odd, $[n_3(k), n_5(k)] = [n_3(k+1), n_5(k+1)]$.
- The map $k \mapsto [n_3(k), n_5(k)]$ is a bijection between the odd positive integers and $\mathbb{N} \times \mathbb{N}$. In Figure 1, this bijection is illustrated and the odd powers of Δ are arranged in a grid where the coordinates of Δ^k are $[n_3(k), n_5(k)]$.

Δ^{85}	Δ^{87}	Δ^{93}	Δ^{95}	Δ^{117}	Δ^{119}	Δ^{125}	Δ^{127}		
Δ^{81}	Δ^{83}	Δ^{89}	Δ^{91}	Δ^{113}	Δ^{115}	Δ^{121}	Δ^{123}		
Δ^{69}	Δ^{71}	Δ^{77}	Δ^{79}	Δ^{101}	Δ^{103}	Δ^{109}	Δ^{111}		
Δ^{65}	Δ^{67}	Δ^{73}	Δ^{75}	Δ^{97}	Δ^{99}	Δ^{105}	Δ^{107}		
Δ^{21}	Δ^{23}	Δ^{29}	Δ^{31}	Δ^{53}	Δ^{55}	Δ^{61}	Δ^{63}		
Δ^{17}	Δ^{19}	Δ^{25}	Δ^{27}	Δ^{49}	Δ^{51}	Δ^{57}	Δ^{59}		
Δ^{5}	Δ^{7}	Δ^{13}	Δ^{15}	Δ^{37}	Δ^{39}	Δ^{45}	Δ^{47}	Δ^{133}	Δ^{135}
Δ	Δ^{3}	Δ^{9}	Δ^{11}	Δ^{33}	Δ^{35}	Δ^{41}	Δ^{43}	Δ^{129}	$\Delta^{131}\dots$

FIGURE 1: The odd powers of Δ arranged according to their code.

We use this bijection to define a new ordering of the integers.

Definition 12. *[6] If k and ℓ are odd integers, we define the relation $\prec$ as follows:*

$$k \prec \ell \text{ if } \begin{cases} h(k) < h(\ell) \text{ or} \\ h(k) = h(\ell) \text{ and } n_5(k) < n_5(\ell). \end{cases}$$

This, along with the standard equality, is a total order relation on the odd integers. In terms of the table, the heights correspond to the diagonals of slope $\nwarrow$, with the arrow pointing towards greater integers.

4.2 Properties

The map $k \to [n_3(k), n_5(k)]$ is not linear. However, it satisfies certain properties which we make explicit in this section. We first introduce the notion of a code with negative coefficients. This will account for the fact that addition of positive integers can result in an negative variation in the code.

Definition 13. *Let k be an integer, and let d be a representation*[2] *of k as a finite sum of powers of 2*

$$\sum_{i=1}^{\infty} \beta_i(d) 2^i = k$$

[2] Here, the word "representation" is used as "way to represent" and not to describe a group morphism whose image is a linear group.

where this time, $\beta_i(d) \in \{-1, 0, 1\}$. Note that this representation is no longer uniquely determined by k.

(i) We define the code of k associated to d as for the standard code:

$$n_3(d) = \sum_{i=0}^{\infty} \beta_{2i+1}(d) 2^i = \sum_{\substack{i=1 \\ i \ odd}}^{\infty} \beta_i(d) 2^{\frac{i-1}{2}} \tag{4.3}$$

$$n_5(d) = \sum_{i=0}^{\infty} \beta_{2i+2}(d) 2^i = \sum_{\substack{i=2 \\ i \ even}}^{\infty} \beta_i(d) 2^{\frac{i-2}{2}}. \tag{4.4}$$

This is denoted $k \sim [n_3(d), n_5(d)]^*$.

(ii) The order relation $\prec$ is defined on the set of all codes associated to k exactly the way it is on usual codes.

The following lemma borrows heavily from proposition 2 in [8].

Lemma 1. *Let k and ℓ be integers with ℓ even.*

(i) We have

$$h(\ell + k) \leq h(\ell) + h(k).$$

(ii) If equality is achieved, then $\mathcal{S}(k) \cap \mathcal{S}(\ell)$ only contains even powers of 2, and if $2^{2i} \in \mathcal{S}(k) \cap \mathcal{S}(\ell)$, then $2^{2i+1} \notin \mathcal{S}(k) \cup \mathcal{S}(\ell)$ and

$$n_5(k + \ell) = n_5(k) + n_5(\ell) - \sum_{2^{2i} \in \mathcal{S}(k) \cap \mathcal{S}(\ell)} 2^i.$$

(iii) In particular if k is odd and m is the odd integer such that

$$m \simeq [n_3(k) + n_3(\ell), n_5(k) + n_5(\ell)],$$

we have

$$k + \ell \preceq m$$

with equality precisely when $\mathcal{S}(k) \cap \mathcal{S}(l) = \emptyset$.

Proof. Part (iii) immediately follows from parts (i) and (ii) and the definition of the order relation $\prec$. We will first prove part (i) and (ii) when $\ell = 2^i$.

Let $2^i \simeq [a, b]$. If $2^i \notin \mathcal{S}(k)$, then $\mathcal{S}(k + 2^i) = \mathcal{S}(k) \cup \{2^i\}$ so

$$[n_3(k + 2^i), n_5(k + 2^i)] = [n_3(k) + a, n_5(k) + b].$$

If $2^i \in \mathcal{S}(k)$, consider the set of all possible codes $2^i \sim [\alpha, \beta]^*$, allowing negative entries. The only possible representations of 2^i are all of the form

$$d_0 = 2^i \quad d_1 = 2^{i+1} - 2^i \quad d_2 = 2^{i+2} - 2^{i+1} - 2^i, \quad d_n = 2^{i+n} - \sum_{i=0}^{n-1} 2^i.$$

One of these representations correponds to the change in the code. Indeed, starting from 2^i, there is a finite collection

$$\mathcal{S}' = \{2^i, 2^{i+1}, ..., 2^{i+n-1}\} \subset \mathcal{S}(k)$$

such that $\mathcal{S}'$ contains the maximal list consecutive powers of 2, in the sense that $2^{i+n} \notin \mathcal{S}(k)$. Doing the addition with carries in binary arithmetic shows that

$$\mathcal{S}(k + 2^i) = \mathcal{S}(k) + \{2^{i+n}\} \setminus \mathcal{S}'.$$

Thus if the code associated to d_n is denoted by $[\alpha_n, \beta_n]^*$, effect of addition of the code is

$$[n_3(k + 2^i), n_5(k + 2^i)] = [n_3(k) + \alpha_n, n_5(k) + \beta_n].$$

The claim (i) is that in this setting,

$$h(k + 2^i) \leq h(k) + h(2^i) = h(k) + a + b.$$

Part (ii) states that there is equality if and only if $n = 1$ and i is even, in which case $n_5(k) + \beta_1 < n_5(k) + b$. Given that

$$h(k + 2^i) = h(k) + \alpha_n + \beta_n$$

it suffices to show that

$$\alpha_n + \beta_n \leq a + b$$

and that if equality is reached, then $\beta_n < b$. For this we show that the sequence $\alpha_n + \beta_n$ is decreasing. Let

$$d_n = 2^{i+n} - \sum_{i=0}^{n-1} 2^i \sim [\alpha_n, \beta_n]^*.$$

The representation d_n is obtained from d_{n-1} by replacing the largest term 2^{i+n-1} by $2^{i+n} - 2^{i+n-1}$. We compute the effect of this substitution on the code.

- If $i + n$ is even, then

$$d_n \sim [\alpha_n, \beta_n]^* = [\alpha_{n-1} - 2 \cdot 2^{\frac{i+n-2}{2}}, \beta_{n-1} + 2^{\frac{i+n-2}{2}}]^* = [\alpha_{n-1} - 2^{\frac{i+n}{2}}, \beta_{n-1} + 2^{\frac{i+n-1}{2}}]^*$$

  so

$$\alpha_n + \beta_n < \alpha_{n-1} + \beta_{n-1}.$$

- If $i + n$ is odd we have

$$d_n \sim [\alpha_n, \beta_n]^* = [\alpha_{n-1} + 2^{\frac{i+n-1}{2}}, \beta_{n-1} - 2 \cdot 2^{\frac{i+n-3}{2}}]^* = [\alpha_{n-1} + 2^{\frac{i+n-1}{2}}, \beta_{n-1} - 2^{\frac{i+n-1}{2}}]^*.$$

  Here, $\alpha_n + \beta_n = \alpha_{n-1} + \beta_{n-1}$ but $\beta_n < \beta_{n-1}$.

Combining the even and odd cases we find that (i) holds and if $a + b = \alpha_n + \beta_n$ then i is even, $n = 1$ and $\beta = b - 2^{\frac{i}{2}}$ which proves (ii). This completes the proof when $\ell = 2^i$. When $\ell \neq 2^i$, (i) holds if one successively adds all powers of 2 contained in $\mathcal{S}(\ell)$. Likewise, (ii) holds inductively, since in order to preserve equality at each step, $2^i \in \mathcal{S}(\ell)$ must satisfy that i is even and $2^{i+1} \notin \mathcal{S}(\ell)$. □

Corollary 1. *In particular, if the integer k is in the interval $0 < k < 2^i$, then $h(k + 2^i) = h(k) + h(2^i)$.*

The last lemma explicits the relation between k mod powers of 2 of and its code mod powers of 2.

Lemma 2. *Let k, ℓ be odd integers. Then*

(i)

$$k \equiv \ell \mod 2^{2i+1} \Leftrightarrow n_3(k) \equiv n_3(\ell) \mod 2^i \text{ and } n_3(k) \equiv n_3(\ell) \mod 2^{i-1}.$$

(ii)

$$k \equiv \ell \mod 2^{2i+2} \Leftrightarrow n_3(k) \equiv n_3(\ell) \mod 2^i \text{ and } n_3(k) \equiv n_3(\ell) \mod 2^i.$$

Proof. In both cases, this follows directly from the definition of the code. If

$$k = \sum_{i=0}^{\infty} \beta_i(k) 2^i$$

then

$$n_3(k) = \sum_{\substack{i=1 \\ i \text{ odd}}}^{\infty} \beta_i(k) 2^{\frac{i-1}{2}}, \qquad n_5(k) = \sum_{\substack{i=2 \\ i \text{ even}}}^{\infty} \beta_i(k) 2^{\frac{i-2}{2}}.$$

□

4.3 The code of a polynomial

We extend the definition of the code to certain polynomials. Recall that $\mathcal{F} \subset \mathbb{F}[\Delta]$ is the subspace of polynomials whose terms all have odd exponents.

Definition 14. *Let $f \in \mathbb{F}_2[\Delta]$ be a polynomial whose exponents are all odd. Then*

$$f(\Delta) = \Delta^{e_1} + ... + \Delta^{e_n}, \quad e_1 \succ ... \succ e_n.$$

We define the code of f to be the code of its highest exponent:

$$[n_3(f), n_5(f)] = [n_3(e_1), n_5(e_1)].$$

The height $h(f)$ and support $\mathcal{S}(f)$ are likewise defined as $h(e_1)$ and $\mathcal{S}(e_1)$.

Remark With this definition, it is immediate that if f, g are two polynomials, $h(f + g) \leq \max h(f), h(g)$.

Lemma 3. *Let $f \in \mathcal{F}$. Then $h(\Delta^{2^i} f) \leq h(f) + h(2^i)$. If equality is reached, then either $2^i \notin \mathcal{S}(f)$ or i is even, $2^i \in \mathcal{S}(f)$ but 2^{i+1} is not. In this case,*

$$[n_3(\Delta^{2^i} f), n_5(\Delta^{2^i} f)] = [n_3(f) + 2^{\frac{i}{2}}, n_5(f) - 2^{\frac{i}{2}}].$$

Proof. Let k be the highest exponent of f. If $k+2^i$ is the highest exponent of $\Delta^{2^i} f$, then this is an immediate consequence of Lemma 1. If this is not the case, then there is another exponent $j \prec k$ such that $j+2^i \succ k+2^i$. However, Lemma 1 still gives us the bounds

$$h(j+2^i) \leq h(j) + h(2^i) \leq h(k) + h(2^i).$$

□

5 The action of T_3

5.1 The recurrences

In their study of the action of Hecke operators on $\mathcal{F}$, Nicolas and Serre determine the following recurrence formula for the action of T_3. Suppose $k \geq 4$, then

$$T_3(\Delta^k) = \Delta T_3(\Delta^{k-3}) + \Delta^4 T_3(\Delta^{k-4}). \tag{5.1}$$

This recursive linear relation for the action of T_3 is the central tool for the proof of our result. We first generalize it to recurrences involving higher powers of 2 (that is, higher than the initial formula where we considered 2^0.)

Lemma 4. *For all $i \geq 0$, if $k \geq 2^{i+2}$, then T_3 can be expressed as :*

$$T_3(\Delta^k) = \Delta^{2^i} T_3(\Delta^{k-3\cdot 2^i}) + \Delta^{4\cdot 2^i} T_3(\Delta^{k-4\cdot 2^i}). \tag{5.2}$$

Proof. The proof is by induction. The base case $i = 0$ is Nicolas and Serre's initial recurrence:

$$T_3(\Delta^k) = \Delta T_3(\Delta^{k-3}) + \Delta^{k-4} T_3(\Delta^{k-4}).$$

Then suppose that we have $T_3(\Delta^k) = \Delta^{2^i} T_3(\Delta^{k-3\cdot 2^i}) + \Delta^{4\cdot 2^i} T_3(\Delta^{k-4\cdot 2^i})$ for $k \geq 2^i$, and suppose $k \geq 2^{i+1}$. We simply compose the i^{th} identity with itself to get:

$$\begin{aligned}
T_3(\Delta^k) &= \Delta^{2^i} T_3(\Delta^{k-3\cdot 2^i}) + \Delta^{4\cdot 2^i} T_3(\Delta^{k-4\cdot 2^i}) \\
&= \Delta^{2^i}(\Delta^{2^i} T_3(\Delta^{k-6\cdot 2^i}) + \Delta^{4\cdot 2^i} T_3(\Delta^{k-7\cdot 2^i})) + \Delta^{4\cdot 2^i}(\Delta^{2^i} T_3(\Delta^{k-7\cdot 2^i}) + \Delta^{4\cdot 2^i} T_3(\Delta^{k-8\cdot 2^i})) \\
&= \Delta^{2\cdot 2^i} T_3(\Delta^{k-6\cdot 2^i}) + \Delta^{5\cdot 2^i} T_3(\Delta^{k-7\cdot 2^i}) + \Delta^{5\cdot 2^i} T_3(\Delta^{k-7\cdot 2^i}) + \Delta^{8\cdot 2^i} T_3(\Delta^{k-8\cdot 2^i}) \\
&= \Delta^{2^{i+1}} T_3(\Delta^{k-3\cdot 2^{i+1}}) + \Delta^{4\cdot 2^{i+1}} T_3(\Delta^{k-4\cdot 2^{i+1}})
\end{aligned}$$

The key point is the fact that the middle terms cancel out since we are working over $\mathbb{F}_2$. □

5.2 Proof of proposition 4.3

Proposition 4.3 in [6] states that the operator T_3 lowers the n_3 part of the code by 1.

Proposition 3 (Proposition 4.3, [6]). *Let $f \in \mathcal{F}$ have highest term $[a, b]$, and let $[c, d]$ denote the highest term of $T_3(f)$. Then:*

(i) $c + d \leq a + b - 1$

(ii) *If $a \neq 0$, then $[c, d] = [a - 1, b]$.*

We use the following notation for T_3.

Definition 15. *Let $k \simeq [a,b]$ be odd. Then $T_{[a,b]}$ denotes $T_3(\Delta^k)$. Similarly, let $T_{[a,b]-2^{i+2}}$ denote $T_3(\Delta^{k-2^{i+2}})$ and let $T_{[a,b]-3\cdot 2^i}$ denote $T_3(\Delta^{k-3\cdot 2^i})$.*

Lemma 5. *If proposition 3 holds for monomials with odd exponents, then it holds for all $f \in \mathcal{F}$.*

Proof. Assume the proposition holds for monomials and let $f \in \mathcal{F}$. It can be written:

$$f = \Delta^{e_1} + ... + \Delta^{e_n}, \quad e_1 \succ ... \succ e_n \quad e_i \simeq [a_i, b_i].$$

We now apply T_3 and get that:

$$T_3(f) = T_{[a_1,b_1]} + T_{[a_2,b_2]} + ... + T_{[a_n,b_n]}.$$

- If $a_1 \neq 0$, then the highest exponent of $T_{[a_1,b_1]}$ has code $[a_1 - 1, b_1]$. For all $i > 1$, the highest exponent of $T_{[a_i,b_i]}$ is $[c_i, d_i]$ and satisfies

$$c_i + d_i \leq a_i + b_i - 1 \leq a_1 + b_1 - 1.$$

  If both inequalities are equalities, then $a_i + b_i = a_1 + b_1$, which implies, since e_1 is the highest term, that

$$b_i < b_1 \quad \Rightarrow \quad [a_i - 1, b_i] \prec [a_1 - 1, b_1].$$

- If $a_1 = 0$ then for all $i > 1$, $a_i + b_i \leq b_1$. So if $[c_i, d_i]$ is the highest exponent of $T_{[a_i,b_i]}$ it satisfies

$$c_i + d_i \leq a_i + b_i - 1 \leq b_1 - 1$$

  which is all that had to be shown.

□

Proof of Proposition 3.

The proof is by induction, using the recurrence of Lemma 4:

$$T_{[a,b]} = \Delta^{2^i} T_{[a,b]-3\cdot 2^i} + \Delta^{4\cdot 2^i} T_{[a,b]-4\cdot 2^i}$$

This formula tells us that the behavior under T_3 of Δ^k is essentially the same as the one of monomials whose exponents are smaller but congruent to $k \simeq [a,b]$ modulo large enough power of 2. The proof is split in three cases. Case 0 is concerned with $[a,b]$ where $a = 0$, in which case the only statement to prove is (i). Case 1 deals with all the $[a,b]$ for which the highest term will appear in $\Delta^{4\cdot 2^i} T_{[a,b]-4\cdot 2^i}$. Finally case 2 takes care of the integers for which highest term comes from $\Delta^{2^i} T_{[a,b]-3\cdot 2^i}$.

Case 0 : $k \simeq [0,b]$

Let i be such that $2^i < b < 2^{i+1}$. Then $[a, b] > 2^{2i+2}$ and we use the $2^{2i^{\text{th}}}$ iteration of the recurrence:

$$T_{[0,b]} = \Delta^{2^{2i}} T_{[0,b]-3\cdot 2^{2i}} + \Delta^{2^{2i+2}} T_{[0,b]-2^{2i+2}}.$$

By our first remark on heights of polynomials and by Lemma 3 on multiplication by Δ^{2^i}, we have that

$$\begin{aligned} h(T_{[0,b]}) &\le \max\{h(\Delta^{2^{2i}} T_{[0,b]-3\cdot 2^{2i}}), h(\Delta^{2^{2i+2}} T_{[0,b]-2^{2i+2}})\} \\ &\le \max\{2^{i-1} + h(T_{[0,b]-3\cdot 2^{2i}}), 2^i + h(T_{[0,b]-2^{2i+2}})\}. \end{aligned}$$

We first compute $h(T_{[0,b]-2^{2i+2}})$. Since $2^{2i+2} \in \mathcal{S}([0, b])$, then $2^{2i+2} \notin \mathcal{S}([0, b] - 2^{2i+2})$ and

$$h([0, b]) = h([0, b] - 2^{2i+2}) + h(2^{2i+2}) \quad \Rightarrow \quad h([0, b] - 2^{2i+2}) = h([0, b]) - h(2^{2i+2}) = b - 2^i.$$

We apply the induction hypothesis to $T_{[0,b]-2^{2i+2}}$ and find that

$$h(T_{[0,b]-2^{2i+2}}) \le h([0, b] - 2^{2i+2}) - 1 = b - 2^i - 1.$$

It follows that

$$2^i + h(T_{[0,b]-2^{2i+2}}) \le b - 1.$$

We now consider the term $\Delta^{2^{2i}} T_{[0,b]-3\cdot 2^{2i}}$. Here we use ideas introduced in the proof of Lemma 1. All the possible ways in which subtracting $3 \cdot 2^{2i}$ from $[0, b]$ could affect the code correspond to all admissible dyadic representations of the negative integer $-3 \cdot 2^{2i}$, where one allows both positive and negative coefficients. These depend on the binary expansion of $[0, b]$. Note that $2^i < b < 2^{i+1}$ and so $2^{2i+2} < [0, b] < 2^{2i+3}$. It follows that the maximal power of 2 that can be subtracted from $[0, b]$, that is, the maximal one that can appear in these representations, is 2^{2i+2}. Moreover, since $a = 0$, no odd powers of 2 can be subtracted. This gives us 2 possible representations :

$$d_1 : -2^{2i+2} + 2^{2i+1} - 2^{2i} = [2^i, -2^i - 2^{i-1}]^* \qquad d_2 : -2^{2i+2} + 2^{2i} = [0, -2^{i-1}]^*.$$

This gives us two possible cases:

$$\Delta^{2^{2i}} T_{[0,b]-3\cdot 2^{2i}} = \Delta^{2^{2i}} T_{[2^i,b-2^i-2^{i-1}]} \quad \text{or} \quad \Delta^{2^{2i}} T_{[0,b]-3\cdot 2^{2i}} = \Delta^{2^{2i}} T_{[0,b-2^{i-1}]}.$$

We apply the induction hypothesis and use Lemma 3:

$$\begin{aligned} h(T_{[2^i,b-2^i-2^{i-1}]}) &= b - 1 + (2^i - 2^i) - 2^{i-1} & &\Rightarrow & h(\Delta^{2^{2i}} T_{[2^i,b-2^i-2^{i-1}]}) &\le b - 1 \\ h(T_{[0,b-2^{i-1}]} &\le b - 2^{i-1} - 1 & &\Rightarrow & h(\Delta^{2^{2i}} T_{[0,b-2^{i-1}]}) &\le b - 1. \end{aligned}$$

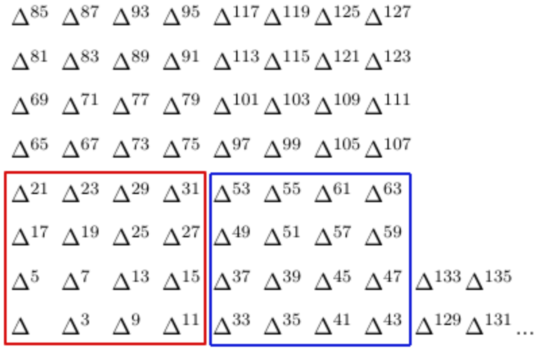
We find that both terms in the recurrence have height less than $b - 1$, which completes the proof.

Case 1 : $k \simeq [a, b]$ such that a is not a single, maximal power of 2.

Let i be the integer such that $2^{i+2} < [a, b] < 2^{i+3}$, and assume that $a \neq 2^{\frac{i+1}{2}}$. We will prove the proposition using the table introduced in Figure 1. We first partition the odd integers $(0, 2^{i+3})$ in two subsets which we refer to as boxes. Let

$$\mathcal{B}_1 = \{k\,;\, k \in \mathbb{Z}_{\text{odd}},\ 0 < k < 2^{i+2}\} \text{ and } \mathcal{B}_2 = \{k\,;\, k \in \mathbb{Z}_{\text{odd}},\ 2^{i+2} < k < 2^{i+3}\}.$$

Here $\mathcal{B}_1$ and $\mathcal{B}_2$ each contain representatives of the residue classes mod 2^{i+2}. If one considers the code $[n_3(k), n_5(k)]$ as system of coordinates indicating how to arrange the odd integers in the plane, then the sets $\mathcal{B}_1$ and $\mathcal{B}_2$ are indeed rectangular. Moreover, the pictorial counterpart of the statement of Lemma 2 is that addition of 2^{i+2} translates $\mathcal{B}_1$ to $\mathcal{B}_2$ while preserving the arrangement of integers inside each box. Thus two integers $k \simeq [c, d] \in \mathcal{B}_1$ and $k' \simeq [c', d'] \in \mathcal{B}_2$ will be said to be in the same position inside their respective boxes when $k \equiv k' \mod 2^{i+2}$. Figure 2 provides an illustration.



Δ^{85}	Δ^{87}	Δ^{93}	Δ^{95}	Δ^{117}	Δ^{119}	Δ^{125}	Δ^{127}			
Δ^{81}	Δ^{83}	Δ^{89}	Δ^{91}	Δ^{113}	Δ^{115}	Δ^{121}	Δ^{123}			
Δ^{69}	Δ^{71}	Δ^{77}	Δ^{79}	Δ^{101}	Δ^{103}	Δ^{109}	Δ^{111}			
Δ^{65}	Δ^{67}	Δ^{73}	Δ^{75}	Δ^{97}	Δ^{99}	Δ^{105}	Δ^{107}			
Δ^{21}	Δ^{23}	Δ^{29}	Δ^{31}	Δ^{53}	Δ^{55}	Δ^{61}	Δ^{63}			
Δ^{17}	Δ^{19}	Δ^{25}	Δ^{27}	Δ^{49}	Δ^{51}	Δ^{57}	Δ^{59}			
Δ^{5}	Δ^{7}	Δ^{13}	Δ^{15}	Δ^{37}	Δ^{39}	Δ^{45}	Δ^{47}	Δ^{133}	Δ^{135}	
Δ	Δ^{3}	Δ^{9}	Δ^{11}	Δ^{33}	Δ^{35}	Δ^{41}	Δ^{43}	Δ^{129}	Δ^{131}	...

FIGURE 2: The two boxes $\mathcal{B}_1$ (in red) and $\mathcal{B}_2$ (in blue) in the case $i = 3$.

By construction, $[a, b] \in \mathcal{B}_2$. Our induction hypothesis will be that the proposition is proved for all monomials whose leading exponent is in $\mathcal{B}_1$. We will show that the leading term of $\Delta^{2^{i+2}} T_{[a,b]-2^{i+2}}$ is $[a-1, b]$. Let $[a', b'] = [a, b] - 2^{i+2}$; we have that $[a', b'] \in \mathcal{B}_1$ occupies the same position as $[a, b] \in \mathcal{B}_2$. Moreover, $a' \neq 0$ since $a \neq 2^{\frac{i+1}{2}}$. Thus it follows from the induction hypothesis that

$$T_{[a',b']} = [a'-1, b'] + \text{ lower monomials.}$$

We now compute the leading exponent of $\Delta^{2^{i+2}} T_{[a-b]-2^{i+2}}$. Multiplication by $\Delta^{2^{i+2}}$ translates $\mathcal{B}_1$ to $\mathcal{B}_2$. Lemma 2 tells us that since $[a', b'] \equiv [a, b] \mod 2^{i+2}$, then $[a'-1, b'] \equiv [a-1, b]$ mod ${}^{2^i+2}$. It follows that $[a-1, b]$ appears in $\Delta^{2^{i+2}} T_{[a-b]-2^{i+2}}$ as the translate of $[a'-1, b']$. Given any other term of $T_{[a-b]-2^{i+2}}$ with exponent $[c, d]$, then by Lemma 1,

$$h([c, d] + 2^{i+2}) = h([c, d]) + h(2^{i+2}) \leq h([a, b]) + h(2^{i+2})$$

and in case of equality,

$$n_5([c, d] + 2^{i+2}) = d + n_5(2^{i+2}) \leq b + h(2^{i+2}).$$

To complete this section we only need to show that $\Delta^{2^i} T_{[a,b]-3\cdot 2^i}$ is a sum of monomials

$[c_i, d_i]$ which are all lower than $[a-1, b]$. For this, we refine our partition by splitting each $\mathcal{B}_i$ into four smaller boxes. This gives us eight boxes $B_1, ..., B_8$:

$$B_n = \{k\,;\, k \in \mathbb{Z}_{\text{odd}},\ 2^i(n-1) < k < 2^i n\}, \quad 1 \leq n \leq 8.$$

Each B_i contains a unique representative for each odd residue class in $\mathbb{Z}/2^i\mathbb{Z}$. Lemma 2 still holds and we say that $[c, d]$ and $[c'', d'']$ are in the same position inside their respective boxes when $[c, d] \equiv [c'', d''] \mod 2^i$.

By construction, $[a, b] \in B_n$ for $5 \leq n \leq 8$. So the induction hypothesis is that the proposition holds for boxes B_1 through B_4. Let $[a'', b''] = [a, b] - 3 \cdot 2^i$ as integers. Here we have two different cases, depending on whether i is even or odd.

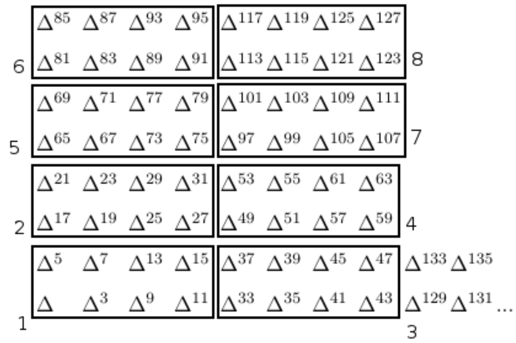

Δ^{85} Δ^{87} Δ^{93} Δ^{95} Δ^{117} Δ^{119} Δ^{125} Δ^{127}
6 Δ^{81} Δ^{83} Δ^{89} Δ^{91} Δ^{113} Δ^{115} Δ^{121} Δ^{123} 8
Δ^{69} Δ^{71} Δ^{77} Δ^{79} Δ^{101} Δ^{103} Δ^{109} Δ^{111}
5 Δ^{65} Δ^{67} Δ^{73} Δ^{75} Δ^{97} Δ^{99} Δ^{105} Δ^{107} 7
Δ^{21} Δ^{23} Δ^{29} Δ^{31} Δ^{53} Δ^{55} Δ^{61} Δ^{63}
2 Δ^{17} Δ^{19} Δ^{25} Δ^{27} Δ^{49} Δ^{51} Δ^{57} Δ^{59} 4
Δ^{5} Δ^{7} Δ^{13} Δ^{15} Δ^{37} Δ^{39} Δ^{45} Δ^{47} Δ^{133} Δ^{135}
Δ Δ^{3} Δ^{9} Δ^{11} Δ^{33} Δ^{35} Δ^{41} Δ^{43} Δ^{129} Δ^{131} ...
1
3

FIGURE 3: An example of a partition into 8 boxes for i even (here $i = 4$).

- If i is even, the arrangement of the boxes is indicated in figure 3. Depending on in which box $[a, b]$ is contained, the values of $[a'', b'']$ are the following:

$$[a, b] \in B_5 \text{ or } B_7 \Rightarrow [a'', b''] = [a, b - 3 \cdot 2^{\frac{i-2}{2}}] \tag{5.3}$$

$$[a, b] \in B_6 \Rightarrow [a'', b''] = [a + 2^{\frac{i}{2}}, b - 3 \cdot 2^{\frac{i-2}{2}}] \tag{5.4}$$

$$[a, b] \in B_8 \Rightarrow [a'', b''] = [a - 2^{\frac{i}{2}}, b - 2^{\frac{i-2}{2}}]. \tag{5.5}$$

  In each of those cases, induction tells us that each term $[c'', d'']$ of $T_{[a'',b'']}$ will be at most $[a'' - 1, b'']$. By Lemma 1(iii),

$$[c, d] = [c'', d''] + 2^i \prec [c'', d'' + 2^{\frac{i-2}{2}}].$$

  By comparing this maximal possible increase with each of the codes of $[a'', b'']$ in equations (5.3)-(5.5), we find that $[c, d] \prec [a - 1, b]$. So in this case, $[a - 1, b]$ is not an exponent of $\Delta^{2^i} T[a, b] - 3 \cdot 2^i$

- If i is odd, the arrangement of boxes is the following.

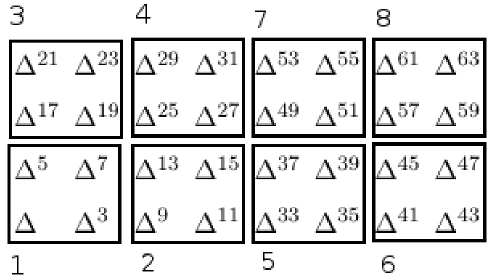


FIGURE 4: An example of a partition into 8 boxes for i odd (here $i = 3$).

The possible values of $[a'', b''] = [a, b] - 3 \cdot 2^i$ are the following:

$$[a, b] \in B_5 \text{ or } B_7 \Rightarrow [a'', b''] = [a - 2^{\frac{i+1}{2}} + 2^{\frac{i-1}{2}}, b] = [a - 2^{\frac{i-1}{2}}, b] \tag{5.6}$$

$$[a, b] \in B_6 \Rightarrow [a'', b''] = [a - 3 \cdot 2^{\frac{i-1}{2}}, b + \cdot 2^{\frac{i-1}{2}}] \tag{5.7}$$

$$[a, b] \in B_8 \Rightarrow [a'', b''] = [a - 2^{\frac{i-1}{2}}, b - \cdot 2^{\frac{i-1}{2}}] \tag{5.8}$$

By the induction hypothesis, each term $[c'', d'']$ of $T_{[a'',b'']}$ is lower or equal than $[a''-1, b'']$. To bound the possible height of $[c'', d''] + 2^i$, we use Lemma 1:

$$[c, d] = [c'', d''] + 2^i \preceq [c'' + 2^{\frac{i-1}{2}}, d'']. \tag{5.9}$$

By comparing this increase with the decrease of (5.7) and (5.8), we see that if $[a, b] \in B_6$ or B_8, $[c, d] \prec [a - 1, b]$. However things are different if $[a, b] \in B_5$ or B_7. The maximal possible increase in the code in 5.9 is equal to the decrease in (5.6). Since $[a'' - 1, b]$ is the leading term of $T[a'', b'']$, this implies that if

$$h([a'' - 1, b''] + 2^i) = h([a'' - 1, b]) + h(2^i)$$

and

$$n_5([a'' - 1, b''] + 2^i) = n_5([a'' - 1, b]) + n_5(2^i)$$

then $[a - 1, b]$ appears in $\Delta^{2^i} T_{[a'',b'']}$. We now turn to the table to understand this maximal increase.

Multiplying to by Δ^{2^i} preserves positions inside each box, but sends B_n to B_{n+1}. So the increase in the code is determined by the box in which $[a'' - 1, b'']$ is contained. In particular, the maximal possible increase of (5.9) occurs when $2^i \notin \mathcal{S}([a'', b''])$ and corresponds to translating a box to the one immediately to its right. This occurs precisely when $[a'' - 1, b''] \in B_n$ for $n = 1, 3, 5, 7$. Only 1 and 3 are of interest to us. Recall that $[a'', b'']$ is assumed to be in B_2 (or B_4 if $[a, b] \in B_7$). Also note that $[a'' - 1, b'']$ is the monomial which is immediately to the left of $[a, b]$. It follows that $[a'' - 1, b''] \in B_1$ (resp. B_3) is the image of $[a'', b''] \in B_2$ (resp B_4) if and only if $[a'', b'']$ was in the leftmost column of B_2 (resp. B_4). Since $[a, b]$ and $[a'', b'']$ have the same respective positions in their boxes, this happens only if $[a, b]$ is in the leftmost column of B_5 (resp. B_7). This happens if and only if $[a, b]$ is in the leftmost column of $\mathcal{B}_2$, which is equivalent to

$$[a, b] \equiv \text{ a sum of even powers of 2} \mod 2^{i+2} \Leftrightarrow a \equiv 0 \mod 2^{\frac{i+1}{2}}.$$

This last criterion corresponds to the case that we are excluding by assumption. We conclude that all terms $[c, d]$ of $\Delta^{2^i} T_{[a'', b'']}$ are strictly lower than $[a - 1, b]$, which completes the proof for this case.

Case 2 : $[a, b]$ *where* $2^{i+2} < [a, b] < 2^{i+3}$ *and* $a = 2^{\frac{i+1}{2}}$.

An immediate upshot of the above discussion is that if $2^{i+2} < [a, b] < 2^{i+3}$, where i is odd and $a = 2^{\frac{i+1}{2}}$, the term $[a - 1, b]$ *does* indeed appear as the leading exponent of $\Delta^{2^i} T_{[a,b]-3\cdot 2^i}$. This puts us in a situation that is the reverse of Case 1. Indeed, to prove the proposition, it suffices to show that $[a - 1, b]$ does not appear in $\Delta^{2^{i+2}} T_{[a,b]-2^{i+2}}$. However, this is straightforward. We have

$$[a, b] - 2^{i+2} = [0, b].$$

Let $[c', d']$ be any exponent in $T_{[0,b]}$, and $[c, d] = [c', d'] + 2^{i+2}$. Then by the induction hypothesis and by Lemma 1,

$$c' + d' \leq b - 1 \quad \Rightarrow \quad c + d \leq 2^{i+2} + b - 1 = a + b - 1.$$

This could still be an equality. But note that

$$[a', b'] < 2^{i+2} \quad \Rightarrow \quad [c', d'] < 2^{i+2}, \quad \text{for all terms } [c', d'] \text{ of } T_{[a',b']}.$$

It then follows from corollary 1 that

$$[c, d] = \Delta^{2^i}[c', d'] = [c' + 2^{\frac{i+1}{2}}, d'].$$

So $c > 2^{\frac{i+1}{2}}$ for all terms in $\Delta^{2^{i+2}} T_{[a',b']}$, which implies that $d < b - 1$, and excludes the possibility that $[c, d] \succeq [a - 1, b]$.

□

6 The action of T_5

6.1 More recurrences

For T_5, the authors obtain a similar recurrence when $k > 6$:

$$T_5(\Delta^k) = \Delta^2 T_5(\Delta^{k-2}) + \Delta^4 T_5(\Delta^{k-4}) + \Delta^6 T_5(\Delta^{k-6}) + \Delta T_5(\Delta^{k-5}) \tag{6.1}$$

that we generalize identically.

Lemma 6. *For all* $i \geq 0$*, if* $k \geq 6 \cdot 2^i$*, then* T_5 *can be expressed as :*

$$T_5(\Delta^k) = \Delta^{2\cdot 2^i} T_5(\Delta^{k-2\cdot 2^i}) + \Delta^{4\cdot 2^i} T_5(\Delta^{k-4\cdot 2^i}) + \Delta^{6\cdot 2^i} T_5(\Delta^{k-6\cdot 2^i}) + \Delta^{2^i} T_5(\Delta^{k-5\cdot 2^i}). \tag{6.2}$$

The proof is identical to that for T_3: we compose the i^{th} identity with itself to obtain the $i+1^{th}$. Mixed terms cancel out since we are in characteristic 2.

6.2 Proposition 4.4 and integers such that $n_3(\ell) = 0$

Proposition 4.4 is identical to proposition 4.3, except that the decrease is in the n_5 coordinate.

Proposition 4 (Proposition 4.4, [6])**.** *Let $f \in \mathcal{F}$ have highest term $[a, b]$, and let $[c, d]$ denote the highest term of $T_5(f)$. Then:*

(i) $c + d \leq a + b - 1$

(ii) If $b \neq 0$, then $[c, d] = [a, b-1]$.

The statements of the two propositions being extremely similar, but the proofs are not. The reason is that the recurrence formula asks to simultaneously apply induction in 4 different manners, and that the cancellation between the distinct terms appears unpredictable. Thus to prove proposition 4.4, we use a tool that we now have at our disposition. When possible, we will conjugate T_5 by T_3 and let

$$T_5(\Delta^k) = T_3^{-1} T_5 T_3(\Delta^k).$$

Since the leading term of T_3 is smaller than k, see [6], we can apply the induction hypothesis to $T_3(\Delta^k)$. For example if $k \simeq [a, b]$ with $a, b \neq 0$, we have

$$[n_3(T_5T_3(\Delta^k)), n_3(T_5T_3(\Delta^k))] = [a-1, b-1].$$

The next step is to use commutativity of Hecke operators and to apply T_3^{-1} to conclude that

$$[n_3(T_3^{-1}T_5T_3(\Delta^k)), n_3(T_3^{-1}T_5T_3(\Delta^k))] = [n_3(T_5(\Delta^k)), n_3(T_5(\Delta^k))] = [a, b-1].$$

Of course, even for the highest term, inversion of T_3 is not well-defined in general. Nevertheless, proposition 4.3 is precise about what the highest term possible preimages of $\Delta^{k'}$ with $k \simeq [a-1, b-1]$ can be: either it is $j \simeq [a, b-1]$ or it is $\ell \simeq [0, d]$. However, since $\ell < k$, there are very few possibilities for ℓ. Moreover, the induction hypothesis implies that we would have

$$h(T_3(\Delta^\ell)) = h(T_5T_3(\Delta^k)) = h(k) - 2.$$

Since T_3 lowers the code by at least 1, $h(l) \geq h(k) - 1$.

Lemma 7. *If $\ell < k$ and $n_3(\ell) = 0$ then $h(\ell) < h(k)$.*

Proof. Simply note that

$$2^{2i+1} \simeq [2^i, 0] \leq [0, 2^i] \simeq 2^{2i+2}. \quad (6.3)$$

It then follows by Lemma 1 that

$$[n_3(k), n_5(k)] = [n_3(k), 0] + [0, n_5(k)] \leq [0, n_3(k)] + [0, n_5(k)] \leq [0, n_3(k) + n_5(k)] = [0, h(k)].$$

□

So we find that $h(\ell) = h(k) - 1$. Putting together $\ell < k$, $n_3(\ell) = 0$ and $h(\ell) = h(k) - 1$, we find a condition on $\mathcal{S}(k)$ for the k such that $T_3^{-1}(\Delta^k)$ is not well-defined.

Lemma 8. *Let k be an odd integer. Suppose that there is another odd integer ℓ such that $h(\ell) = h(k) - 1$, $n_3(\ell) = 0$ and $\ell < k$. Then $\mathcal{S}(k)$ contains at most a single 2^i such that i is odd. Moreover, if for j even we have $2^j \in \mathcal{S}(k)$, then $j > i$.*

Proof. We begin with an integer ℓ such that $n_3(\ell) = 0$ and consider all possible ways of constructing a $k > \ell$ such that $h(k) = h(\ell) + 1$. The two trivial cases that satisfy this are

$$k \simeq [0, n_5(\ell) + 1] \quad \text{and} \quad k \simeq [1, n_5(\ell)].$$

In the first case, $\mathcal{S}(k)$ contains no odd power of 2. In the second case, 2^1 is the only power of 2 in $\mathcal{S}(k)$ and is trivially the smallest. The other possibilities come from adding $a > 1$ to $n_3(\ell)$ and subtracting $a - 1$ to $n_5(\ell)$ to get

$$k \simeq [a, n_3(\ell) - a + 1].$$

In other words, we want the code

$$[a, 1 - a]$$

to represent a positive integer. However, if 2^i is the smallest power of 2 in $\mathcal{S}(a)$, then by doing the binary arithmetic, we find that

$$\mathcal{S}(a - 1) = (\mathcal{S}(a) \setminus 2^i) \cup \{1, 2, ..., 2^{i-1}\}.$$

Let $\bar{a}$ be

$$\bar{a} = \sum_{2^j \in \mathcal{S}(a) \cap \mathcal{S}(a-1)} 2^j.$$

Then we can decompose $[a, (1 - a)]$ into

$$[a, 1 - a] = [\bar{a}, -\bar{a}] + \left[2^i, -\sum_{j=0}^{i-1} 2^j \right].$$

The integer corresponding to the second term is

$$\left[2^i, \sum_{j=0}^{i-1} 2^i \right] \simeq 2^{2i+1} - \sum_{j=0}^{i-1} 2^{2j+2} < 2^{2i+1}.$$

This integer is positive. However,

$$2^{2j+2} \simeq [0, 2^j],\ 2^{2j+1} \simeq [2^j, 0] \quad \Rightarrow \quad [2^j, -2^j] \simeq 2^{2j+1}.$$

By construction of $\bar{a}$, all powers of 2 in $\mathcal{S}(\bar{a})$ are strictly greater than i. It follows that

$$[\bar{a}, -\bar{a}] \simeq n < -2^{2i+1}.$$

So if $\bar{a}$ is non-zero, $[a, 1 - a]$ represents a positive number. It follows that in all cases $a = 2^i$

and $a-1=\sum_{j=0}^{i-1} 2^j$. So there is only way to obtain a k satisfying our conditions from ℓ: if $\mathcal{S}(\ell)$ contains a sequence $2^2, 2^4, ..., 2^{2i}$ the integer is of the form

$$k = \ell - \sum_{j=i}^{i-1} 2^{2j} + 2^{2i+1}.$$

So k has the prescribed form. □

The next lemma gives a lower bound on the exponents in the $T_p(\Delta^k)$.

Lemma 9. *The image of Δ^k under T_p is a polynomial whose degrees in Δ all lie in the interval $[\frac{k}{p}, k-2]$.*

Proof. The upper bound is a direct consequence of the nilpotency of the T_p. The lower bound follows from the fact that the coefficient of q^n in $T_p(\Delta^k)$ is $\tau_k(pn) + \tau_k(\frac{n}{p})$, the latter appearing only if $p \mid n$. This second term is zero if $\frac{n}{p} < k \Rightarrow n < kp$. The first term is zero if $pn < k \Rightarrow n < \frac{k}{p}$. Thus both terms are zero if $n < \frac{k}{p}$ and since the term q^j appears in the q-expansion of Δ^j, we conclude. □

Finally, we show, as we did for T_3, that it is sufficient to demonstrate the proposition for monomials.

Definition 16. *Let $k \simeq [a,b]$ is an odd integer, and ℓ is an even integer. When used in the rest of the text, the notations $T_{[a,b]}$ and $T_{[a,b]-\ell}$ will be used to denote $T_5(\Delta^k)$ and $T_5(\Delta^{k-\ell})$.*

Lemma 10. *If proposition 4 holds for monomials with odd exponents, then it holds for all $f \in \mathcal{F}$.*

Proof. The reasoning we used for T_3 holds here. Assume the proposition holds for monomials and let $f \in \mathcal{F}$. The function f has the form

$$f = \Delta^{e_1} + ... + \Delta^{e_n}, \quad e_1 \succ ... \succ e_n \quad e_i \simeq [a_i, b_i].$$

We apply T_5 and get that:

$$T_5(f) = T_{[a_1,b_1]} + T_{[a_2,b_2]} + ... + T_{[a_n,b_n]}.$$

- If $b_1 \neq 0$, then the highest exponent of $T_{[a_1,b_1]}$ has code $[a_1, b_1 - 1]$. For all $i > 1$, the highest exponent of $T_{[a_i,b_i]}$ is $[c_i, d_i]$ and satisfies

  $$c_i + d_i \leq a_i + b_i - 1 \leq a_1 + b_1 - 1.$$

  If both inequalities are equalities, then $a_i + b_i = a_1 + b_1$, which implies, since e_1 is the highest term, that

  $$b_i < b_1 \quad \Rightarrow \quad [a_i, b_i - 1] \prec [a_1, b_1 - 1].$$

- If $b_1 = 0$ then all other exponents $[a_i, b_i]$ satisfy $a_i + b_i < a_1$. Otherwise we would have $b_1 < b_i$, which can't happen by definition. Thus if $[c_i, d_i]$ is the highest exponent of $T_{[a_i,b_i]}$ it satisfies

  $$c_i + d_i \leq a_i + b_i - 1 < a_1 - 1.$$

The highest exponent of $T_{[a_1,0]}$ also has height less or equal that $a_1 - 1$, so we are done.

□

6.3 Proof of proposition 4.4

We now prove proposition 4 stated in the previous subsection. The proof will be divided in 5 cases. As for proposition 3, case 0 will be concerned with the integers that only satisfy the assumptions of (i). Case 1 will describe the ideal situation in which T_3 can be inverted. Cases 2, and 3 will use the recurrence (6.1) to deal with situations where T_3 cannot be inverted. Finally, case 4 will use the recurrence to show that despite the appearances, T_3 can be inverted.

Proof of Proposition 4 . Case 0: $k \simeq [a, 0]$.

If $f = \Delta^k$ and $k \simeq [a, 0]$, the claim in [6] is that $h(T_5(\Delta^k)) < h(\Delta^k)$. We will need a slightly stronger result later and will show that

$$h(T_5(\Delta^k)) \leq a - 3. \tag{6.4}$$

If $k \neq 1$, then $a \neq 0$ so by proposition 3, we have

$$[n_3(T_3(\Delta^k)), n_5(T_3(\Delta^k))] = [a - 1, 0].$$

Thus if $\tilde{k}$ is the the leading exponent of $T_3(\Delta^k)$ then $n_5(\tilde{k}) = 0$. We apply the induction hypothesis to $T_3(\Delta^k)$ and find that

$$h(T_5 T_3(\Delta^k)) \leq h(T_3(\Delta^k)) - 3 = a - 4.$$

We will determine the highest exponent of $T_5(\Delta^k)$ by considering the possibilities for the highest exponent of the preimage under T_3 of $T_5 T_3(\Delta^k)$. By proposition 3, it can be one of two things. In general it will be integer

$$\ell \simeq [n_3(T_3 T_5(\Delta^k)) + 1, n_5(T_3 T_5(\Delta^k)].$$

In this case,

$$h(T_5(\Delta^k)) = h(\ell) = h(T_3 T_5(\Delta^k)) + 1 \leq h(\Delta^k) - 3$$

and we are done.

The other possibility is that the leading exponent is of the form $\ell \simeq [0, d]$. In this case, its exact value is not given by proposition 3. However, it is still possible to show that

$$h(T_5(\Delta^k)) = h(\ell) \leq a - 3.$$

By Lemma 7, the only two possibilities are $h(\ell) = a - 2$ and $h(\ell) = a - 1$. We will assume these in turn and derive contradictions.

- Assume that $h(\ell) = h(k) - 2$. This equality also holds modulo 4 by Lemma 2. There are four possibilities for the code of ℓ where each entry is taken modulo 4:

$$\begin{array}{lcl} \ell \simeq [a \mod 4, 2 \mod 4] & \Rightarrow & \ell \equiv k \mod 16 \\ \ell \simeq [a+1 \mod 4, 1 \mod 4] & \Rightarrow & \ell \equiv k+6 \mod 8 \\ \ell \simeq [a+2 \mod 4, 0 \mod 4] & \Rightarrow & \ell \equiv k \mod 8 \\ \ell \simeq [a+3 \mod 4, 3 \mod 4] & \Rightarrow & \ell \equiv k+6 \mod 8 \end{array}$$

However, we know from [6] all terms of $T_5(\Delta^k)$ are congruent to $5k \mod 8$, which is equivalent to $k+4 \mod 8$.

- Assume that ℓ is the leading term of $h(T_5(\Delta^k))$, that $h(\ell) = h(k) - 1$, and $n_3(\ell) = 0$. By Lemma 8, this implies that $\mathcal{S}(k)$ can contain at most a single odd power of 2. However, since $n_5(k) = 0$, $\mathcal{S}(k)$ only contains odd power of 2. It follows that $k = 2^{2i+1}+1 \simeq [2^i, 0]$ and

$$\ell \simeq [0, a-1] \quad \Rightarrow \quad \ell = \sum_{\substack{j=1 \\ j \text{ even}}}^{2i} 2^j.$$

We will now use the recurrence 6.1 to show that this specific term never appears in $T_5(\Delta^k)$.

If $k = 2^{2i+1} + 1 \simeq [2^i, 0]$ we use following iteration of the recurrence:

$$T_{[2^i,0]} = \Delta^{2\cdot 2^{2i-2}} T_{[2^i,0]-2\cdot 2^{2i-2}} + \Delta^{4\cdot 2^{2i-2}} T_{[2^i,0]-4\cdot 2^{2i-2}} + \Delta^{6\cdot 2^{2i-2}} T_{[2^i,0]-6\cdot 2^{2i-2}} + \Delta^{2^{2i-2}} T_{[2^i,0]-5\cdot 2^{2i-2}}.$$

The integers to which we apply the induction hypothesis are

$$\begin{array}{ll} [2^i,0] - 2\cdot 2^{2i-2} = 2^{2i} + 2^{2i-1} \simeq [2^{\frac{2i-2}{2}}, 2^{\frac{2i-2}{2}}] & [2^i,0] - 4\cdot 2^{2i-2} = 2^{2i} \simeq [0, 2^{\frac{2i-2}{2}}] \\ [2^i,0] - 5\cdot 2^{2i-2} = 2^{2i-1} \simeq [2^{\frac{2i-2}{2}}, 0] & [2^i,0] - 6\cdot 2^{2i-2} = 2^{2i-1} + 2^{2i-2} \simeq [2^{\frac{2i-2}{2}}, 2^{\frac{2i-6}{2}}] \end{array}$$

We first consider the two terms in the top row for which, by the induction hypothesis, the codes are the following:

$$T_{[2^i,0]-2\cdot 2^{2i-2}} \simeq [2^{\frac{2i-2}{2}}, 2^{\frac{2i-2}{2}} - 1] \qquad T_{[2^i,0]-4\cdot 2^{2i-2}} \simeq [0, 2^{\frac{2i-4}{4}} - 1]$$

So the code of the highest exponent of $\Delta^{2\cdot 2^{2i-2}} T_{[2^i,0]-2\cdot 2^{2i-2}}$ is

$$[2^{\frac{2i-2}{2}}, 2^{\frac{2i-2}{2}} - 1] + 2^{2i-1} = [2^{\frac{2i-2}{2}} + 2^{\frac{2i-2}{2}}, 2^{\frac{2i-2}{2}} - 1] = [0, 2^{\frac{2i-2}{2}} + 2^{\frac{2i-2}{2}} - 1] = [0, 2^{\frac{2i}{2}} - 1] \simeq \ell.$$

Likewise, the code of $\Delta^{2\cdot 4^{2i-2}} T_{[2^i,0]-2\cdot 4^{2i-2}}$ is

$$[0, 2^{\frac{2i-4}{4}} - 1] + 2^{2i} = [0, 2^{\frac{2i-2}{2}} + 2^{\frac{2i-2}{2}} - 1] = [0, 2^{\frac{2i}{2}} - 1] \simeq \ell.$$

So ℓ appears as the highest exponent of both terms, and the Δ^ℓ cancel each other out.

Next, ℓ is not an exponent of $\Delta^{2\cdot 6^{2i-2}}T_{[2^i,0]-2\cdot 6^{2i-2}}$ because it is too small:

$$\ell = \sum_{\substack{j=1 \\ j \text{ even}}}^{2i} 2^j < 2^{2i} + 2^{2i-1} = 6 \cdot 2^{2i-2}.$$

Finally, ℓ is too large to be an exponent of $T_{[2^i,0]-5\cdot 2^{2i-2}}$ since they are all strictly less than $2^{2i+1} - 5 \cdot 2^{2i-2}$. So all the exponents of $\Delta^{2^{2i-2}}T_{[2^i,0]-5\cdot 2^{2i-2}}$ are smaller than

$$2^{2i+1} - 4 \cdot 2^{2i-2} = 2^{2i-1} < \ell = \sum_{\substack{j=1 \\ j \text{ even}}}^{2i} 2^j.$$

This completes the proof that ℓ is not the leading exponent of $T_{[2^i,0]}$.

Case 1: the general case

Let $k \simeq [a, b]$ be an odd integer not of the form

$$\beta_{2i+1}(k)2^{2i+1} + \sum_{\substack{j>2i+1 \\ j \text{ even}}}^{\infty} \beta_j(k)2^j.$$

In particular this means that $a \neq 0$. Then by proposition 3,

$$T_3(\Delta^k) \simeq [a-1, b]$$

and since the exponents of $T_3(\Delta^k)$ are smaller than k, by the induction hypothesis we have

$$T_5T_3(\Delta^k) \simeq [a-1, b-1].$$

By Lemma 8, the highest exponent of $T_5(\Delta^k)$ is not of the form $\ell \simeq [0, d]$. If follows that $T_5T_3(\Delta^k)$ has a unique preimage under T_3, whose leading exponent is $[a, b-1]$.

Case 2: $k \simeq [0, 2^i]$.

The integers such that $n_3(k) = 0$ and $n_5(k) = 2^i$ are the smallest ones such that the integer $[a, b] - [a, b-1]$ is of a given form. They are the analogue of the case 2 in the proof of proposition 3 in the sense that the leading exponent will arise from the $\Delta^{2^i}T_5(\Delta^{k-5\cdot 2^i})$ term. As in case 1, we first apply T_3. By proposition 3,

$$h(T_3(\Delta^k)) \leq h(k) - 1 = 2^i - 1.$$

By the induction hypothesis,

$$h(T_3T_5(\Delta^k)) \leq h(k) - 2 = 2^i - 2.$$

This bounds the preimages under T_3 : by proposition 3, all exponents $[c, d]$ of $T_5(\Delta^k)$ satisfy

$$c + d \leq h(k) - 1 \text{ or } c = 0. \tag{6.5}$$

However, if $\ell = [0, d]$ then $d < 2^i$ since $\ell < k$ so $h(\ell) \leq h(k) - 1$ in any case. We will now show that the highest integer satisfying $h(\ell) = h(k) - 1$, namely

$$[0, 2^i - 1] \simeq \ell = \sum_{\substack{j=0 \\ j \text{ even}}}^{2i} 2^j$$

appears in $T_5(\Delta^k)$, which automatically makes it the highest exponent.

For this, we will show using the recurrence formula that is appears as the leading term of the fourth term of the recurrence, and that is is absent from all three others. Recall that $k = 2^{2i+2} + 1 \simeq [0, 2^i]$. We use the following iteration of the recurrence.

$$T_{[0,2^i]} = \Delta^{2 \cdot 2^{2i-1}} T_{[0,2^i]-2\cdot 2^{2i-1}} + \Delta^{4\cdot 2^{2i-1}} T_{[0,2^i]-4\cdot 2^{2i-1}} + \Delta^{6\cdot 2^{2i-1}} T_{[0,2^i]-6\cdot 2^{2i-1}} + \Delta^{2^{2i-1}} T_{[0,2^i]-5\cdot 2^{2i-1}} \tag{6.6}$$

and

$$\begin{array}{llll} (a) & [0,2^i] - 2\cdot 2^{2i-1} \simeq [2^i, 2^{i-1}] & (b) & [0,2^i] - 4\cdot 2^{2i-1} \simeq [2^i, 0] \\ (c) & [0,2^i] - 6\cdot 2^{2i-1} \simeq [0, 2^i] & (d) & [0,2^i] - 5\cdot 2^{2i-1} \simeq [2^{i-1}, 2^{i-1}]. \end{array}$$

We do (d) first. By induction,

$$T_{[0,2^i]-5\cdot 2^{2i-1}} \simeq [2^{i-1}, 2^{i-1} - 1] = \left[2^{i-1}, \sum_{j=1}^{i-2} 2^j \right].$$

Thus the highest exponent of $T_{[0,2^i]-5\cdot 2^{2i-1}}$ is the integer

$$m = 2^{2i-1} + \sum_{\substack{j=0 \\ j \text{ even}}}^{2i-2} 2^j = \ell - 2^{2i-1}.$$

It follows that $\ell = m + 2^{2i-1}$ is an exponent of $\Delta^{2i-1} T_{[0,2^i]-5\cdot 2^{2i-1}}$.

We now need to ensure that ℓ does not appear as an exponent in any of the three other terms. In this case, the two occurrences of Δ^ℓ would cancel out. For (b) and (c), notice that

$$\ell = \sum_{\substack{j \text{even} \\ j \leq i}} 2^j < 2^{2i+1} = 4 \cdot 2^{2i-1} < 6 \cdot 2^{2i-1}$$

so it is too small to possibly appear in $\Delta^{4\cdot 2^{2i-1}} T_{[0,2^i]-4\cdot 2^{2i-1}}$ or $\Delta^{6\cdot 2^{2i-1}} T_{[0,2^i]-6\cdot 2^{2i-1}}$ Finally, if

ℓ appeared in $\Delta^{2\cdot 2^{2i-1}} T_{[0,2^i]-2\cdot 2^{2i-1}}$ it would imply that

$$\ell - 2^{2i} = \sum_{\substack{j \leq 2i-2 \\ j \text{ even}}} 2^j$$

appeared as an exponent in $T_{[0,2^i]-2\cdot 2^{2i-1}}$. This contradicts the lower bound of Lemma 9 since

$$[0, 2^i] - 2 \cdot 2^{2i-1} = 2^{2i} \text{ and } \sum_{\substack{j \leq 2i-2 \\ j \text{ even}}} 2^j < \frac{2^{2i}}{5}$$

We conclude that the exponent ℓ appears exactly once the recurrence (6.6); by our previous remarks, it must be the leading exponent.

Case 3: $k \simeq [a, b]$ where k satisfies the assumptions of Lemma 8

Suppose that k satisfies the assumptions of Lemma 8. Then it is not possible to determine the preimage under of $T_3 T_5(\Delta^k)$ under T_3. Luckily, in these cases it is possible to use the recurrence formula to show that

$$T_{[a,b]} \simeq [a, b-1].$$

Although inversion is not well-defined, some information can still be extracted from applying $T_3 T_5$, since the reasoning that led to 6.5 in case 2 still applies here. Thus if $[c, d]$ is the highest exponent in the preimage of $T_3 T_5(\Delta^k)$ under T_3, then either

$$c + d \leq h(k) - 1 \text{ or } c = 0.$$

Let $k \simeq [a, b]$. We now make the extra assumption that $b \neq 2^i$; this will constitute the fourth and final case. Let 2^{2i+2} be the greatest power of 2 in $\mathcal{S}(k)$. Then

$$2^{2i+2} < k < 2^{2i+2} + 2^{2i+1} \quad \Rightarrow \quad k = \sum_{j<2i+2} \beta_j(k) 2^j + 2^{2i+2}$$

where there is at least one even value of $j < 2i + 2$ such that $2^j \in \mathcal{S}(k)$. So we use the 2^{i-1}th iteration of the recurrence:

$$T_{[a,b]} = \Delta^{2\cdot 2^{2i-1}} T_{[a,b]-2\cdot 2^{2i-1}} + \Delta^{4\cdot 2^{2i-1}} T_{[a,b]-4\cdot 2^{2i-1}} + \Delta^{6\cdot 2^{2i-1}} T_{[a,b]-6\cdot 2^{2i-1}} + \Delta^{2^{2i-1}} T_{[a,b]-5\cdot 2^{2i-1}}. \tag{6.7}$$

Let $\ell \simeq [a, b-1]$. We will first show that ℓ appears an odd number of times in the first three terms of the above recurrence.

- Suppose $b \neq 2^i + 2^{i-1}$, i.e. $b \neq 0 \mod 2^{i-1}$. This implies that to obtain $[a, b]$ from $[a, b-1]$, it is not necessary to "borrow" from powers of 2 larger than 2^{2i-1}. So the operations of subtracting 1 from b, and of subtracting and adding large powers of 2 affect disjoint subsets of $\mathcal{S}(k)$, which implies that they commute. So for the three first terms of the recurrence, the quantities subtracted (before applying induction) and added (after applying induction) are equal, we find that the exponent

$$\ell = [a, b - 1]$$

is the highest exponent in all three terms, two of which cancel out.

- When $b = 2^i + 2^{i-1}$, the above argument only applies to $\Delta^{4\cdot 2^{2i-1}} T_{[a,b]-4\cdot 2^{2i-1}}$, whose highest highest is thus ℓ. On the other hand,

  $$[a, b] - 2 \cdot 2^{2i-1} = [a, b - 2^{i-1}] = [a, 2^i] \Rightarrow T_{[a,b]-2\cdot 2^{2i-1}} \simeq [a, 2^i - 1].$$

  This implies that

  $$\Delta^{2\cdot 2^{2i-1}} T_{[a,b]-2\cdot 2^{2i-1}} \simeq [a + 2^i, 2^{i-1} - 1] \prec \ell.$$

  Finally, since

  $$[a, b] - 6 \cdot 2^{2i-1} = [a + 2^i, 0]$$

  we use the slightly stronger lower bound (6.4) that we obtained in case 0, and find that

  $$h(T_{[a,b]-6\cdot 2^{2i-1}})) \le h([a, b]-6\cdot 2^{2i-1})-3 \quad \Rightarrow \quad h(\Delta^{6\cdot 2^{2i-1}} T_{[a,b]-6\cdot 2^{2i-1}}) \le h(k)-3 < h(\ell).$$

  Again, the exponent ℓ appears only once.

- If $k \simeq [2^j, 2^i]$ with $j < i$ then for the first term

  $$[2^j, 2^i] - 2 \cdot 2^{2i-1} = [2^j, 2^i] - 2^{2i} \simeq [2^j, 2^{i-1}].$$

  So

  $$T_{[2^j,2^i]-2\cdot 2^{2i-1}} \simeq [2^j, 2^{i-1}-1] \Rightarrow \Delta^{2\cdot 2^{2i-1}} T_{[2^j,2^i]-2\cdot 2^{2i-1}} \simeq [2^j, 2^{i-1}+2^{i-1}-1] = [2^j, 2^i-1].$$

  So ℓ is the leading term. Next come

  $$[2^j, 2^i] - 4 \cdot 2^{2i-1} = [2^j, 2^i] - 2^{2i+1} \simeq [2^j + 2^i, 0]$$

  So by case 0, the height of $T_{[2^j,2^i]-4\cdot 2^{2i-1}} \simeq [c, d]$ is less than $h(k) - 3$. Moreover, one of two things can happen either $2^i \in \mathcal{S}(c)$ or not. If it is the case, then $[c, d] + 4 \cdot 2^{2i-1} = [c - 2^i, 2^i + d]$, whose height is strictly less than $h(\ell)$. If 2^i is not in $\mathcal{S}(c)$, then the largest $[c, d]$ can be is $[2^i - 1, 2^i - 1]$

It remains to check that ℓ is not an exponent of $\Delta^{2^{2i-1}} T_{[a,b]-5\cdot 2^{2i-1}}$, nor is any higher integer. Recall that by assumption, $b \neq 2^i$, so 2^{2i+2} is not the smallest even power of 2 in $\mathcal{S}(k)$. Since by Lemma 8, the only possible odd power of 2 in $\mathcal{S}(k)$ needs to be smaller than all the even ones, $2^{2i+1} \notin \mathcal{S}(k)$. However,

$$5 \cdot 2^{2i-1} = 2^{2i+1} + 2^{2i-1} \Rightarrow [a, b] - 5 \cdot 2^{2i-1} = [a + 2^i, b - 2^i] - 2^{2i-1}.$$

We now have to check two cases:

- If $2^{2i-1} \in \mathcal{S}(k)$, then
$$[a,b] - 5 \cdot 2^{2i-1} = [2^i, b-2^i].$$
It then follows that
$$T_{[a,b]-5\cdot 2^{2i-1}} \simeq [2^i, b-2^i-1] \Rightarrow \Delta^{2^{2i-1}} T_{[a,b]-5\cdot 2^{2i-1}} \simeq [a+2^i, b-2^i-1] \prec \ell.$$
Since 2^{2i-1} was not contained in $\mathcal{S}(T_{[a,b]-5\cdot 2^{2i-1}})$, the exponent of code $[a+2^i, b-2^i-1]$ is the highest exponent of this term, so ℓ is the highest exponent of $T_{[a,b]}$.

- If If $2^{2i-1} \notin \mathcal{S}(k)$, then
$$[a,b] - 5 \cdot 2^{2i-1} = [a+2^i+2^{i-1}, b-2^i-2^{i-1}] \text{ or } [a+2^{i-1}, b-2^i].$$
Then
$$T_{[a,b]-5\cdot 2^{2i-1}} \simeq [a+2^i, b-2^i-2^{i-1}-1] \text{ or}[a+2^{i-1}, b-2^i-1]$$
or something of lower height. In both cases, the leading term is lower than ℓ.

We have shown that in all cases, $\ell \simeq [a, b-1]$ is the leading exponent of $T_{[a,b]}$. This completes the proof of this section.

Case 4: $k \simeq [2^i, 2^j]$, $i \leq j$.

Here, the goal will be, as in part 0. We want to show that the integer ℓ such that $n_3(\ell) = 0$ and $h(\ell) = h(k) - 1$ is not an exponent in $T_5(\Delta^k)$. The conclusion will be that $T_5T_3(\Delta^k)$ has a unique preimage under T_3, and that the method of case 1 can be applied.

Since $k \simeq [2^i, 2^j]$ for $i \leq j$, then the integer ℓ which we want to show does not appear is
$$\ell \simeq [0, 2^j + 2^i - 1] \quad \Rightarrow \quad \ell = 2^{2j+2} + \sum_{\substack{r=2 \\ r \text{ even}}}^{2i} 2^r.$$

Since $k \geq 2^{2i+2} + 2^{2i+1} = 6 \cdot 2^{2i}$, we use the $2i^{\text{th}}$ iteration of the recurrence
$$T_{[2^i,2^j]} = \Delta^{2\cdot 2^{2i}} T_{[2^i,2^j]-2\cdot 2^{2i}} + \Delta^{4\cdot 2^{2i}} T_{[2^i,2^j]-4\cdot 2^{2i}} + \Delta^{6\cdot 2^{2i}} T_{[2^i,2^j]-6\cdot 2^{2i}} + \Delta^{2^{2i}} T_{[2^i,2^j]-5\cdot 2^{2i}}.$$
We need to show that the exponent ℓ is absent from each term of the recurrence. We start with $T_{[2^i,2^j]-2\cdot 2^{2i}}$.

We have
$$[2^i, 2^j] - 2 \cdot 2^{2i} = [0, 2^j] \simeq 2^{2j+2}.$$
So by the induction hypothesis, the leading term of $T_{[2^i,2^j]-2\cdot 2^{2i}}$ has code $[0, 2^j - 1]$. On the other hand, we note that if ℓ was an exponent in this term, then $\ell - 2 \cdot 2^{2i} = \ell - 2^{2i+1}$ would

be an exponent in $T_{[2^i,2^j]-2\cdot 2^{2i}}$. However,

$$\ell - 2^{2i+1} = \sum_{s=2i+1}^{2j+1} 2^s + \sum_{\substack{r=2\\ r \text{ even}}}^{2i} 2^r = \sum_{\substack{s=2i+1\\ s \text{ odd}}}^{2j+1} 2^s + \sum_{\substack{r=2\\ r \text{ even}}}^{2j} 2^r \simeq \left[\sum_{s=i}^{j} 2^s, \sum_{r=0}^{j-1} 2^r\right] = \left[\sum_{s=i}^{j} 2^s, 2^j - 1\right].$$

So the integer $\ell - 2^{2i+1}$ is higher than the highest possible exponent of $T_{[2^i,2^j]-2\cdot 2^{2i}}$. It follows that ℓ does not appear in this term.

We adopt the same strategy for $T_{[2^i,2^j]-4\cdot 2^{2i}}$. We will show that $\ell - 2^{2i+2}$ cannot be not an exponent in $T_{[2^i,2^j]-4\cdot 2^{2i}}$. We first assume $i < j$ and compute:

$$[2^i, 2^j] - 4 \cdot 2^{2i} = 2^{2i+1} + \sum_{s=2i+2}^{2j+1} 2^s = \sum_{\substack{s=2i+1\\ s \text{ odd}}}^{2j+1} 2^s + \sum_{\substack{r=2i+2\\ r \text{ even}}}^{2j} 2^r \simeq \left[\sum_{s=i}^{j} 2^s, \sum_{r=i}^{j-1} 2^r\right].$$

Applying the induction hypothesis, we get the following code for the leading term of $T_{[2^i,2^j]-4\cdot 2^{2i}}$:

$$T_{[2^i,2^j]-4\cdot 2^{2i}} \simeq \left[\sum_{s=i}^{j} 2^s, \left(\sum_{r=i}^{j-1} 2^r\right) - 1\right] = \left[\sum_{s=i}^{j} 2^s, \sum_{r=i+1}^{j-1} 2^r + \sum_{t=0}^{i-1} 2^t\right].$$

We compare with the code of $\ell - 2^{2i+2}$:

$$\ell - 2^{2i+2} = \sum_{s=2i+2}^{2j+1} 2^s + \sum_{\substack{r=2\\ r \text{ even}}}^{2i} 2^r = \sum_{\substack{s=2i+3\\ s \text{ odd}}}^{2j+1} 2^s + \sum_{\substack{r=2\\ r \text{ even}}}^{2j} 2^r \simeq \left[\sum_{s=i+1}^{j} 2^s, \sum_{r=0}^{j-1} 2^r\right].$$

We find that

$$h(\ell - 2^{2i+2}) = h(T_{[2^i,2^j]-4\cdot 2^{2i}}) \quad \text{but} \quad n_5(\ell - 2^{2i+2}) > n_5(T_{[2^i,2^j]-4\cdot 2^{2i}}).$$

So $\ell - 4 \cdot 2^{2i}$ is higher than the highest exponent of $T_{[2^i,2^j]-4\cdot 2^{2i}}$ thus ℓ is not an exponent of $\Delta^{4\cdot 2^{2i}} T_{[2^i,2^j]-4\cdot 2^{2i}}$.

We now consider the third term $T_{[2^i,2^j]-6\cdot 2^{2i}}$. Again we compute:

$$[2^i, 2^j] - 6 \cdot 2^{2i} = \sum_{s=2i+2}^{2j+1} 2^s = \sum_{\substack{s=2i+3\\ s \text{ odd}}}^{2j+1} 2^s + \sum_{\substack{r=2i+2\\ r \text{ even}}}^{2j} 2^r \simeq \left[\sum_{s=i+1}^{j} 2^s, \sum_{r=i}^{j-1} 2^r\right].$$

We compare with $\ell - 6 \cdot 2^{2i}$:

$$\ell - 6 \cdot 2^{2i} = 2^{2i+1} + \sum_{s=2i+3}^{2j+1} 2^s + \sum_{\substack{r=2\\ r \text{ even}}}^{2i} 2^r = \sum_{\substack{s=2i+1\\ s \text{ odd}}}^{2j+1} 2^s + \sum_{\substack{r=2\\ r \text{ even}}}^{2i} 2^r + \sum_{\substack{t=2i+4\\ t \text{ even}}}^{2j} 2^t \simeq \left[\sum_{s=i}^{j} 2^s, \sum_{r=0}^{i-1} 2^r + \sum_{t=i+1}^{j-1} 2^t\right].$$

We find that

$$h(\ell - 6\cdot 2^{2i}) = h([2^i, 2^j] - 6\cdot 2^{2i})$$

so by induction

$$h(\ell - 6\cdot 2^{2i}) > h(T_{[2^i,2^j]-6\cdot 2^{2i}}).$$

This excluded the possibility that $\ell - 6\cdot 2^{2i}$ is an exponent of $T_{[2^i,2^j]-6\cdot 2^{2i}}$, so ℓ does not appear in $\Delta^{6\cdot 2^{2i}}T_{[2^i,2^j]-6\cdot 2^{2i}}$.

Finally, if ℓ was to appear in the $T_{[2^i,2^j]-5\cdot 2^{2i}}$ term then $\ell - 2^{2i}$ would have to be an exponent in ${}_{[2^i,2^j]-5\cdot 2^{2i}}$. However,

$$[2^i, 2^j] - 5\cdot 2^{2i} = 2^{2i} + \sum_{s=2i+2}^{2j+1} 2^s < 2^{2j+2} < 2^{2j+2} + \sum_{\substack{r=2\\ r \text{ even}}}^{2i-2} 2^r = \ell - 2^{2i}.$$

Since $\ell - 2^{2i}$ is larger than the degree of the polynomial to which we are applying T_5, then it cannot appear as an exponent. This shows that $\ell \simeq [0, 2^j + 2^i - 1]$ is not an exponent in $T_{[2^i,2^j]}$. So we apply T_3 and then T_5 to the polynomial Δ^k where $k \simeq [2^i, 2^j]$. By proposition 3 and the induction hypothesis, the highest term of the resulting polynomial is $[2^i - 1, 2^j - 1]$. Since our discussion excludes ℓ as the possible leading term of $T_5(\Delta^k)$, we find by looking at the possible preimages under T_3 that it must be $[2^i, 2^j - 1]$. □

7 Possibilities or further research

Analogues of "Nicolas-Serre theory"[3] have been pursued in different directions, among others by Bellaiche and Khare for $p > 2$ in [2] and by Monsky for level $N > 1$. A third possible alley of research would be to consider different automorphic forms. A topic could be the study of rings of Hilbert modular forms mod 2. These are generalizations of modular forms defined on the product of two copies of $\mathbb{H}$, quotiented by the action of $PSL_2(\mathcal{O}_K)$ where $\mathcal{O}_K$ is a totally real quadratic number field. Of particular interest could be the field $\mathbb{Q}(\sqrt{5})$, for which it is known that, like in the classical case, there are no systems of eigenvalues for the Hecke operators mod 2. This corresponds to the absence of an irreducible representation or $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{5}))$. One can ask whether or not the nilpotent action of the Hecke operators enjoys properties similar to that of classical modular forms, and whether or not these behave according to a "code".

Other questions concern the algebra $\mathcal{A}$. Let $G_{\mathbb{Q},2}$ be the Galois group of the largest extension of $\mathbb{Q}$ unramified outside of 2 and G its largest pro-2 group. Bellaiche [1] has constructed a two-dimensional representation of G the with values in $\mathcal{A}$ and such that the T_p are the traces of Hecke operators. An open question about this representation is whether or not by taking finite quotients of the image, one can obtain the images of the Galois group of all finite extensions of $\mathbb{Q}$ unramified away from 2 and whose Galois groups are 2-groups. The Frobenian nature of the assignment $p \to a_{ij}(p)$ described in section 3 could also deserve further investigation. Would it be possible, for example, to find a way to compute the extension $K/\mathbb{Q}$ with the property that $a_{ij}(p)$ is determined by the image of the Frobenius at p in $\mathrm{Gal}(K/\mathbb{Q})$?

[3] A term coined, to my knowledge, by Paul Monsky.

References

[1] Joel Bellaiche, *Une représentation Galoisienne universelle attachée aux formes modulaires modulo* 2, C.R. Acad. Sci. Paris, Ser. I 350, 2012.

[2] J. Bellaiche and C. Khare, *Level 1 Hecke Algebras of Modular Forms Modulo* p, preprint.

[3] H. Darmon, *Serre's Conjectures*, CMS conference proceedings, Vol. 17, 2007.

[4] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics **228**, Springer-Verlag, 2005.

[5] K. Hatada, *On the Divisibility by* 2 *of the Eigenvalues of Hecke Operators*, Proceedings of the Japan Academy Ser B, Vol. 53, No. 1, 1977.

[6] J.-L. Nicolas et J.-P. Serre, *Formes modulaires modulo 2: Ordre de nilpotence des opérateurs de Hecke*, C.R. Acad. Sci. Paris, Ser. I 350, 2012.

[7] J.-L. Nicolas et J.-P. Serre, *Formes modulaires modulo 2: Structure de l'algèbre de Hecke*, C.R. Acad. Sci. Paris, Ser. I 350, 2012.

[8] J.-L. Nicolas et J.-P. Serre, *Formes modulaires modulo 2: Ordre de nilpotence des opérateurs de Hecke modulo 2 (document de travail n^o 7)*, preprint, December 17, 2012.

[9] J.P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics **7**, Springer-Verlag, 1973.

[10] J.P. Serre, *Sur les représentations modulaires de degré 2 de Gal*$(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Mathematical Journal, Vol. 54, No. 1, 1987.

[11] J. Tate, The Non-Existence of Certain Galois Extensions of $\mathbb{Q}$ Unramified Outside 2, Contemporary Mathematics, Vol. 174, 1974.

[12] G. Wiese, *Galois Representations*, version of 13$^{\text{th}}$ of February 2012, available online at `maths.pratum.net`.