

Theoretical and algorithmic aspects
of congruences between modular
Galois representations

Xavier Taixés i Ventosa

Dissertation

Theoretical and algorithmic aspects
of congruences between modular
Galois representations

Dissertation zur Erlangung des Grades
eines Doktors der Naturwissenschaften

Dem Fachbereich 6
(Mathematik und Informatik)
der Universität Duisburg-Essen

vorgelegt von

Xavier Taixés i Ventosa
aus Barcelona

Barcelona, 14. April 2009

Tag der Disputation:

Prüfungsvorsitzender:

1. Gutachter: Prof. Dr. Dr. h.c. Gerhard Frey
2. Gutachter: Prof. Dr. Luis Dieulefait

Hiermit erkläre ich, dass ich diese Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen verwendet habe.

Xavier Taixés i Ventosa
Barcelona, 14. April 2009

A la meva àvia Angelina.

Agraïments

Primer de tot, és un plaer agrair sincerament al meu director de tesi, el Prof. Dr. Dr. h.c. Gerhard Frey, per l'oportunitat que m'ha brindat de treballar amb ell, així com per la seva inestimable ajuda, mestratge, guia i paciència a l'hora de realitzar aquest treball. Per les hores i l'esforç infinit que m'ha dedicat, així com per les converses plenes d'idees que m'han fet endinsar al món de la recerca, i m'han ajudat a descobrir un fragment tan meravellós de la teoria de nombres.

A tots els companys de l'IEM i de la Universität Duisburg-Essen els dec la sort d'haver trobat un magnífic ambient de treball. Vull mencionar particularment al Dr. Enric Nart, Dr. Roberto Avanzi, Dra. Tanja Lange, Dr. Roger Oyono, Dr. Christophe Ritzenthaler, Dra. Irene Bouw, Dr. Guido Blady, Dr. Wolfgang Happle, Dr. Gebhard Böckle, Ralf Butenuth, Dr. Alp Bassa, Dr. Claus Diem, Björn Buth, Marco Wolter, Marios Magioliditis, Julia Thiemann, Anil Mengi, Ira Terwyen i en general a tot el personal de l'Akademisches Auslandsamt. D'un forma molt especial, vull donar les gràcies també al Dr. Gabor Wiese per les nombroses hores de discussions, contribucions i correccions que ha fet en aquest treball.

Vull agrair també a tot el Grup de Teoria de Nombres de Barcelona el suport rebut cada vegada que ho he necessitat, i molt especialment al Dr. Luis Dieulefait per les innombrables hores de discussions i intercanvi d'idees. Vull fer també una menció especial a la Dra. Pilar Bayer, per haver-me encoratjat a anar a la meravellosa Alemanya, així com també vull agrair la seva ajuda i la del Dr. Artur Travesa a l'hora de sol·licitar la beca que em va permetre iniciar aquest projecte. De la mateixa manera, vull agrair a la Hanna, en Pep i la Sandra la traducció a l'alemany de tota la (no poca) documentació que vaig necessitar per demanar aquesta beca.

El finançament d'aquest projecte s'ha degut parcialment gràcies a la beca de "la Caixa" en col·laboració amb el DAAD. Vull fer constar el meu agraïment a sengles entitats, així com a la Rosa Ma. Molins i a la Ma. Teresa Torrents per la meravellosa atenció rebuda. També dec als projectes europeus ECRYPT i GTEM, i al "Graduiertenkolleg" „Mathematische und ingenieurwissenschaftliche Methoden der sicheren Datenübertragung" part del sosteniment econòmic rebut.

Vull fer també menció dels nombrosos amics d'arreu del món que he fet durant aquests anys, i que em faran guardar un record inoblidable d'aquest període. Una menció destacada va per la Laia, la Marcia, el Jarek, i per les

Agraïments

meves companyes de pis; especialment per la Sabine, per tots els problemes que m'ha ajudat a resoldre, per les seves classes gratuïtes d'alemany, i pel seu sempre tracte afable diari. A la Sarah li vull donar també les gràcies per la seva ajuda en la traducció i correcció desinteressada d'aquest text.

Finalment, vull agrair molt especialment:

- Al Jordi, per les nombroses correccions, ajudes de programació i de \LaTeX , i en general per haver estat durant molts anys un referent que ha anat obrint camí a la meva vida.
- Als pares, perquè tot i que sembli un tòpic, tot el que sóc ho dec a ells, i aquest treball no és més que un fruit, una conseqüència natural del camí pel que m'han portat.
- A l'Ariadna, per ser sempre i malgrat la distància al meu costat. Pel constant esperonament, en la tesi, en el treball i en la relació. Perquè si hem superat això, podem enfrontar-nos a qualsevol cosa.

A tots quatre, us estimo.

Danksagung

An erster Stelle möchte ich meinen aufrichtigen Dank für meinen Doktorvater, Herrn Prof. Dr. Dr. h.c. Gerhard Frey, ausdrücken, der mir die Gelegenheit bat, mit ihm zu arbeiten, und mir mit seiner unschätzbaren Hilfe geduldig zur Seite stand. Ihm gebührt der Dank für die vielen Stunden und unendlichen Mühen, die er mir widmete, sowie für die lehrreichen Gespräche, die es mir ermöglichten, in die Forschungswelt einzutauchen und einen sehr interessanten Teil der Zahlentheorie kennen zu lernen.

Allen Mitarbeitern des IEM sowie der Universität Duisburg-Essen danke ich für das großartige und sehr angenehme Arbeitsklima. Im Besonderen bedanke ich mich bei Prof. Dr. Enric Nart, Prof. Dr. Roberto Avanzi, Prof. Dr. Tanja Lange, Dr. Roger Oyono, Dr. Christophe Ritzenthaler, Prof. Dr. Irene Bouw, Dr. Guido Blady, Dr. Wolfgang Happle, Prof. Dr. Gebhard Böckle, Ralf Butenuth, Dr. Alp Bassa, Prof. Dr. Claus Diem, Björn Buth, Marco Wolter, Marios Magioladitis, Julia Thiemann, Anil Mengi, Ira Terwyen und generell beim Personal des Akademischen Auslandsamtes. Besonders möchte ich meinen Dank Prof. Dr. Gabor Wiese für die zahlreichen Stunden an Diskussionen sowie für seine Verbesserungsvorschläge und Beiträge zur Doktorarbeit ausdrücken.

Dankbar anerkennen will ich mich auch bei der Arbeitsgruppe Zahlentheorie Barcelonas für die Unterstützung, die sie mir anboten, wenn immer ich sie brauchte, und speziell bei Prof. Dr. Luis Dieulefait für die unzählbaren Stunden an Diskussionen und Inspirationen. Ferner möchte ich mich bei Prof. Dr. Pilar Bayer für die Ermutigung, an eine Universität im wunderschönen Deutschland zu promovieren, sowie für ihre und Prof. Dr. Artur Travesas Hilfe bei der Bewerbung eines Stipendiums bedanken, das mir den Anfang dieses Projektes ermöglichte. Auf dieselbe Weise sei Hanna, Pep und Sandra gedankt, die bei der Übersetzung ins Deutsche aller (nicht wenigen) Dokumente, die ich für die Bewerbung dieses Stipendiums brauchte, ausnehmend hilfreich waren.

Die Finanzierung dieses Projektes ermöglichten mir teilweise das Stipendium der “la Caixa” in Zusammenarbeit mit dem DAAD. Desweiteren gebührt mein Dank Rosa Ma. Molins und Ma. Teresa Torrents für die großzügige Hilfsbereitschaft sowie den europäischen Projekten ECRYPT und GTEM und dem Graduiertenkolleg „Mathematische und ingenieurwissenschaftliche Methoden der sicheren Datenübertragung” für die ökonomische Unterstützung.

Danksagung

Weiterhin möchte ich meine zahlreichen Freundschaften aus aller Welt erwähnen, die ich in diesen Jahren geschlossen habe, und die mir als unvergessliche Zeit in Erinnerung bleiben. Auch möchte ich an dieser Stelle Laia, Marcia, Jarek und meine Mitbewohnerinnen nennen; insbesondere aber Sabine, die mir bei der Lösung von Problemen hilfreich war, mir kostenlosen Deutschunterricht erteilte und immer Freude und gute Stimmung verbreitete. Außerdem möchte ich mich bei Sarah für ihre ehrenhafte Hilfe bei der Übersetzung und Korrektur dieses Textes bedanken.

Zuletzt möchte ich mein herzliches Dankeschön ausrichten an:

- Jordi, für die zahlreichen Korrekturen und Hilfen beim Programmieren sowie Lösungen, die er parat hatte, wenn sich \LaTeX weigerte, meinem Willen zu folgen; und generell, weil er mich während meines Reifeweges als Vorbild lenkte.
- Meine Eltern, weil sie mir zu dem verhalfen, der ich heute bin, und diese Arbeit nichts anderes ist, als die Frucht ihrer elterlichen Fürsorge, mich in diesen Weg zu leiten.
- Ariadna, die mir trotz der Entfernung immer zur Seite stand. Sie ermutigte mich bei der Doktorarbeit und in sämtlichen Herausforderungen und trug dazu bei, unsere Beziehung aufrechtzuerhalten und zu festigen. Wir haben es gemeinsam geschafft, diese Zeit zu überwinden, deshalb können wir uns auch jeglicher anderen Situation stellen.

Ihr vier liegt mir sehr am Herzen.

Contents

Agraiments	ix
Danksagung	xi
0 Introduction	1
0.1 Motivations	2
0.2 Contents	3
1 Necessary background	7
1.1 Introduction to modular curves and modular forms	7
1.2 Introduction to representations	12
1.3 Conductor of a representation	14
1.4 Representations attached to modular forms	16
1.5 Representations on Hecke algebras	22
1.6 Abelian varieties of GL_2 -type and Serre's Conjecture	25
1.7 Congruences between modular forms	25
2 Algorithms to compute congruences modulo ℓ^n	29
2.1 Congruences modulo ℓ^n	30
2.2 Local problem	31
2.3 Global problem	32
2.4 Global upper bound	33
2.5 Local congruence number	35
2.6 $Q_{f,p}$	37
2.7 Improving the global upper bound	38
2.8 pBound	39
2.9 Description of UpperBound1.0	41
2.10 Congruences between f and $\sigma(f)$	44

Contents

2.11	Global lower bound I: Hecke Bound	46
2.12	Global lower bound II	48
2.13	Description of <code>LowerBound1.0</code>	50
2.14	L^+ vs. L^- and other results	52
2.15	Heuristic realization of Galois Groups	54
3	Deformation Theory and lowering the level modulo ℓ^n	57
3.1	Main results	58
3.2	Deformation theory	61
3.3	Proof of Theorem 3.1.3	64
3.4	Examples	65
	Further work	69
A	<code>UpperBound1.0.res</code>	73
B	Congruences with conjugates	77
C	Theorem 3.1.3	81
	Bibliography	85
	Glossary of Notations	91
	Index	97

Chapter 0

Introduction

The study of Galois representations has been a central research field in Number Theory and Arithmetic Geometry during the last half century—especially since 1994, when Andrew Wiles proved Fermat’s Last Theorem ([Wil95]) using, among others, Deformation Theory and the relationship that G. Frey established between the Theorem and the Taniyama-Shimura Conjecture.

Research on Galois representations goes back to the study of the absolute Galois group $G_{\mathbb{Q}}$ and, particularly, its structure. Given a ring (in fact, usually a topological field) \mathcal{R} , we would like to obtain as much information as possible about the linear representations $\rho : G_{\mathbb{Q}} \rightarrow GL_n(\mathcal{R})$, for any integer n . Although the topic has been subject to research for many years now, the work is still at an early stage: until now only the case $n = 1$ is completely solved, and the case $n = 2$ has been thoroughly studied.

One direct application of such research is the study of the Galois inverse problem. That is, given a finite group \mathcal{G} , it has been conjectured that there exists a field having \mathcal{G} as Galois group over \mathbb{Q} . Among the most remarkable contributions towards a solution for this problem, we find the partial results given by Galois representations, which confirm affirmatively several cases by studying the images of the representations. The idea is the following: Given a group \mathcal{G} , if we can find a Galois representation such that its image is precisely \mathcal{G} , then the Isomorphism Theorem affirms that \mathcal{G} is a quotient of the absolute Galois group, and therefore is itself a Galois group. This fact reveals the determination of images of Galois representations as one of the current crucial problems in Number Theory.

Galois representations research applications do not only concern the Galois group, but also many other problems, such as the aforementioned Fermat’s

Last Theorem—probably the most representative example. It was not until 1986, when G. Frey proposed the relationship between some solution of the Fermat equation $a^n + b^n = c^n$, the elliptic curve $y^2 = x(x - a^n)(x + b^n)$ and the Taniyama-Shimura Conjecture, that Galois representations ever played a rôle in the proof of this problem that had remained unsolved for more than 300 years.

Yet another classical problem, *a priori* not directly related to Galois representations but that could also be attacked using their techniques, is the so-called ABC Conjecture:

Conjecture 0.0.1 (ABC-conjecture [Oes88]). *Let $\text{rad}(n)$ denote the radical of n , this is, the product of all prime numbers dividing n . For every $\epsilon > 0$, there exists a constant $C(\epsilon)$ such that*

$$c \leq C(\epsilon)(\text{rad } abc)^{1+\epsilon}$$

for every triple (a, b, c) of positive integers, such that they verify $a + b = c$.

This conjecture was stated by Joseph Oesterlé and David Messer in 1985. In [Fre01] some generalizations of these (and many other related) conjectures are studied.

In this case, the study of congruences between modular Galois representations might provide a key tool for a better understanding of the behaviour of the conjecture.

Today, the field of Galois representations is a dynamic one, specially in Deformation Theory. In particular, recent improvements developed over the last few years—among which L. Dieulefait’s, C. Khare’s and J. P. Wintenberger’s are worth mentioning—, allowed to prove Serre’s celebrated conjecture in 2007.

0.1 Motivations

Let N be an integer and let A_1 and A_2 be two non-isogenous \mathbb{Q} -simple Abelian subvarieties of $J_0(N)$. Then it is known that $A_1 \cap A_2 \subset J_0^{\text{Tor}}(N)$. With these conditions, we ask ourselves the following question.

Question 0.1.1. *Depending on N , how big can $A_1 \cap A_2$ actually be?*

In other words: For every m , we would like to determine all the different groups $C \subset (A_1 \cap A_2)[m]$. We know that there exist two newforms f and g that provide A_1 and A_2 as their Shimura constructions (see §1.1). Then, searching subgroups C as mentioned above is equivalent to searching common representation spaces modulo m of the torsion point representations of f and g .

In fact, this can be reduced to the study of the cases where m is a power of a prime, ℓ^n . Then, given a place $\lambda \mid \ell$ and calling $\bar{\rho}_{f,\lambda^n}$ the representation modulo λ^n attached to f , Question 0.1.1 can be reformulated as:

Question 0.1.2. *Let f and g be two different newforms. For every prime ℓ , which is the largest $n := n(\ell)$ such that there exists a place $\lambda \mid \ell$ with*

$$\bar{\rho}_{f,\lambda^n} \sim \bar{\rho}_{g,\lambda^n}?$$

Now let λ be a place such that $\bar{\rho}_{f,\lambda} \sim \bar{\rho}_{g,\lambda}$, and let $n \geq 1$ be the exponent defined in Question 0.1.2. The following natural question is:

Question 0.1.3. *If $\bar{\rho}_{f,\lambda^n} \sim \bar{\rho}_{g,\lambda^n}$ and $\bar{\rho}_{f,\lambda^{n+1}} \not\sim \bar{\rho}_{g,\lambda^{n+1}}$, what does actually force the representations modulo λ^{n+1} not to be equivalent any more?*

In other words, we would like to determine subrepresentations of the representations modulo λ^{n+1} that happen to be non-equivalent.

0.2 Contents

In this thesis we examine a number of cases in which the Questions posed above can be answered. In the whole work (except just in some definitions in Chapter 1) we will deal with normalized newforms of weight 2 without nebentypus. Whenever we work with congruences between two modular forms f and g of respective levels N_f and N_g ($N_f \geq N_g$), we will assume $N_g \mid N_f$. Such assumption is not too restrictive, since for g minimal and irreducible in a prime ℓ , and f and g congruent modulo λ (with $\lambda \mid \ell$), Ribet's lowering the level provides a modular form of level dividing both N_f and N_g which is congruent modulo λ with f and g .

In Chapter 1 we give some basic background and tools, to be used in the following chapters. We give the basic definitions of modular forms, Hecke algebras, representations and, to every newform, we attach different kinds of representations. Then, we define the concept of congruent representations

and finally state Serre's conjecture, which will allow us to apply the work developed in the next chapters to all Abelian varieties of GL_2 -type.

In Chapter 2 we develop some algorithms to give an answer to Question 0.1.2 above. This chapter served as an inspiration for a joint work with Gabor Wiese ([TW09]), and it owes some of the results to it.

All our algorithms will be based on computations with the characteristic polynomials Q_p of the eigenvalues of the Hecke operators of the newforms to be compared (§2.6). Thus, our very first task is merely to compute a huge database containing all these polynomials up to some prescribed order—namely we compute the polynomials for all newforms of level $N \leq 2000$ and all primes $p < 1000$.

Given two different newforms, in §2.4 we will use the resultant of the pre-computed polynomials to compute a finite set $\{\ell_1^{n_1}, \dots, \ell_s^{n_s}\}$ containing all possible congruences between f and g (i.e. if $\ell^n \nmid \ell_1^{n_1} \cdot \dots \cdot \ell_s^{n_s}$, then there exists no congruence between f and g modulo λ^n , for any $\lambda \mid \ell$):

Lemma 0.2.1. *If f and g are congruent modulo λ^n , then ℓ^n divides the resultant of every couple $P_{f,p}$ and $P_{g,p}$, $p \nmid \ell N_f$.*

This result is not optimal, nevertheless it suggests the idea to define the local congruence number (§2.5), which will provide an algorithm to get a better upper bound L^+ than the one computed with the resultants (§§2.7–2.9).

Our next algorithm will find an upper bound (in sense described above) for congruences between a given newform f and its conjugates $\sigma(f)$ (§2.10).

Next step is to find an algorithm to determine a lower bound for congruences between modular forms (§2.13). In other words, we will get a number L^- such that if ℓ^n divides L^- , f and g are congruent modulo ℓ^n .

To develop this algorithm we will have to introduce first two results: applying the Hecke bound (§2.11) and an idea of Gabor Wiese (§2.12).

We finish this chapter giving some examples that compare upper bound algorithms with the lower bound one and we see that in many cases we obtain that $L^- = L^+$ and thence our algorithms do determine all congruences between the tested modular forms.

Chapter 3 is based on a joint work with Luis Dieulefait ([DT09]). The main result (§3.1) answers Question 0.1.3 in some cases.

Theorem 0.2.2. *Let $\ell, p \nmid N_g$, $\ell > 2$ be two different prime numbers. Let f be in $S_2(p^k N_g)$, $k \geq 1$, and let $g \in S_2(N_g)$ be minimal with respect to λ . Let $\bar{\rho}_{f, \lambda^n}$ be the representation modulo λ^n attached to f . Suppose that*

$\bar{\rho}_{f,\lambda} \sim \bar{\rho}_{g,\lambda}$ and that they are irreducible, and assume that for any other $h \in S_2(N_g)$, $\bar{\rho}_{g,\lambda} \not\sim \bar{\rho}_{h,\lambda}$. If $\ell = 3$, let $L = \mathbb{Q}(\sqrt{-3})$ and suppose that $\bar{\rho}_{g,\lambda}|_{G_L}$ is irreducible. Then,

$$m := \min\{n \in \mathbb{N} : \bar{\rho}_{f,\lambda^n} \approx \bar{\rho}_{g,\lambda^n}\} = \min\{n \in \mathbb{N} : \bar{\rho}_{f,\lambda^n}|_{\mathcal{I}_p} \approx \bar{\rho}_{g,\lambda^n}|_{\mathcal{I}_p}\}.$$

In the case of this theorem, then, we can assert that the reason for f and g not to be congruent any more is that the p -inertia modulo λ^m does not vanish as it did for λ^{m-1} . This can be reread also as a generalization of Ribet's Lowering the Level.

Using Theorem 0.2.2 we can give two corollaries which tell how the image of the p -inertia of the representation on f must look like. These results can be applied to determine images of Galois representations.

In the next section (§3.2) we introduce the necessary terminology about deformation theory to prove this theorem, and it follows (§3.3) the proof of Theorem 0.2.2.

Finally we will give some examples—computed with the algorithms from Chapter 2—of couples of newforms satisfying the conditions of the theorem as well as ones of the corollaries.

Due to the nature of the first chapter, the knowledge of its content is indispensable to understand the following parts of the work. Chapter 2 and 3 can be read independently but they complement each other being the algorithms of the former an easy way to find examples for the latter.

The last chapter is a brief description of possible expansions and improvements of the work developed in this thesis.

In appendices A-C we give lists of some of the most interesting results obtained with our algorithms.

The complete lists of results and the codes of the algorithms can be found in <http://www.iem.uni-due.de/~xavier/thesis>.

Chapter 1

Necessary background

In this chapter we introduce the concepts we use in the whole work. First of all, we define and describe the most general properties of modular forms, newforms and Hecke algebras, and we show the Abelian variety associated to a modular form by the Shimura construction. In the next two sections we give the definition of a representation, we describe its most important types and we define the notion of conductor of a representation. It follows the construction of some of these kinds of representations coming from the Tate-module of an Abelian variety. Then, we give some constructions of representations attached to Hecke algebras and we see in which cases the representations of these two sections coincide. Finally, we define the concept of Abelian variety of GL_2 type, we state Serre's Conjecture and we introduce congruences between modular forms.

[DDT97] has been the source of many of the definitions of this chapter.

1.1 Introduction to modular curves and modular forms

It is well known that the group $SL_2(\mathbb{Z})$ acts by linear fractional transformations on the completed complex upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{i\infty\}$, where $\mathbb{Q} \cup \{i\infty\}$ are the cusps. If $\gamma \in SL_2(\mathbb{Z})$, $\gamma(z)$ is given by

$$\gamma(z) = \frac{az + b}{cz + d} \in \mathcal{H}^*$$

for every $z \in \mathcal{H}^*$.

Let N be a positive integer. The **modular group** $\Gamma_0(N)$ is defined as

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Given a positive integer N , with the action described above we can define the **modular curve** over \mathbb{C} of $\Gamma_0(N)$ as

$$X_0(N)_{\mathbb{C}} := \Gamma_0(N) \backslash \mathcal{H}^*$$

which is a Riemann Surface.

We want to define the Hecke Operators over this curve in a geometrical point of view in the same way as in [Fre94].

$X_0(N)_{\mathbb{C}}$ has a moduli interpretation in the following sense: for a given z in \mathcal{H} , the $\Gamma_0(N)$ -orbit of z corresponds to the complex torus $E := \mathbb{C} / \langle 1, z \rangle$ with the cyclic subgroup of order N generated by $1/N$. Every point of $X_0(N)_{\mathbb{C}}$ can be seen as a \mathbb{C} -isomorphism class of pairs (E, C_N) , where E is an elliptic curve defined over \mathbb{C} and a C_N is a cyclic group of order N . Then it follows that this curve comes from an extension of a curve $X_0(N)$ defined over \mathbb{Q} . In [DR73] it can be seen that this curve is also defined over \mathbb{Z} .

Now let $n \in \mathbb{N}$ be coprime with N . We can define the maps α_n and β_n from $X_0(nN)$ to $X_0(N)$ as follows: given an extension K of \mathbb{Q} , let y be the point of $X_0(nN)(K)$ corresponding to the isomorphism class of (E, C_{nN}) . Then

$$\alpha(y)_n := \text{isomorphism class of } (E, nC_{nN}) \in X_0(N)(K)$$

and

$$\beta(y)_n := \text{isomorphism class of } (E/N \cdot C_{nN}, C_{nN}/NC_{nN}) \in X_0(N)(K).$$

The maps α_n and β_n induce homomorphisms $\alpha_n^* : J_0(N) \rightarrow J_0(nN)$ and $(\beta_n)_* : J_0(nN) \rightarrow J_0(N)$ by Pic functoriality and Albanese functoriality, respectively.

Definition 1.1.1. *Using the \mathbb{Q} -morphisms α_n^* and $(\beta_n)_*$ we can define the n -th **Hecke operator** as*

$$T_n = (\beta_n)_* \circ \alpha_n^*$$

which is a \mathbb{Q} -rational correspondence on divisor classes of $X_0(N)$.

T_n induces endomorphisms on the Jacobian $J_0(N)$ of $X_0(N)$.

Now we will introduce some basic definitions concerning modular forms.

Definition 1.1.2. *Let N and k be a positive integers. A **modular form** of weight k and level N on $\Gamma_0(N)$ is a holomorphic function f on \mathcal{H} satisfying:*

- **Transformation property:** $f(\gamma z) = (cz + d)^k f(z)$ for all $\gamma \in \Gamma_0(N)$,
- **Behaviour at the cusps:** f has holomorphic continuation to \mathcal{H}^* .

If f vanishes at every cusp, we will call f a **cuspidal form**.

We denote by $M_k(N)$ (resp. $S_k(N)$) the complex vector space of modular forms (resp. cusp forms) of weight k on $\Gamma_0(N)$.

Let $f \in M_k(N)$, since $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$, then $f(z + 1) = f(z)$. Hence f has a Fourier expansion at the cusp $i\infty$ of the form

$$f(z) = \sum_{n=0}^{\infty} a_n q^n, \text{ where } q = e^{2\pi iz} \text{ and } a_n \in \mathbb{C}.$$

For a given f , we will denote the n -th coefficient by $a_n(f)$ or simply a_n when f is clear by the context. If f is a cusp form, then $a_0 = 0$.

Remark 1.1.3. *Let $S_k(\Gamma, \mathbb{Z})$ be the space of modular forms of $S_k(\Gamma)$ with integral coefficients, and in general $S_k(\Gamma, \mathcal{R}) = S_k(\Gamma, \mathbb{Z}) \otimes \mathcal{R}$. We describe some properties concerning Hecke operators and modular forms.*

- T_n defined before induces endomorphisms on $M_k(N)$ and $S_k(N)$.
- $T(N) := \mathbb{Z}[T_n \in \text{End}(S_k(N)) : n \in \mathbb{N}, n \text{ prime to } N]$ is the **Hecke algebra of level N** . We will write it simply \mathbb{T} when N is clear by the context.
- For every N , \mathbb{T} is a finitely generated \mathbb{Z} -module.
- \mathbb{T} is commutative and $T_n \circ T_m = T_{nm}$ for $(n, m) = 1$, and

$$T_{p^n} = \begin{cases} T_p T_{p^{n-1}} - p^{k-1} T_p^{n-2} & p \nmid N \\ T_p^n & p \mid N. \end{cases}$$

- If $f(z) = \sum_{n=0}^{\infty} a_n q^n \in M_k(N)$ and $p \nmid N$, then $T_p(f) = \sum_{n=0}^{\infty} b_n q^n$, where $b_n = (a_{pn} + p^{k-1} a_{n/p})$ and $a_{n/p} = 0$ if $p \nmid n$.
- Let \mathcal{R} be an arbitrary ring. We define $\mathbb{T}_{\mathcal{R}}$ to be the \mathcal{R} -algebra $\mathbb{T} \otimes \mathcal{R}$. For $\mathcal{R} = \mathbb{Z}_{\ell}$ we will simply write $\mathbb{T}_{\mathbb{Z}_{\ell}}$ as \mathbb{T}_{ℓ} . Given a place $\lambda \mid \ell$, \mathbb{T}_{λ} will denote $\mathbb{T}_{\mathcal{O}_{\lambda}}$.

J. Basmaji [Bas96] and G. Blady [Bla07] give efficient algorithms to compute Hecke operators explicitly.

Definition 1.1.4. A modular form f is an **eigenform** if it is simultaneously an eigenvector for all Hecke operators (i.e. $T_n(f) = \lambda_n f$, $\lambda_n \in \mathbb{C}$ for every $n \in \mathbb{N}$, $(n, N) = 1$).

Let M be a positive divisor of N and d a positive divisor of N/M . The automorphism in \mathcal{H} defined by $z \mapsto d \cdot z$ induces a non-constant morphism $t_{M,d} : X_0(N) \rightarrow X_0(M)$. If $f(z) \in S_k(M)$ and $M \mid N$, then $f(dz) \in S_k(N)$ for $d \mid \frac{N}{M}$. We then define

$$S_k^{\text{old}}(N) := \langle f(dz) : f(z) \in S_k(M) \text{ with } M \mid N, M \neq N, d \mid \frac{N}{M} \rangle$$

the space of **old forms** of $S_k(N)$. We denote it by S_k^{old} when N is clear by the context.

Definition 1.1.5. We call **new space** the orthogonal complement space $S_k^{\text{new}}(N)$ of S_k^{old} with respect to the **Petersson scalar product**

$$\langle f, g \rangle := \int_{X_0(N)} f(z) \overline{g(z)} dx dy \text{ with } f, g \in S_k(N); z = x + yi.$$

A **newform** is an element of S_k^{new} which is simultaneously an eigenform.

Remark 1.1.6. Some interesting properties of newforms:

- S_k^{new} and S_k^{old} are invariant under the Hecke operators.
- S_k^{new} admits a basis of eigenfunctions of T_p , $p \nmid N$.
- Every eigenform $f \in S_k^{\text{new}}$ can be **normalized** and admits a Fourier expansion with the form $f(z) = q + \sum_2^{\infty} a_n q^n$, $q = e^{2\pi iz}$.

From now on, we will focus to modular forms which are normalized newforms.

Remark 1.1.7. *During the whole work, we will sort the elements of the basis of S_2^{new} with the `SortDecomposition` function of Magma [BCP97]. So, every time we give a level and an integer (N, i_N) , we are determining explicitly the i -th newform of level N . Given a modular form f , we will write also (N_f, i_f) for (N_f, i_{N_f}) .*

Theorem 1.1.8. *Let $f(z) = q + \sum_{n=2}^{\infty} a_n q^n$ be a newform. The field $K_f := \mathbb{Q}(a_2, \dots)$ generated by all the coefficients of f is a finite extension of \mathbb{Q} .*

Proof. We know that \mathbb{T} is a finitely generated \mathbb{Z} -module. If we take the morphism

$$\begin{aligned} \varphi_f : \mathbb{T}_{\mathbb{Q}} &\rightarrow \mathbb{C} \\ T_n &\mapsto a_n(f) \end{aligned}$$

the image of φ_f is K_f . Therefore $K_f = \mathbb{T}_{\mathbb{Q}} / \ker \varphi_f$, which is a finitely generated \mathbb{Q} -vector space. \square

Now we want to introduce Shimura's construction [Shi73] of abelian varieties arising from modular forms.

Theorem 1.1.9 (G. Shimura). *For every newform $f(z) = q + \sum_{n=2}^{\infty} a_n q^n \in S_2^{\text{new}}$ there exist an abelian subvariety A_f of $J_0(N)$ and an isomorphism from K_f to $\text{End}(A_f) \otimes \mathbb{Q}$ with*

1. $\dim(A_f) = [K_f : \mathbb{Q}]$,
2. A_f is defined over \mathbb{Q} and it is \mathbb{Q} -simple.

Let f be an eigenform with the Fourier coefficients corresponding to a surjective algebra homomorphism $\varphi_f : \mathbb{T}_{\mathbb{Q}} \rightarrow K_f$. Then Shimura constructs the variety A_f as the quotient

$$A_f = J_0(N) / I_f J_0(N)$$

where $I_f \subset \mathbb{T}$ is the ideal $\ker(\varphi_f) \cap \mathbb{T}$.

In particular, we have the diagram

$$\begin{array}{ccc}
 A_f^* & \subset & J_0(N) \\
 & \searrow^{\phi^*} & \downarrow^{\phi_*} \\
 & \simeq & A_f
 \end{array} \tag{1.1}$$

where A_f^* is the dual variety of A_f . Since $J_0(N) \otimes \mathbb{Z}[\frac{1}{N}]$ is an abelian scheme, we get the following result:

Theorem 1.1.10. *Let f be an eigenform of level N and $p \nmid N$ a prime. Then A_f has good reduction at p .*

Remark 1.1.11. *When $\dim(A_f) = 1$ we will denote the variety by E and it is an **elliptic curve**.*

1.2 Introduction to representations

Definition 1.2.1. *Let \mathcal{G} be a topological group, \mathcal{R} a \mathcal{G} -module and V a free \mathcal{R} -module. A **linear representation** of \mathcal{G} over \mathcal{R} is a continuous homomorphism with respect to the Krull topology on \mathcal{G}*

$$\rho : \mathcal{G} \longrightarrow \text{Aut}(V) \simeq GL_n(\mathcal{R}).$$

We say that ρ is **simple** or **irreducible** if V is a simple $\mathcal{R}[\mathcal{G}]$ -module (equivalently, if ρ has no nontrivial invariant subspaces). If V is a direct sum of simple \mathcal{G} -modules, $V = \bigoplus V_i$, ρ is **semi-simple**.

Theorem 1.2.2 (Brauer-Nesbitt). *If ρ is semi-simple and $\mathcal{R} = K$ is a field, ρ is determined up to isomorphism by the characteristic polynomial of all the images.*

Proof. [CR62], (30.16), p.215. □

From now on, we will take \mathcal{G} as the absolute Galois group $\mathcal{G} = G_{\mathbb{Q}}$ with the Krull (profinite) topology. In this case, ρ is called a **Galois representation**.

We call ρ **odd** if $\det(\rho(c)) = -1$, where c is any complex conjugation.

Let p be a prime and \mathfrak{p} a place in $\overline{\mathbb{Q}}$ such that $\mathfrak{p} \mid p$. We denote $\mathcal{I}_{\mathfrak{p}} \subset G_{\mathbb{Q}}$ the inertia group attached to \mathfrak{p} . Then we say that ρ is **unramified** at p if $\rho(\mathcal{I}_{\mathfrak{p}}) = \{\mathbf{1}\}$ for all $\mathfrak{p} \mid p$.

If ρ is unramified at p , we denote $\rho(\text{Frob}_p)$ the image of a p -Frobenius element by the representation ρ . It is an element defined up to conjugation. We denote then

$$\begin{aligned} P_{\rho,p}(X) &:= \det(X \cdot \mathbf{1} - \rho(\text{Frob}_p)) = \\ &= X^n - \text{tr}(\rho(\text{Frob}_p))X^{n-1} + \dots + (-1)^n \det(\rho(\text{Frob}_p)) \end{aligned}$$

It is interesting to describe some different Galois representations, depending on the $G_{\mathbb{Q}}$ -module \mathcal{R} on Definition 1.2.1.

- When $\mathcal{R} = \mathbb{C}$ with the discrete topology, ρ is called an **Artin representation**. Since $\rho(G_{\mathbb{Q}})$ is compact ($G_{\mathbb{Q}}$ is compact) and \mathbb{C} is equipped with the discrete topology, $\rho(G_{\mathbb{Q}})$ is finite. By *Maschke's Theorem* ([Lan84], p.641), ρ is semi-simple and unramified at all but finitely many primes.
- If \mathcal{R} is the ring $\mathbb{Z}/\ell^n\mathbb{Z}$ for a prime ℓ and $n \geq 1$, we call ρ a **mod ℓ^n representation**. Obviously, $\rho(G_{\mathbb{Q}})$ is also finite and unramified at all but finitely many primes.
- When $\mathcal{R} = K$ is an extension of an ℓ -adic field \mathbb{Q}_{ℓ} with the ℓ -adic topology, it will be called an **ℓ -adic representation** and we will consider only the case when ρ is only ramified in a finite set of primes Σ .

Given a representation (ℓ -adic or mod ℓ^n , $n \geq 1$), the projection to the residue field gives a mod ℓ representation which will be called its **residual representation** $\bar{\rho}$, that we will see in more detail for modular forms in section 1.4. In our case, we will mainly work with these types of representations.

In case we work on a ring, Mazur ([Maz97], p.253) gives an analogous result of Theorem 1.2.2.

Proposition 1.2.3. *Let A be a complete noetherian local ring with residue field k_A of characteristic ℓ . Let Π be a profinite group and $\rho : \Pi \rightarrow GL_n(A)$ a representation. Assume that the residual representation $\bar{\rho} : \Pi \rightarrow GL_n(k_A)$ is absolutely irreducible. Let $\rho' : \Pi \rightarrow GL_n(A)$ be a representation such that $\text{tr}_A(\rho(\pi)) = \text{tr}_A(\rho'(\pi))$ for all $\pi \in \Pi$. Then ρ and ρ' are equivalent representations.*

Theorem 1.2.4. Чоботаръов (Chebotarev): *Let $F | \mathbb{Q}$ be a Galois extension unramified outside a finite set of primes Σ . Then $\bigcup_{p \notin \Sigma} [\text{Frob}_p]$ is dense in $\text{Gal}(F | \mathbb{Q})$, where $[\text{Frob}_p]$ is the well-defined conjugacy class in $\text{Gal}(F | \mathbb{Q})$ of the p -Frobenius automorphism.*

Corollary 1.2.5. *With the notation as before,*

- *An Artin representation ρ is determined by the values of $\text{tr}(\rho(\text{Frob}_p))$ on the primes $p \notin \Sigma$ at which ρ is unramified.*
- *A semi-simple mod ℓ representation ρ is determined by the characteristic polynomials of the p -Frobenius $P_{\rho,p}(X)$ on the primes $p \notin \Sigma$ at which ρ is unramified.*
- *For $n > 1$, a semi-simple mod ℓ^n representation ρ such that its residual mod ℓ representation $\bar{\rho}$ is absolutely irreducible, is determined by the characteristic polynomials of the p -Frobenius $P_{\rho,p}(X)$ on the primes $p \notin \Sigma$ at which ρ is unramified.*
- *A semi-simple ℓ -adic representation ρ ramified only in a finite set of primes Σ is determined by the values of $\text{tr}(\rho(\text{Frob}_p))$, where $p \notin \Sigma$.*

Proof. It is a direct consequence of Chebotarev's Theorem applied to Proposition 1.2.3 for the mod ℓ^n case, and to Brauer-Nesbitt in the other cases ([DDT97], p.54). □

Remark 1.2.6. *This Corollary can be applied analogously to the λ -adic, mod λ and mod λ^n representations that will be defined in Section 1.4.*

1.3 Conductor of a representation

We introduce now the notion of conductor of a representation. We will quote the definition for residual representations from [Ser87] and we will extend it to the characteristic 0 case.

Let $\bar{\rho}$ be a residual representation on a vector space V over a finite field of characteristic ℓ , and $p \neq \ell$ a prime. Let $G = \bar{\rho}(G_{\mathbb{Q}})$ and let

$$G_0 \supset G_1 \supset \dots \supset G_i \supset \dots$$

be the ramification groups of G corresponding to an extension in $\overline{\mathbb{Q}}$ of a p -adic valuation of \mathbb{Q} . Let V_i be the subspace of V fixed by G_i . We define

$$n_{\bar{\rho},p} := \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim V/V_i.$$

$n_{\bar{\rho},p}$ is written simply n_p when $\bar{\rho}$ is clear by the context.

We have then

1. $n_{\bar{\rho},p}$ is an integer ≥ 0 .
2. $n_{\bar{\rho},p} = 0$ if and only if $\bar{\rho}$ is not ramified in p .

The **Serre conductor** \overline{N} of a representation $\bar{\rho}$ is defined as

$$\overline{N} := \prod_{p \neq \ell} p^{n_{\bar{\rho},p}}.$$

For the characteristic 0 case, [Ser79] gives an analogous construction. The following is an equivalent definition given in [DDT97]. For any $u \in [-1, \infty]$, let G^u be the closed normal subgroups filtrating the inertia group \mathcal{I}_p , as it is defined in [Ser79] (IV.3). Let ρ be either an ℓ -adic or a *mod* ℓ representation, with $\ell \neq p$. Then

$$n_{\rho,p} := \text{codim} \rho^{\mathcal{I}_p} + \int_0^{\infty} \rho^{G^u} du$$

and we define the conductor N of ρ analogously

$$N := \prod_{p \neq \ell} p^{n_{\rho,p}}.$$

Definition 1.3.1. *Let ρ be an ℓ -adic or a *mod* ℓ^n representation, and let $\bar{\rho}$ be the corresponding residual *mod* ℓ representation. Then, we say that a representation is **minimal** at $p \mid N$ with respect to a prime ℓ if $n_{\bar{\rho},p} = n_{\rho,p}$. We say simply that ρ is minimal if $N = \overline{N}$.*

In [Car89], Carayol studies for a given *mod* ℓ representation, how much the conductor of a deformation can increase. He proves the following result.

Proposition 1.3.2. *Let $N = p_1^{n_{p_1}} \dots p_k^{n_{p_k}}$ and $\overline{N} = p_1^{\bar{n}_{p_1}} \dots p_k^{\bar{n}_{p_k}}$ be the conductors of a λ -adic representation ρ and the corresponding *mod* λ representation $\bar{\rho}_\lambda$, respectively. Let p be a prime dividing N , $p \neq \ell$, and suppose ρ is such that $n_p > \bar{n}_p$. Then locally at p ρ is of one of the following types*

1. $\rho_p = \mu \oplus v$, with $n_{\mu,p} = 1$ and $n_{\bar{\mu},p} = 0$, and then $n_p = n_{v,p} + 1$
2. $\rho_p = \mu \otimes sp(2)$, with $n_{\mu,p} = 0$, and then $n_p = 1$.
3. $\rho_p = \mu \otimes sp(2)$, with $n_{\mu,p} = 1$ and $n_{\bar{\mu},p} = 0$, and then $n_p = 2$.
4. The irreducible case in which $n_p = 2$.

In our case, since we are working without nebensystem, the first case reduces to $\rho_p = \mu \oplus \mu^{-1}$ and then $n_p = n_{v,p} + 1 = n_{\mu,p} + 1 = 2$.

1.4 Representations attached to modular forms

Definition 1.4.1. Let A be an abelian variety over \mathbb{Q} and $m \in \mathbb{Z}$, $m \neq 0$. The **m -torsion subgroup of A** , denoted $A[m]$, is the set of geometric points of order dividing m in A ,

$$A[m] := \{P \in A : [m]P = O\}.$$

The next theorem can be found in [Mum74], §2, Prop.1.

Theorem 1.4.2. Let m be a positive integer and A an abelian variety of dimension d defined over a field K whose characteristic does not divide m . Then $A[m] \simeq (\mathbb{Z}/m\mathbb{Z})^{2d}$ as groups.

Now we will follow [Ser72] to introduce the representations attached to elliptic curves, and we will generalize later this construction to any general A_f .

Let E be an elliptic curve over \mathbb{Q} and $m > 1$ a positive integer. Theorem 1.4.2 shows that $E[m]$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$ and therefore we can take two generators P_1, P_2 of this group, $P_1, P_2 \in E[m]$. Since the absolute Galois group acts on the geometric points of the elliptic curve, we have that for every $\sigma \in G_{\mathbb{Q}}$, $\sigma(P_1)$ can be written as a combination of the elements of the base $p_1^\sigma \cdot P_1 + p_2^\sigma \cdot P_2$, and also with $\sigma(P_2) = q_1^\sigma \cdot P_1 + q_2^\sigma \cdot P_2$. With this construction, we defined a 2-dimensional representation

$$\begin{aligned} \rho_m : G_{\mathbb{Q}} &\longrightarrow \text{Aut}(\mathcal{R})(E[m]) \simeq GL_2(\mathbb{Z}/m\mathbb{Z}) \\ \sigma &\longmapsto \begin{pmatrix} p_1^\sigma & q_1^\sigma \\ p_2^\sigma & q_2^\sigma \end{pmatrix}. \end{aligned}$$

The group $\rho_m(G_{\mathbb{Q}})$ is the Galois group of the extension of \mathbb{Q} obtained by adjoining the coordinates of the points of $E[m]$.

Let E_{tors} be the torsion subgroup of E . Then $\text{Aut}(E_{\text{tors}})$ is the inverse limit of the finite groups $\text{Aut}(E[m])$. This is a group isomorph to

$$\varprojlim_m GL_2(\mathbb{Z}/m\mathbb{Z}) = GL_2(\hat{\mathbb{Z}}), \text{ where } \hat{\mathbb{Z}} = \varprojlim_m \mathbb{Z}/m\mathbb{Z}.$$

Let \mathbb{P} be the set of prime numbers. If $\ell \in \mathbb{P}$, let $E[\ell^\infty]$ be the union of all $E[\ell^m]$. It is the ℓ -primary component of E_{tors} . Its automorphism group is isomorphic to $GL_2(\mathbb{Z}_\ell)$. We then have

$$E_{\text{tors}} = \bigoplus_{\ell \in \mathbb{P}} E[\ell^\infty] \text{ and } \text{Aut}(E_{\text{tors}}) = \prod_{\ell \in \mathbb{P}} GL_2(\mathbb{Z}_\ell)$$

In this way we constructed a 2-dimensional ℓ -adic $G_{\mathbb{Q}}$ -representation of E .

Now, we generalize this argument to abelian varieties in the natural way.

ℓ -adic representations:

Definition 1.4.3. We define the **Tate module** of an abelian variety A as the inverse limit

$$\mathcal{T}_\ell(A) := \varprojlim_n A[\ell^n].$$

From now on, f will denote a newform in $S_2(N)$, for a given N .

Lemma 1.4.4. The module $\mathcal{T}_\ell(A_f) \otimes \mathbb{Q}_\ell$ is a free module of rank 2 over $K_{f,\ell} := K_f \otimes \mathbb{Q}_\ell$.

The action of $G_{\mathbb{Q}}$ on $\mathcal{T}_\ell(A_f)$ commutes with the one of K_f , and by Theorem 1.1.9, K_f is isomorphic to $\text{End}_{\mathbb{Q}}(A_f) \otimes \mathbb{Q}$. Hence, choosing a basis of the Tate module will provide an ℓ -adic representation

$$\rho_{f,\ell} : G_{\mathbb{Q}} \rightarrow GL_2(K_{f,\ell}).$$

Theorem 1.4.5 (Criterion of Néron-Ogg-Shafarevich). *Let A be an abelian variety over a field K and v a discrete valuation of K . Let ℓ be a prime different from the characteristic of the residue field of K . Then A has good reduction at v if and only if $\mathcal{T}_\ell(A)$ is unramified at v .*

Proof. It can be found in [ST68], Theorem 1. □

Corollary 1.4.6. *Let f be a newform. Then $\rho_{f,\ell}$ is unramified outside ℓN .*

Proof. It is a direct consequence of the theorem, since outside ℓ we know by Theorem 1.1.10 that A_f has good reduction at every $p \nmid N$. \square

Given a modular form f , the above described relation between representations and newforms, and Definition 1.3.1 will provide the following definition.

Definition 1.4.7. *Given a newform f , we say that f is **minimal** at ℓ if $\rho_{f,\ell}$ is minimal at ℓ .*

λ -adic representations: Now we want to decompose this ℓ -adic representation into λ -adic representations, for $\lambda \mid \ell$, $\lambda \in K_f$.

Proposition 1.4.8. *Let f be a newform. The decomposition of ℓ in K_f induces the decomposition of $K_{f,\ell} = \bigoplus_{\lambda \mid \ell} K_{f,\lambda}$, and then the decomposition of $\rho_{f,\ell}$ as a direct sum of representations*

$$\rho_{f,\ell} = \bigoplus_{\lambda \mid \ell} (\rho_{f,\lambda} : G_{\mathbb{Q}} \rightarrow GL_2(K_{f,\lambda}))$$

follows forthwith.

Proof. Simply using the canonical projection of $K_{f,\ell}$ onto $K_{f,\lambda}$ \square

Let us introduce the fundamental Eichler-Shimura relation ([DDT97]).

Theorem 1.4.9 (Eichler-Shimura relation). *Let f be a modular form of level N and p a prime not dividing N . Then, the endomorphism T_p of $J_0(N)_{\mathbb{F}_p}$ satisfies*

$$T_p = \text{Frob}_p + \text{Ver}_p$$

where Frob_p and Ver_p are the p -Frobenius and the p -Verschiebung morphisms, respectively.

This relation is used to show that the representation $\rho_{f,\lambda}$ has nice properties.

Theorem 1.4.10. *The λ -adic Galois representations $\rho_{f,\lambda}$ are unramified outside ℓN , and satisfy that for every prime $p \nmid \ell N$,*

$$\text{tr}(\rho_{f,\lambda}(\text{Frob}_p)) = a_p, \text{ and } \det(\rho_{f,\lambda}(\text{Frob}_p)) = p.$$

Remark 1.4.11. In [Del73], Deligne generalizes this result to modular forms of arbitrary weight.

Remark 1.4.12. Let \mathcal{O}_f be the ring of integers of K_f , $\mathcal{O}_{f,\ell} := \mathcal{O}_f \otimes \mathbb{Z}_\ell$, and $\mathcal{O}_{f,\ell} = \prod_{\lambda|\ell} \mathcal{O}_{f,\lambda}$. Using the fact that λ -adic representations are determined by $\text{tr}(\rho_{f,\lambda})$ and knowing that $a_p \in \mathcal{O}_{f,\lambda}$, we can restrict the representations to

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\lambda}).$$

Remark 1.4.13. Since $\rho_{f,\lambda}$ is a 2-dimensional representation, the characteristic polynomial of the Frobenius at $p \nmid \ell N$ is

$$P_{\rho,p}(X) = X^2 - a_p X + p. \quad (1.2)$$

mod ℓ representations: From ℓ -adic representations, we can find also *mod ℓ* representations simply by taking the semi-simplification of the reduction of $\rho_{f,\ell}$

$$\bar{\rho}_{f,\ell} := \bar{\rho}_{f,\ell}^{ss} : G_{\mathbb{Q}} \rightarrow GL_2(k_f) \quad (1.3)$$

where k_f is the finite dimensional \mathbb{F}_ℓ -algebra $\mathcal{O}_{f,\ell} \otimes \mathbb{F}_\ell \simeq \mathcal{O}_{f,\ell}/\ell\mathcal{O}_{f,\ell}$.

Remark 1.4.14. Using Theorem 1.4.5 as in Corollary 1.4.6 we can see that $\bar{\rho}_{f,\ell}$ is also unramified outside ℓN .

mod λ representations:

Remark 1.4.15. Let $\mathbb{F}_{f,\lambda}$ the residue field of $\mathcal{O}_{f,\lambda}$. As before, the representation in (1.3) splits using the decomposition of $\mathcal{O}_{f,\ell}$ and, for every $\rho_{f,\lambda}$ on $\mathcal{O}_{f,\lambda}$, one gets a mod λ representation $\bar{\rho}_{f,\lambda}$ on $\mathcal{O}_{f,\lambda} \otimes \mathbb{F}_{f,\lambda}$ such that for every $p \nmid \ell N$, $\text{tr}(\bar{\rho}_{f,\lambda}(\text{Frob}_p)) \equiv a_p \pmod{\lambda}$ and $\det(\bar{\rho}_{f,\lambda}(\text{Frob}_p)) \equiv p \pmod{\lambda}$.

With the following result ([DV00]) we will be able to determine if a representation is irreducible.

Proposition 1.4.16. Let f be a newform of weight 2 and level N and $\lambda \mid \ell$ a prime in \mathcal{O} such that $\bar{\rho}_{f,\lambda}$ is reducible. If $\ell > 2$, $\ell \nmid N$, then for every $p \nmid \ell N$, we have

$$a_p \equiv \epsilon(p) + p\epsilon^{-1}(p) \pmod{\lambda},$$

where ϵ is a character unramified outside N whose conductor c verifies $c^2 \mid N$.

Hence, finding one prime p such that $a_p \not\equiv \epsilon(p) + p\epsilon^{-1}(p) \pmod{\lambda}$ will be enough to ensure that f is irreducible modulo λ . If $p \equiv 1 \pmod{c}$, then the character ϵ is trivial and hence we just have to check if $a_p \not\equiv p + 1 \pmod{\lambda}$.

In [Maz77], Mazur proves the following result.

Proposition 1.4.17. *Let N be a prime and let ℓ be a prime such that it divides the numerator of $(N - 1)/12$. Then there exists a newform of level N reducible modulo λ .*

We can sum up both results with the following criterium. f is irreducible modulo λ for every $\lambda \mid \ell$ if at least one of the following holds:

- If N is prime and $\ell > 3$, then $\ell \nmid N - 1$.
- There exists a prime such that $p \equiv 1 \pmod{c}$ and $\ell \nmid \text{Norm}(a_p - (1+p))$.

Given a newform f and a prime ℓ , finding one criterium to determine if there exists one λ such that $\bar{\rho}_{f,\lambda}$ is reducible is more difficult. Even if we try with a very big number of primes, Proposition 1.4.16 in principle does not say anything when the congruences are always satisfied.

One special case in which both propositions above can be applied together to determine reducibility is the following. Given a basis of $S_2^{\text{new}}(N)$, if we can apply Proposition 1.4.16 to ensure that all elements of the basis but one are irreducible, Proposition 1.4.17 ensures that this one element left is indeed reducible.

In Remark 2.13.1 we describe another possibility to compute, using the algorithms developed in the next chapter, for which primes is a representation reducible.

mod ℓ^n representations: Let us describe now the *mod ℓ^n* representations, for $n > 1$. The idea of the construction will be analogous to the *mod ℓ* representations.

Given an ℓ -adic representation

$$\rho_{f,\ell} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\ell}),$$

we will use the projection

$$\mathcal{O}_{f,\ell} \rightarrow \mathcal{O}_{f,\ell}/\ell^n \mathcal{O}_{f,\ell}$$

and we semi-simplify to obtain the *mod ℓ^n* representation

$$\bar{\rho}_{f,\ell^n} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\ell}/\ell^n \mathcal{O}_{f,\ell}). \tag{1.4}$$

mod λ^n representations: Again as before, we use the decomposition of ℓ in K_f to split the representation $\bar{\rho}_{f,\ell^n}$ into smaller parts, and then take the projection

$$\prod \mathcal{O}_{f,\lambda_i}/\lambda_i^{e_i n} \mathcal{O}_{f,\lambda_i} \rightarrow \mathcal{O}_{f,\lambda_i}/\lambda_i^n \mathcal{O}_{f,\lambda_i}$$

to obtain the *mod λ^n* representation

$$\bar{\rho}_{f,\lambda^n} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\lambda}/\lambda^n \mathcal{O}_{f,\lambda}) \quad (1.5)$$

attached to f .

2d-dimensional representations: For a given λ , we know that $\mathcal{O}_{f,\lambda}$ (resp. $\mathcal{O}_{f,\lambda}/\lambda \mathcal{O}_{f,\lambda}$) is a \mathbb{Z}_{ℓ} -algebra (resp. an \mathbb{F}_{ℓ} -algebra) of dimension d_{λ} , where d_{λ} is the inertia degree of λ (if ℓ decomposes as $\ell = \lambda_1^{e_1} \cdot \dots \cdot \lambda_s^{e_s}$, then $d = [K_f : \mathbb{Q}] = e_{\lambda_1} d_{\lambda_1} + \dots + e_{\lambda_s} d_{\lambda_s}$). Let $\hat{\rho}_{f,\lambda}$ (resp. $\hat{\rho}_{\bar{f},\lambda}$) be the $2d_{\lambda}$ -dimensional over \mathbb{Z}_{ℓ} (resp. over \mathbb{F}_{ℓ}) representation associated to $\rho_{f,\lambda}$ (resp. $\bar{\rho}_{f,\lambda}$). Then we obtain two semi-simple $2d$ -dimensional representations

$$\hat{\rho}_{f,\ell} : G_{\mathbb{Q}} \rightarrow GL_{2d}(\mathbb{Z}_{\ell}) \text{ and } \hat{\rho}_{\bar{f},\ell} : G_{\mathbb{Q}} \rightarrow GL_{2d}(\mathbb{F}_{\ell}).$$

Using then the decomposition of ℓ given above we get then $\rho_{f,\ell}$ as a conjugate of

$$\hat{\rho}_{f,\ell} = \left(\begin{array}{ccccccc} \boxed{\hat{\rho}_{f,\lambda_1}} & & & & & & \\ & \ddots & & & & & \\ & & e_1 & & & & \\ & & & \ddots & & & \\ & & & & \boxed{\hat{\rho}_{f,\lambda_1}} & & \\ & & & & & \boxed{\hat{\rho}_{f,\lambda_2}} & \\ & & & & & & \ddots \\ & & & & & & & \boxed{\hat{\rho}_{f,\lambda_s}} \end{array} \right). \quad (1.6)$$

and analogously $\hat{\rho}_{\bar{f},\ell}$ is a conjugate of $\bar{\rho}_{f,\ell}$.

In (1.2) we saw that the characteristic polynomial of a Frobenius element had degree two and it is contained in $\mathcal{O}_{f,\lambda}[X]$. If we compute now the characteristic polynomial of the Frobenius in $\hat{\rho}_{f,\ell}$ (resp. in $\hat{\rho}_{\bar{f},\ell}$), we see that it has degree $2d$, but the coefficients lie in \mathbb{Z}_{ℓ} —in fact, in \mathbb{Z} — (resp. in \mathbb{F}_{ℓ}), which is much easier to compute with. Actually, we have that

$$P_{\hat{\rho}_{f,\ell},p} = \prod_{\lambda|\ell} P_{\rho_{f,\lambda},p} \text{ and } P_{\hat{\rho}_{\bar{f},\ell},p} = \prod_{\lambda|\ell} P_{\bar{\rho}_{f,\lambda},p}. \quad (1.7)$$

Clearly, $P_{\hat{\rho}_{\bar{f},\ell},p}$ is the reduction modulo ℓ of $P_{\hat{\rho}_{f,\ell},p}$.

1.5 Representations on Hecke algebras

In this section, we want to describe how the Hecke algebra acts on the space of cusp forms and we will introduce λ -adic representations on these Hecke algebras.

In §1.1 we saw that the Hecke algebra \mathbb{T} acts on $S_2(N)$. For a fixed normalized eigenform f of level N , we have a map

$$\begin{aligned} \varphi_f : \mathbb{T}(N) &\rightarrow \overline{\mathbb{Z}} \\ T_p &\mapsto a_p(f) \end{aligned}$$

and given a fixed ring surjection of $\overline{\mathbb{Z}}$ in $\overline{\mathbb{F}}_\ell$, $\overline{\varphi}_f$ is a reduction to $\overline{\mathbb{F}}_\ell$. Then $\mathfrak{m}_f := \text{Ker}(\overline{\varphi}_f)$ is a maximal ideal in \mathbb{T} , and $\mathbb{T}/\mathfrak{m}_f$ is a finite field of characteristic ℓ .

Likewise, for a given maximal ideal \mathfrak{m} of \mathbb{T} , there exists a modular form \overline{f} with coefficients \overline{a}_p in \mathbb{T}/\mathfrak{m} such that each \overline{a}_p is the image of $\overline{\varphi}_f(T_p)$.

Remark 1.5.1. *Given a field K and a modular form \overline{f} with coefficients in the residue field of K , there exists not always a modular form f of the same weight and level with coefficients in K lifting \overline{f} . Some examples concerning modular forms of weight 1 with coefficients in \mathbb{F}_8 can be found in Appendices A and B in [MW06].*

Now we will quote some results from [Rib90a]. First, we will find representations on \mathbb{T}/\mathfrak{m} related to Remark 1.4.15.

Proposition 1.5.2. *Let \mathfrak{m} be a maximal ideal in $\mathbb{T}(N)$ and $\ell = \text{char}(\mathbb{T}/\mathfrak{m})$. Then, there exists a unique semisimple representation on a finite field*

$$\overline{\rho}_{\mathfrak{m}} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{T}/\mathfrak{m}),$$

satisfying

$$\text{tr}(\rho_{\mathfrak{m}}(\text{Frob}_p)) \equiv \overline{a}_p \pmod{\mathfrak{m}}, \text{ and } \det(\rho_{\mathfrak{m}}(\text{Frob}_p)) \equiv p \pmod{\mathfrak{m}}$$

for all the primes p not dividing ℓN , and it is unramified at all these primes.

We consider the $(\mathbb{T}/\mathfrak{m})[G_{\mathbb{Q}}]$ -module

$$W = J_0(N)[\mathfrak{m}]$$

defined as the elements of $J_0(N)(\overline{\mathbb{Q}})$ annihilated by \mathfrak{m} . If the characteristic of \mathbb{T}/\mathfrak{m} is ℓ , W is a $G_{\mathbb{Q}}$ -submodule of $J_0(N)[\ell]$.

Since one of our interests is to compare congruences between modular forms not only modulo λ but also modulo λ^n , we want to make the analogous construction with powers of maximal ideals of \mathbb{T} .

For a given $n > 1$, we now consider the $(\mathbb{T}/\mathfrak{m}^n)[G_{\mathbb{Q}}]$ -module

$$W^n = J_0(N)[\mathfrak{m}^n]$$

analogously as W . If the characteristic of \mathbb{T}/\mathfrak{m} is ℓ , W^n is a $G_{\mathbb{Q}}$ -submodule of $J_0(N)[\ell^n]$.

Now we would like to find a representation over $(\mathbb{T}/\mathfrak{m}^n)$ and relate it again with the *mod* λ^n representation we constructed in (1.5) (see Section 1.4).

In the following result from [Car94], Carayol provides a more general λ -adic representation. Then we will simply take the quotients in each side.

Let A be a complete local ring with residue field F . Let f be a normalized eigenform with coefficients in A . Let \bar{f} be the residual form with coefficients in F . Actually, the coefficients of \bar{f} lie in a finite field $\mathbb{F} \subset F$. Let $\bar{\rho}_{\mathfrak{m}}$ be the residual representation on $\mathbb{F} = \mathbb{T}/\mathfrak{m}$ given in Proposition 1.5.2.

Theorem 1.5.3. *Let the residual representation $\bar{\rho}_{\mathfrak{m}}$ be absolutely irreducible. Then, there exists a unique (up to isomorphism) continuous representation on A*

$$\rho_{f,A} : G_{\mathbb{Q}} \rightarrow GL_2(A)$$

unramified outside ℓN , which verifies for every $p \nmid \ell N$

$$\mathrm{tr}(\rho_{f,A}(\mathrm{Frob}_p)) = a_p, \text{ and } \det(\rho_{f,A}(\mathrm{Frob}_p)) = p.$$

Proof. The proof can be found in [Car94], Theorem 3 (p.225). □

We apply now this theorem with the following ingredients. Let $\lambda \mid \ell$ and $f \in S_2^{\mathrm{new}}(N)$ be given and \mathfrak{m} the corresponding maximal ideal in \mathbb{T} . We have a projection

$$\pi : \mathbb{T} \rightarrow \mathbb{T}/\mathfrak{m}$$

and a representation on \mathbb{T}/\mathfrak{m} from Proposition 1.5.2. Let $A = \mathbb{T}_{\lambda, \mathfrak{m}}$ the localisation of \mathbb{T}_{λ} in \mathfrak{m} . The representation on this A is then the desired λ -adic representation. As a Corollary we get the *mod* λ^n representations we were looking for.

Corollary 1.5.4. *Let \mathfrak{m} be a maximal ideal in \mathbb{T} and $\ell = \text{char}(\mathbb{T}/\mathfrak{m})$. Then, there exists a unique (up to isomorphism) semisimple 2-dimensional representation*

$$\bar{\rho}_{f,\mathfrak{m}^n} : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{T}_{\lambda,\mathfrak{m}}/\mathfrak{m}^n),$$

satisfying

$$\text{tr}(\bar{\rho}_{f,\mathfrak{m}^n}(\text{Frob}_p)) \equiv a_p \pmod{\mathfrak{m}^n}, \text{ and } \det(\bar{\rho}_{f,\mathfrak{m}^n}(\text{Frob}_p)) \equiv p \pmod{\mathfrak{m}^n}$$

for every prime $p \nmid \ell N$, and it is unramified outside ℓN .

Since we are specially interested in representations coming from n -torsion points of abelian varieties, we would like to see when this representation from Carayol is related with the n -torsion point representation we saw in the previous section.

Recall from the previous section that $\mathcal{T}(A)$ corresponds to the Tate module of the abelian variety A . Let $\mathcal{T}_{\lambda,\mathfrak{m}}$ denote the localisation of \mathcal{T}_{λ} in \mathfrak{m} . In [KW07] we find the following result.

Proposition 1.5.5. *Let $\rho_{\mathfrak{m}}$ be irreducible and let $\ell \nmid N$. If $\ell = 2$, assume that $\mathbb{T}_{\lambda,\mathfrak{m}}$ is Gorenstein. Then*

$$\mathcal{T}_{\lambda,\mathfrak{m}}(J_0(N)) \simeq \mathbb{T}_{\lambda,\mathfrak{m}} \oplus \mathbb{T}_{\lambda,\mathfrak{m}}$$

as $\mathbb{T}_{\lambda,\mathfrak{m}}$ -modules.

Proof. If $\ell > 2$, Theorem 1.2 from [KW07] ensures that $\rho_{\mathfrak{m}}$ has multiplicity one. Proposition 2.1 from the same article together with Nakayama's Lemma, give then the desired result.

For $\ell = 2$ the same argument works except when $\rho_{\mathfrak{m}}$ is unramified at 2 and the 2-Frobenius is scalar. In this case, Corollary 4.4 from [Wie06] ensures that the multiplicity of $\rho_{\mathfrak{m}}$ is bigger than one. Proposition 2.2 from [KW07] implies then that $\mathbb{T}_{\lambda,\mathfrak{m}}$ is not Gorenstein. \square

Remark 1.5.6. *We can conclude then, that for $\ell \nmid N$ and if $\lambda \mid 2$, assuming that $\mathbb{T}_{\lambda,\mathfrak{m}}$ is Gorenstein, the ℓ^n -torsion points representation $\bar{\rho}_{f,\lambda^n}$ is isomorphic to Carayol's representation on the Hecke algebra $\bar{\rho}_{f,\mathfrak{m}^n}$.*

Remark 1.5.7. *In [Wiea] G. Wiese has implemented an algorithm in Magma to compute the Hecke algebra which can be applied to compute if the Hecke algebra modulo 2 of a given newform f of level N , and the localisations of this algebra are Gorenstein or not.*

1.6 Abelian varieties of GL_2 -type and Serre's Conjecture

In this section we state two recently proven strong results: Serre's Conjecture and the Generalized Shimura-Taniyama-Weil Conjecture. The aim of this section is just to show that since Serre's Conjecture has been proven, all the work done with modular forms can be applied to Abelian varieties of GL_2 -type.

Serre conjectured in [Ser87] (3.2.3?) the following statement.

Theorem 1.6.1 (Serre's conjecture). *Let p a prime number and $\bar{\rho} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_p)$ a Galois representation. Let $\bar{\rho}$ be odd and irreducible. Then, there exists a newform such that $\bar{\rho}_f$ is equivalent to $\bar{\rho}$.*

Proof. This conjecture has been recently proven in [KWb] and [KWc] (see also [KWa]), [Kis] and [Die06] by Chandrashekar Khare and Jean-Pierre Wintenberger, Mark Kisin, and Luis Dieulefait. □

Definition 1.6.2. *An Abelian variety A over \mathbb{Q} is of GL_2 -type if it is simple and there are a number field K such that $[K : \mathbb{Q}] = \dim(A)$ and an order \mathcal{O} of K such that $\mathcal{O} \hookrightarrow \text{End}_{\mathbb{Q}}(A)$.*

Ribet proved that Serre's conjecture implies the Shimura-Taniyama-Weil conjecture.

Theorem 1.6.3 (Generalized Shimura-Taniyama-Weil Conjecture). *Given an Abelian variety A over \mathbb{Q} of GL_2 -type with conductor N , there exists a non constant morphism $\pi : J(X_1(N)) \rightarrow A$.*

Proof. The proof can be found in [Rib92]. □

In other words, every Abelian variety of GL_2 -type comes from a modular form. Thus, we can use all our knowledge about modular forms to this big subset of the category of Abelian varieties, as we will see in the next section.

1.7 Congruences between modular forms

Our work was mainly focused on studying congruences between modular Galois representations. We introduce then finally the concept of congruence between representations.

Let f and g be two newforms of weight 2 and levels $N_g \mid N_f$. Let K_f (resp. K_g) be the field generated by the coefficients of f (resp. g) and K be the composite field $K := K_f \cdot K_g$. $d_f := [K_f : \mathbb{Q}]$, $d_g := [K_g : \mathbb{Q}]$, $d := [K : \mathbb{Q}]$. Let \mathcal{O} , \mathcal{O}_f and \mathcal{O}_g be respectively the rings of integers of K , K_f and K_g . Let Σ_K be the d embeddings of K in \mathbb{C} .

λ will be a place in K dividing a prime $\ell \nmid N_f$ of \mathbb{Z} . We denote also by λ its restrictions to \mathcal{O}_f and \mathcal{O}_g . As before (Section 1.4), the decomposition of $\mathcal{O}_\ell = \mathcal{O} \otimes \mathbb{Z}_\ell$ provides us the ring \mathcal{O}_λ , and $\mathcal{O}_{f,\lambda}$ and $\mathcal{O}_{g,\lambda}$ can be found analogously using the above mentioned restrictions of λ in \mathcal{O}_f and \mathcal{O}_g .

If we take the ideal $\lambda^n \subset \mathcal{O}$ and the projection

$$\pi : \mathcal{O} \rightarrow \mathcal{O}/\lambda^n,$$

then we say that two numbers $\alpha \in \mathcal{O}_f$ and $\beta \in \mathcal{O}_g$ are congruent modulo λ^n if $\pi(\alpha) = \pi(\beta)$.

Definition 1.7.1. f and g are **congruent modulo λ^n** ($n \geq 1$) if $a_p(f) \equiv a_p(g) \pmod{\lambda^n}$ for almost all $p \in \mathbb{P}$. In such case, we say that ℓ is a **prime of congruence**.

Seen in terms of language from §1.5, being congruent can be read as follows: given an integer N and a maximal ideal \mathfrak{m} in $\mathbb{T}(N)$, we ask whether there exist (at least) two modular forms f and g in $S_2(N)$ such that $\mathfrak{m}^n = \mathfrak{m}_f^n = \mathfrak{m}_g^n$.

Now we want to compare the representations attached to the modular forms f and g . However, the vector spaces where they are represented might be not comparable. Therefore, we have to tensor properly our vector spaces with the ring \mathcal{O}_λ to find a place where our representations can be compared.

Let $\rho_{f,\lambda} : G_{\mathbb{Q}} \rightarrow \text{Aut}(V'_{f,\lambda})$ be the λ -adic representation over $\mathcal{O}_{f,\lambda}$ with a 2-dimensional representation space $V'_{f,\lambda}$ over $\mathcal{O}_{f,\lambda}$ with $G_{\mathbb{Q}}$ -action as in Remark 1.4.12.

This representation can be extended to the \mathcal{O}_λ -module $V_{f,\lambda} := V'_{f,\lambda} \otimes_{\mathcal{O}_{f,\lambda}} \mathcal{O}_\lambda$.

Now we are already in a free module with common coefficients for both modular forms. If we want to compare the *mod λ^n* representations, we just have to tensor with the ring $\mathcal{O}_\lambda/\lambda^n \mathcal{O}_\lambda$: $\bar{\rho}_{f,\lambda^n}$ can be seen as the representation attached to the $\mathcal{O}_\lambda/\lambda^n \mathcal{O}_\lambda[G_{\mathbb{Q}}]$ -module $A_{f,\lambda} := V_{f,\lambda} \otimes_{\mathcal{O}_{f,\lambda}} \mathcal{O}_\lambda/\lambda^n \mathcal{O}_\lambda$.

Theorem 1.7.2. *Let $\bar{\rho}_{f,\lambda^n}$ and $\bar{\rho}_{g,\lambda^n}$ be irreducible. Then $f \equiv g \pmod{\lambda^n} \iff A_{f,\lambda^n} \simeq_{\mathcal{O}_\lambda/\lambda^n \mathcal{O}_\lambda[G_{\mathbb{Q}}]} A_{g,\lambda^n}$.*

Proof. This is just Corollary 1.2.5 applied to modular forms. □

Remark 1.7.3. *The following properties are satisfied:*

- *If f and g are congruent modulo λ_1 and modulo λ_2 and $(\lambda_1, \lambda_2) = 1$, then they are obviously also congruent modulo $\lambda_1\lambda_2$.*
- *If f and g are congruent modulo λ , then $\text{Im}(\bar{\rho}_{f,\lambda}) \simeq \text{Im}(\bar{\rho}_{g,\lambda})$.*

Definition 1.7.4. *Let f, g and an integer ℓ be given. We denote by $\hat{\rho}_{f,g,\ell}$ a representation both equivalent to a subrepresentation of $\hat{\rho}_{\bar{f},\ell}$ and to one of $\hat{\rho}_{\bar{g},\ell}$, and such that for any other representation $\hat{\rho}'$ satisfying this condition, $\dim_{\mathbb{F}_\ell}(\hat{\rho}') \leq \dim_{\mathbb{F}_\ell}(\hat{\rho}_{f,g,\ell})$.*

Now, we can already state more precisely the questions we formulated in the introduction. Let A_1 and A_2 two Abelian varieties of GL_2 -type. With the Generalized Shimura-Taniyama-Weil Conjecture, we know that there exist N_1 and N_2 such that they can be found as quotients of $J_1(N_1)$ and $J_1(N_2)$. Let A_1^* and A_2^* be the dual varieties included in $J_1(N_1)$ and $J_1(N_2)$. For simplicity, in this work, for simplicity we restrict ourselves to the case without character. Thus, if $N := \text{lcm}(N_1, N_2)$, we know there are embeddings A_1' and A_2' of A_1^* and A_2^* in $J_0(N)$.

Question 0.1.1 can be reformulated as: given A_1 and A_2 two Abelian varieties of GL_2 -type, how big can $A_1' \cap A_2'$ be?

As explained in the introduction, if A_1' and A_2' are not isogenous this intersection is included in $J_0^{\text{Tor}}(N)$ and therefore we are interested in studying the representations on the torsion points of A_1' and A_2' .

Given a prime number ℓ , we want to determine the biggest n such that there exist groups C of order ℓ^n contained in the intersection above. If f' and g' are the modular forms associated to A_1' and A_2' , finding C will be equivalent to finding congruences between f' and g' modulo λ^n , for some place $\lambda \mid \ell$. Since f' and g' must not necessarily be newforms, we can find two associated newforms f and g of levels $N_f := N/n_f$ and $N_g := N/n_g$, for some positive integers n_f and n_g . If Ribet's Lowering the Level can be generalized (in Chapter 3 we give some cases in which it can be done and in the last section, "Further Work", we suggest more generalizations) we could assume without loss of generality that $N_f \geq N_g$ and that ρ_g is minimal and irreducible modulo ℓ .

In case ρ_g were reducible, it could be split in a direct sum of irreducible representations. If it were not minimal in a prime p and we could apply

1 Necessary background

Lowering the Level modulo λ^n , there would exist a modular form g'' of level N_g/p^k for a $k \geq 1$ such that it would be congruent to ρ_g modulo λ^n . Repeating this step for all primes in which ρ_g is not minimal we could find a minimal representation congruent to the original one. Let us assume after these heuristics that $N_g \mid N_f$.

Question 0.1.2 can be seen now as: Let f and g be two newforms such that g is minimal and $N_g \mid N_f$. For every prime ℓ , which is the largest n such that there exists a place $\lambda \mid \ell$ with

$$\bar{\rho}_{f,\lambda^n} \sim \bar{\rho}_{g,\lambda^n}?$$

In the next chapter we find an algorithm to compute an answer to this question.

Chapter 2

Algorithms to compute congruences modulo ℓ^n

In this chapter we want to give an answer to the first question we asked ourselves in the introduction. Given two modular forms, can we determine which are the primes of congruence between these forms? Moreover, if ℓ is a prime of congruence, which is the maximal n for which f and g are congruent modulo λ^n , $\lambda \mid \ell$?

Even though we follow here a different structure, most of the results of this chapter are included in a joint work with G. Wiese in [TW09].

First of all, we need to introduce the local and the global problems: while the former refers to the congruence modulo ℓ^n between modular forms in a fixed prime p , the latter corresponds to the congruence between modular forms, i.e. at all but a finite amount of primes.

Then we have to redefine what congruences modulo ℓ^n mean in our context: since there is no good Galois theory in $\mathcal{O}/\lambda^n\mathcal{O}$, if λ ramifies, it is rather difficult to compare modular forms modulo λ^n . Hence, we have to introduce $\gamma(n)$, which will depend on the ramification index. Then we can easily work with $\mathcal{O}/\lambda^{\gamma(n)}\mathcal{O}$ instead of $\mathcal{O}/\lambda^n\mathcal{O}$.

In the following sections we give an algorithm to determine an upper bound for the question aforementioned. In other words, if there exists a congruence modulo ℓ^n (using the redefined definition of congruence modulo ℓ^n), the algorithm will return an integer L^+ such that $\ell^n \mid L^+$. We show also an analogous algorithm to compute if there exists any congruence between one given modular form and one of its Galois conjugates.

Next we will describe an algorithm which finds a lower bound. This

means, given two newforms f and g , our algorithm will give a number L^- such that, if ℓ^n divides L^- , f and g (or one of their conjugates) are congruent modulo ℓ^n .

Section 2.14 will be reserved to give some examples comparing both algorithms. It is interesting to see that in many cases both algorithms (lower and upper bound) give the very same number. In this case we have determined the true value of congruences that we were looking for. Finally in the last section, we give an idea for an heuristic way to realize groups.

We recall the notation of the preceding chapter. f and g will denote newforms of weight 2 (with trivial character) and levels $N_g \mid N_f$. K_f is the field generated by the coefficients of f , and K is the composite field of K_f and K_g . $\ell \nmid N_f$ is a prime and λ a place in K dividing ℓ . \mathcal{O} (resp. \mathcal{O}_f) is the ring of integers of K (resp. K_f) and $\mathcal{O}_{f,\lambda} = \mathcal{O}_f \otimes \mathcal{O}_\lambda$. Σ_K (resp. Σ_f) is the set of embeddings of K (resp. K_f) in \mathbb{C} .

2.1 Congruences modulo ℓ^n

Given two polynomials P, Q with integer coefficients and a place λ , we want to determine if there exist two roots in $\overline{\mathbb{Z}}$ $P(\alpha) = Q(\beta) = 0$ such that α and β are congruent modulo λ^n . However, ring extensions of $\mathbb{Z}/\ell^n\mathbb{Z}$ do not have a good Galois theory and whence the projections of P and Q in $\mathbb{Z}/\ell^n\mathbb{Z}[X]$ do not suffice to determine these congruences, and we have to work directly in $\mathcal{O}/\lambda^n\mathcal{O}$.

More precisely, in a joint work with G. Wiese ([TW09], §2) it is shown that, in general, $\mathbb{Z}/\ell^n\mathbb{Z}$ does not inject into $\mathcal{O}/\lambda^n\mathcal{O}$. Moreover, if λ ramifies in \mathcal{O} , comparing the polynomials modulo ℓ^n –whatever it means– can give information about congruences modulo λ^{en} , instead of λ^n . Therefore, we introduce a new concept of congruence modulo ℓ^n described in the above mentioned article.

Definition 2.1.1. *Let L/K be an extension of local fields and let $e_{L/K}$ denote the ramification index. For $n \in \mathbb{N}$ we let*

$$\gamma_{L/K}(n) := (n - 1)e_{L/K} + 1. \tag{2.1}$$

We will simply write $\gamma(n)$ if L/K is clear by the context.

Proposition 2.1.2. *Fix an integer n . Field homomorphisms $\mathbb{Q}_\ell \hookrightarrow L \hookrightarrow M$ of finite type induce ring injections*

$$\mathbb{Z}/\ell^n\mathbb{Z} \hookrightarrow \mathcal{O}_L/(\pi_L^{\gamma_{L/\mathbb{Q}_\ell}(n)}) \hookrightarrow \mathcal{O}_M/(\pi_M^{\gamma_{M/\mathbb{Q}_\ell}(n)}).$$

In this chapter, we will refer to *mod* ℓ^n representations as the representations over $\mathcal{O}_M/(\pi_M^{\gamma_{M/\mathbb{Q}_\ell}(n)})$

$$\bar{\rho}_{f,\ell^n} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\lambda}/\lambda^{\gamma(n)}\mathcal{O}_{f,\lambda}).$$

We can now define congruences *mod* ℓ^n for elements in ℓ -adic fields in the following way.

Definition 2.1.3. *Fix an integer n . Let K and L be ℓ -adic fields contained in some fixed \mathbb{Q}_ℓ . Let $a \in K$ and $b \in L$ be any integral elements.*

The elements a and b are called congruent mod ℓ^n if

$$a - b \in (\pi_M^{\gamma_{M/\mathbb{Q}_\ell}(n)})$$

for any field M containing $a - b$.

Again, in this chapter we will use this definition to speak about congruences *mod* ℓ^n between modular forms.

Thus, for a fixed p , the local problem of finding congruent roots of two polynomials, modulo λ^n , can be now reformulated modulo ℓ^n as follows.

Remark 2.1.4. *If $n = 1$ or $e = 1$, it is clear that $\gamma(n) = n$. Thence, in this case congruences modulo ℓ^n are equivalent to congruences modulo λ^n , for one $\lambda \mid \ell$.*

2.2 Local problem

Our first idea to find whether two representations are congruent, was to compare the Frobenius action: **Чоботарьов** and Corollary 1.2.5 guarantee that this information is sufficient to determine the representations.

Let $P'_{f,p}(X) = X^2 - a_p X + p$ be the characteristic polynomial of the p -Frobenius of $\rho_{f,\lambda}$ from equation (1.2). We are interested in computing when $P'_{f,p} \equiv P'_{g,p} \pmod{\lambda^n}$. However, it might be impossible to compute congruences of elements of 100 cyphers over a composite field of two different fields of dimension 100. Therefore, we compute the “norm” of the polynomials.

Let $d := [K_f : \mathbb{Q}]$ and σ_i the d embeddings of K_f in \mathbb{C} . Let $P_{f,p}$ be

$$P_{f,p} := \prod_{\sigma} P'_{\sigma(f),p}. \quad (2.2)$$

Since $P_{f,p}$ are polynomials of degree $2d$ with integer coefficients, it is possible to work much faster with them. In fact $P_{f,p}$ corresponds to the polynomial $P_{\hat{\rho}_{f,\ell,p}}$ of equation (1.7). Therefore, we will call \hat{P}_{f,p,ℓ^n} the projection to $\mathbb{Z}/\ell^n\mathbb{Z}[X]$ of $P_{f,p}$.

However, in the previous section we saw that working in $\mathbb{Z}/\ell^n\mathbb{Z}[X]$ did not provide the desirable results. Using the definition of congruence modulo ℓ^n given in Section 2.1 and given a fixed prime p , we want to determine for which primes, the the p -Frobenius of f and g are congruent. We can define then what we call the local problem at p of congruence between newforms.

Problem 2.2.1. *Given two polynomials $P_{f,p}$ and $P_{g,p}$ in $\mathbb{Z}[X]$ and a prime power ℓ^n , we want to determine if there exist one $\lambda \mid \ell$ and $\alpha, \beta \in \mathbb{Z}$ such that $P_{f,p}(\alpha) = P_{g,p}(\beta) = 0$ and $\alpha \equiv \beta \pmod{\ell^n}$.*

2.3 Global problem

While in the previous section we just focused on the characteristic polynomials of a fixed prime, now we describe the problem concerning (almost) all the primes.

Problem 2.3.1. *Let f and g be two newforms of levels $N_g \mid N_f$.*

(ub) (*Upper Bound*) *Determine a number $L^+(f, g)$ with prime decomposition $\{\ell_1^{n_1}, \dots, \ell_r^{n_r}\}$ such that*

- *for all primes ℓ different from all the ℓ_i , the representations ρ_f and ρ_g are incongruent modulo ℓ and*
- *for all $i \in \{1, \dots, r\}$ and all $n > n_i$, the representations ρ_f and ρ_g are incongruent modulo ℓ_i^n .*

(lb) (*Lower Bound*) *Determine a number $L^-(f, g)$ with prime decomposition $\{\ell_1^{n_1}, \dots, \ell_r^{n_r}\}$ such that for all $i \in \{1, \dots, r\}$ the representations ρ_f and ρ_g are congruent modulo $\ell_i^{n_i}$.*

We write $L^+(f, g)$ and $L^-(f, g)$ simply L^+ and L^- when f and g are clear by the context.

Definition 2.3.2. *When the upper bound L^+ equals the lower bound L^- , we have found the true value L which determines all the congruences between f and g . We will call L the **global congruence number**, or simply the congruence number between f and g .*

2.4 Global upper bound

In this section, we give one upper bound for the global problem. Using the polynomials with integer coefficients from (2.2), we can obtain in a very fast way a finite set with all possible congruences. Let us remark that in this section the ramification of λ does not represent a problem and therefore we can work with congruences modulo λ^n .

Lemma 2.4.1. *Let $P_{f,p}$ and $P_{g,p}$ be coprime in $\mathbb{Z}[X]$ and let R be their resultant. If ℓ divides R , then there are two roots $P_{f,p}(\alpha_f) = P_{g,p}(\alpha_g) = 0$ in \mathcal{O} such that $\alpha_f \equiv \alpha_g \pmod{\lambda}$ and the gcd between $\hat{P}_{f,p,\ell}$ and $\hat{P}_{g,p,\ell}$ is not trivial. Conversely, if there exist two roots $P_{f,p}(\alpha_f) = P_{g,p}(\alpha_g) = 0$ in \mathcal{O} such that $\alpha_f \equiv \alpha_g \pmod{\lambda^n}$, then $\ell^n \mid R$.*

Proof. If $\ell \mid R$, it means that $R = 0$ in the residue field k of K . This implies that $\hat{P}_{f,p,\ell}$ and $\hat{P}_{g,p,\ell}$ have a common root in \bar{k} . Therefore, there exist an irreducible factor $\hat{P}'_{f,p,\ell}$ of $\hat{P}_{f,p,\ell}$ in $k[X]$, and another one $\hat{P}'_{g,p,\ell}$ of $\hat{P}_{g,p,\ell}$, such that they have a common root in $\bar{k}[X]$. Since they are irreducible and monic, they must have all roots in common (the Galois conjugates of the common root). Hence, $\hat{P}'_{f,p,\ell} = \hat{P}'_{g,p,\ell}$ and the gcd of $\hat{P}_{f,p,\ell}$ and $\hat{P}_{g,p,\ell}$ is not trivial.

On the other hand, if e is the ramification index of λ in K , there exist e embeddings $\sigma_1, \dots, \sigma_e$ such that $\sigma_i(\lambda) = \lambda$. Let $\sigma_i|_f$ (resp. $\sigma_i|_g$) be the restriction of σ_i in K_f (resp. in K_g). For every $i \neq j \in \{1 \dots e\}$, we have that $(\sigma_i|_f, \sigma_i|_g) \neq (\sigma_j|_f, \sigma_j|_g)$.

Since $\alpha_f \equiv \alpha_g \pmod{\lambda^n}$, we have that $\alpha_f = \alpha_g + \lambda^n \cdot \eta$, for one $\eta \in \mathcal{O}$. Then $\sigma_i(\alpha_f) - \sigma_i(\alpha_g) = \lambda^n \eta_i$ for every $i \in \{1 \dots e\}$, and we have e elements $\sigma_i(\alpha_f) - \sigma_i(\alpha_g)$ multiple of λ^n dividing the resultant. Hence λ^{en} divides the resultant, and since the resultant is an integer number, ℓ^n must divide the resultant. \square

Lemma 2.4.2. *If f and g are congruent modulo λ^n , then ℓ^n divides the resultant of every couple $P_{f,p}$ and $P_{g,p}$, $p \nmid \ell N_f$.*

Proof. If f and g are congruent modulo λ^n , it means that $a_p(f) \equiv a_p(g)$, for every $p \nmid \ell N_f$. Whence, if $P_{f,p} = X^2 - a_p(f)X + p$, then $P_{g,p} = X^2 - (a_p(f) + \lambda^n \eta)X + p$. The roots of these polynomials satisfy

$$\alpha_f \beta_f = p = \alpha_g \beta_g$$

and

$$\alpha_f + \beta_f = a_p(f) = \alpha_g + \beta_g + \lambda^n \eta.$$

β_f and β_g can not be 0 (because $\alpha_i \beta_i = p$ and $p \neq 0$). Then,

$$\frac{p}{\beta_f} - \frac{p}{\beta_g} + \beta_f - \beta_g = \lambda^n \eta$$

and it follows that

$$(\beta_f - \beta_g) \left(1 - \frac{p}{\beta_f \beta_g}\right) = \lambda^n \eta.$$

Thence,

$$(\beta_f - \beta_g)(\beta_f - \alpha_g) = \lambda^n \eta \beta_f.$$

Then, we use a similar argument as in the last lemma. Let $\sigma_1, \dots, \sigma_e$ be the e embeddings that leave λ fixed. Then, we have that for every i ,

$$(\sigma_i(\beta_f) - \sigma_i(\beta_g))(\sigma_i(\beta_f) - \sigma_i(\alpha_g)) = \lambda^n \sigma_i(\eta \beta_f)$$

divides also the resultant, and therefore ℓ^n divides the resultant. \square

Thus, given $P_{f,p}$ and $P_{g,p}$ coprime (the coprime condition ensures that the resultant will not be equal 0), the finite number of integers dividing their resultant are the only possibilities of congruence between f and g outside p . We can use a second prime p' to determine the highest power of p which can bring also to a congruence. Using some additional primes we can still reduce this finite set of possible congruences. Let us remark that if f and g are not in the same conjugacy class, we can clearly always find an infinite number of primes such that $P_{f,p}$ and $P_{g,p}$ are coprime.

Still another easier way to obtain an upper bound in some specific cases is to apply Proposition 1.3.2.

Corollary 2.4.3. *If f and g are congruent modulo λ with $N_g \mid N_f$, then for any prime $p \neq \ell$ dividing N_f/N_g , $p^3 \nmid N_f$.*

Proof. With the notation from Proposition 1.3.2, in our case we always have $n_p \leq 2$. \square

2.5 Local congruence number

The result obtained using the algorithm with the resultant is not always optimal. In some cases it happens that ℓ^n divides all the resultants, but there is no congruence modulo λ^n between the newforms that we are comparing.

We might think that if f and g are congruent modulo λ^n , we could define a gcd in $\mathbb{Z}/\ell^n\mathbb{Z}[X]$ such that the gcd of \hat{P}_{f,p,ℓ^n} and \hat{P}_{g,p,ℓ^n} should be also non trivial, and then we could use this fact to improve the bound computed with the resultants' step. However, $\mathbb{Z}/\ell^n\mathbb{Z}[X]$ is not a UFD for $n > 1$ and therefore, polynomial theory over this ring does not work as well as over a field and in particular, gcd's over this ring are not defined. Nonetheless, we will try to get rid of this problem and use somehow this idea.

Using the Sylvester matrix, Ford ([Pau01]) provides an algorithm to approximate the gcd of two polynomials over a local field to any desired precision. We can not use directly this approximation, but this result inspired another use of this matrix.

Definition 2.5.1. *The **Sylvester matrix** $S_{\Phi,\Psi}$ of the polynomials $\Phi(X) = c_0X^s + \dots + c_s$ and $\Psi(X) = b_0X^t + \dots + b_t$ is the $(t+s) \times (t+s)$ matrix*

$$S_{\Phi,\Psi} := \left(\begin{array}{cccccc} b_0 & \dots & \dots & b_t & & 0 \\ & \ddots & & & \ddots & \\ 0 & & b_0 & \dots & \dots & b_t \\ c_0 & \dots & \dots & c_s & & 0 \\ & \ddots & & & \ddots & \\ 0 & & c_0 & \dots & \dots & c_s \end{array} \right) \left. \begin{array}{l} \vphantom{\begin{matrix} b_0 \\ \dots \\ b_t \end{matrix}} \right\} s \\ \left. \begin{array}{l} \vphantom{\begin{matrix} c_0 \\ \dots \\ c_s \end{matrix}} \end{array} \right\} t$$

If reduce the matrix to the Echelon form, we see that the last non zero row is a linear combination of the polynomials Φ and Ψ . Hence, if we want the polynomials to have a common root modulo some prime, this linear combination must be 0 modulo this prime.

Definition 2.5.2. *Given two polynomials P and Q , we define the **congruence number** $c(P,Q)$ of P and Q as the last coefficient of the Echelon form of the Sylvester matrix over \mathbb{Z} of P and Q . If P and Q correspond to the characteristic polynomial of a p -Frobenius (or a p -Hecke operator, as we will use later), we call $c_p(P,Q)$ (or simply c_p) also the **local congruence number** at p of f and g .*

Remark 2.5.3. In [TW09] the congruence number is defined in another way, but it is proven that both definitions are equivalent.

Also in [TW09] the following results are proven:

Proposition 2.5.4. Let $P, Q \in \mathbb{Z}[X]$ be coprime polynomials and let ℓ^n be the exact power of ℓ dividing $c(P, Q)$.

Then there are no $\alpha, \beta \in \overline{\mathbb{Z}}$ such that

- (i) $P(\alpha) = Q(\beta) = 0$ and
- (ii) $\alpha \equiv \beta \pmod{\ell^m}$ for any $m > n$.

Proposition 2.5.5. Let P, Q be coprime monic polynomials in $\mathbb{Z}[X]$ (or $\mathbb{Z}_\ell[X]$) and let ℓ^n be the highest power of ℓ dividing the congruence number $c(P, Q)$ and let $r, s \in \mathbb{Z}[X]$ (or $\mathbb{Z}_\ell[X]$) be polynomials such that $c(P, Q) = rP + sQ$ with $\deg(r) < \deg(Q)$ and $\deg(s) < \deg(P)$.

- (a) If $n = 0$, then no root of P is congruent to a root of Q modulo ℓ .
- (b) If $n = 1$, then there are α, β in \mathbb{Z} (in \mathbb{Z}_ℓ , respectively) with $P(\alpha) = Q(\beta) = 0$ such that they are congruent modulo ℓ , and incongruent modulo ℓ^2 .
- (c) Suppose now that $n \geq 2$ and that \overline{P} does not have any multiple factors and also that \overline{Q} does not have any multiple factors (i.e. $\ell \nmid c(P, P')$ and $\ell \nmid c(Q, Q')$). Then there are α, β in $\overline{\mathbb{Z}}$ (in $\overline{\mathbb{Z}}_\ell$, respectively) with $P(\alpha) = Q(\beta) = 0$ such that they are congruent modulo ℓ^n , and incongruent modulo ℓ^{n+1} .
- (d) Suppose that $n \geq 2$. In general, we have the following result:
 - (i) If \overline{s} and \overline{Q} are coprime, then there are α, β in $\overline{\mathbb{Z}}$ (in $\overline{\mathbb{Z}}_\ell$, respectively) with $P(\alpha) = Q(\beta) = 0$ such that they are congruent modulo ℓ^m with $m = \lceil \frac{n}{\deg(Q)} \rceil$.
 - (ii) If \overline{r} and \overline{P} are coprime, then there are α, β in $\overline{\mathbb{Z}}$ (in $\overline{\mathbb{Z}}_\ell$, respectively) with $P(\alpha) = Q(\beta) = 0$ such that they are congruent modulo ℓ^m with $m = \lceil \frac{n}{\deg(P)} \rceil$.

Given two polynomials $P_{f,p}$ and $P_{g,p}$, with Proposition 2.5.4 we obtain an upper bound for the possible congruences between $P_{f,p}$ and $P_{g,p}$ (local upper bound at p). On the other side, with Proposition 2.5.5 we obtain a lower bound and, in some cases, the exact congruence between $P_{f,p}$ and $P_{g,p}$.

Remark 2.5.6. *If $n = 1$, gcd's in $\mathbb{Z}/\ell\mathbb{Z}$ are well defined and therefor, it is clear that $c(P_{f,p}, P_{g,p}) \equiv 0 \pmod{\ell}$ if and only if*

$$\deg(\gcd(\hat{P}_{f,p,\ell}, \hat{P}_{g,p,\ell})) > 0.$$

Moreover, in this case we can explicitly compute the $\gcd(\hat{P}_{f,p,\ell}, \hat{P}_{g,p,\ell})$ to get more information about the image of the mod ℓ representation, as we will see in Sections 2.15 and before Remark 3.4.1.

Remark 2.5.7. *Let us remark that, given 3 polynomials $P_{f,p}$, $P_{g,p}$ and $P_{h,p}$, if $\gcd(c(P_{f,p}, P_{g,p}), c(P_{f,p}, P_{h,p}), c(P_{g,p}, P_{h,p})) > 1$, even though the conditions of Proposition 2.5.5, part c are satisfied, this does not imply that there exist a common root of the three polynomials. If we want to check if they have a root in common modulo some ℓ^n , one can reduce modulo ℓ^n the coefficients of the Echelon form of the Sylvester matrix of $P_{f,p}$ and $P_{g,p}$ and take the last non zero row as a polynomial in $\mathbb{Z}/\ell^n\mathbb{Z}[X]$. Then, we compute the Sylvester matrix of this polynomial and $P_{h,p}$ and we check if now this congruence number is still 0 modulo ℓ^n .*

2.6 $Q_{f,p}$

In some cases, the polynomials $P_{f,p}$ have large degree (for $N \leq 2000$, some degrees are greater than 200), and so the computation can be time consuming. The Eichler-Shimura relation allows us to replace Frobenius endomorphism by Hecke endomorphism. Let $Q'_{f,p} := X - a_p(f)$ denote the minimal polynomial of the eigenvalue of the p -Hecke Operator on f . As we did before with $P_{f,p}$, we take the product of all Q' so that we obtain a polynomial with integer coefficients.

$$Q_{f,p} := \prod_{\sigma} Q'_{\sigma(f),p}.$$

We denote also $\hat{Q}_{f,\ell^n,p}$ the reduction modulo ℓ^n of $Q_{f,p}$.

Remark 2.6.1. *The upper bound from Section 2.4 can be also computed using $Q_{f,p}$ instead of $P_{f,p}$. We just have to apply Lemma 2.4.1 to obtain a similar result as Lemma 2.4.2.*

The degree of the Q polynomials is the half of the degree of the P 's. Hence, the time needed to compute every gcd is reduced roughly to $1/4$, because the matrices that we have to reduce to the Echelon form have dimension $\frac{n}{2} \times \frac{n}{2}$ compared with the $n \times n$ that they had before.

2.7 Improving the global upper bound

In Proposition 2.5.4 we saw that given two polynomials, the congruence number provides an upper bound for the possible congruences between them.

Since the resultant of two polynomials can be computed as the determinant of their Sylvester matrix, it is clear that the congruence number will always divide the resultant, and therefore it will be an equal or better bound. Thence, we can repeat the algorithm with the resultant, but now taking instead the congruence number.

First of all, we compute the congruence numbers $c_p = c(Q_{f,p}, Q_{g,p})$ for all primes $p \nmid N_f$ up to some bound **pBound** (in the next section we discuss how big must be this bound). We compute then a slightly modified greatest common divisor of all c_p , taking into account that each c_p does not give us information about the prime p .

Let $V_p(c)$ be the inverse of the p -absolute value of c

$$V_p(c) = |c|_p^{-1} = p^{v_p(c)}.$$

If we have two c_{p_1} and c_{p_2} , the first great common divisor that we compute will be

$$c^{(p_2)} = \gcd(c_{p_1} \cdot V_{p_1}(c_{p_2}), c_{p_2} \cdot V_{p_2}(c_{p_1})). \quad (2.3)$$

Once we have one c computed, we can improve it for the other p_i with

$$c^{(p_i)} = \gcd(c^{(p_{i-1})}, c_{p_i} \cdot V_{p_i}(c^{(p_{i-1})})). \quad (2.4)$$

This bounds will be a fairly good upper bound of the global congruence number. Actually, if we take enough p_i 's, we expect that this upper bound will converge indeed to the true value of the global congruence number. Since $c^{(i)} \in \mathbb{N}$, there exists one i_0 such that $L^+ = c^{(i)}$ for every $i > i_0$.

We have seen that the polynomials $Q_{f,p}$ and $Q_{g,p}$ can determine the non existence of congruences. Furthermore, we wonder if just the product over all conjugates of $a_p(f)$ and $a_p(g)$ (i.e. the coefficients of degree 0 of $Q_{f,p}$ and $Q_{g,p}$) already suffice to compute congruences:

Remark 2.7.1. Let $q_{f,p,0} = \text{Norm}(a_p(f))$ be the coefficient of degree 0 of $Q_{f,p}$. There exist examples with $q_{f,p,0} = q_{g,p,0}$ for every prime p (p.e. (117, 3) and (39, 2)) which gives us no information about the congruences between f and g . In the mentioned example, f and g are twisted and for every prime p , $a_p(f) = \pm a_p(g)$. Then, if $Q_{f,p} = X^2 + q_{f,p,1}X + q_{f,p,0}$, $Q_{g,p} = X^2 \pm q_{f,p,1}X + q_{f,p,0}$.

If we consider $l_p := \text{Norm}(a_p(f) - a_p(g))$ instead of considering $\text{Norm}(a_p(f))$ and $\text{Norm}(a_p(g))$ separately, we can obtain correct results. We just have to make the gcd's of l_p for some p 's, as we did with the resultant to obtain an upper bound. However, in this case we have to compute frequently in extension fields of huge degree. This problem is due to the fact that $\text{Norm}(a_p(f) - a_p(g)) \neq \text{Norm}(a_p(f)) - \text{Norm}(a_p(g))$.

2.8 pBound

Now we see that using a couple of primes, we can easily obtain an upper bound for the global congruence number. However, if we want to have an accurate bound, how many different p 's do we have to use?

We did the following study: We fixed a bound **pBound** (in our case, **pBound** = 1000). Given two newforms, we computed $c^{\text{pB}} = c^{(p_i)}$, being p_i the biggest prime such that $p_i \leq \text{pBound}$. We assumed that $L^+ = c^{\text{pB}}$ (it means, we supposed that **pBound** is enough to determine the global upper bound). For every prime $\ell < 1000$, we stored the smallest p_0 such that $v_\ell(L^+) = v_\ell(c^{\text{pB}})$. This p_0 is the smallest prime that forces the newforms not being congruent modulo $\ell^{v_\ell(L^+)+1}$.

In order to get an estimate of the reliability of this **pBound**, for every $N \leq 2000$ and every prime $\ell < 1000$ we searched which is the maximum of all these minimal p_0 's, for all couples of newforms with $N_i \leq N$. If all these p_0 's are far from **pBound**, taking into account the equidistribution of Frobenius elements, we can think heuristically that our results are trustworthy. However, if the p_0 go close to **pBound**, we can think that perhaps $c^{\text{pB}} \neq L^+$ and we should take a bigger **pBound** to find that $c^{\text{pB}} = L^+$.

Figure 2.1 shows some of these results for $\ell \leq 29$ and a couple of N 's. We can see clearly that when ℓ increases, p decreases. In fact, if we check more accurately, we see that for $N \leq 2000$, $p \leq 53$ suffices to exclude congruences for all primes $\ell < 1000$ except $\ell = 2, 3, 5, 7, 11, 17, 37, 43$ and 53. The maximal

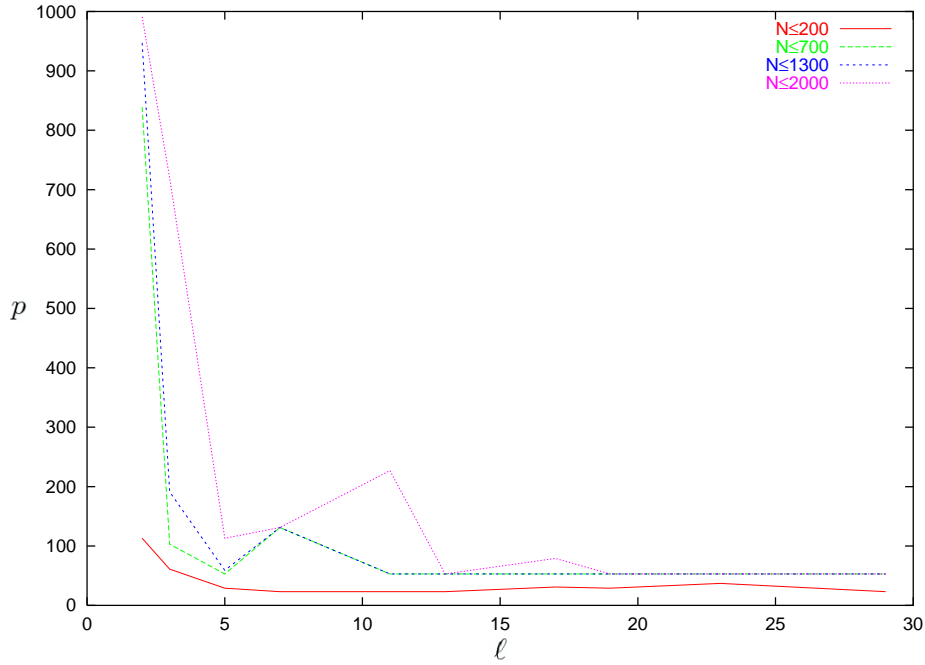


Figure 2.1: Maximal p with respect to ℓ for some N

p_0 that we obtained in each of these cases are

ℓ	2	3	5	7	11	17	37	43	53
p	991	719	113	131	227	79	829	61	83

As we see, most of the p 's are very small. The exceptions are $\ell = 2, 3$ and 37 (and perhaps 11). Figure 2.2 shows how these possible pathological p for every ℓ (except $\ell = 37$) increase with growing N .

Looking the figure, we see that for $\ell = 2$ the graphic increases very quickly. Thus, for $\ell = 2$ and N around 700, pBound will be already too small and c^{pB} will probably be bigger than L^+ (since the weight we are working with is $k = 2$, we already expected that this case could be problematic). For $\ell = 3$ we get one case in which $p = 719$, but the graphic increases quite slowly nevertheless. Whence, we expect that we will have no (or very few) cases in which we should increase pBound . The case $\ell = 37$ is quite strange, because in this case we had that $p \leq 53$ already sufficed to exclude congruences until $N = 1368$ and then it appears suddenly one $p = 829$. This does not make us think that $\ell = 37$ is specially bad, but that it is possible that, for some ℓ 's,

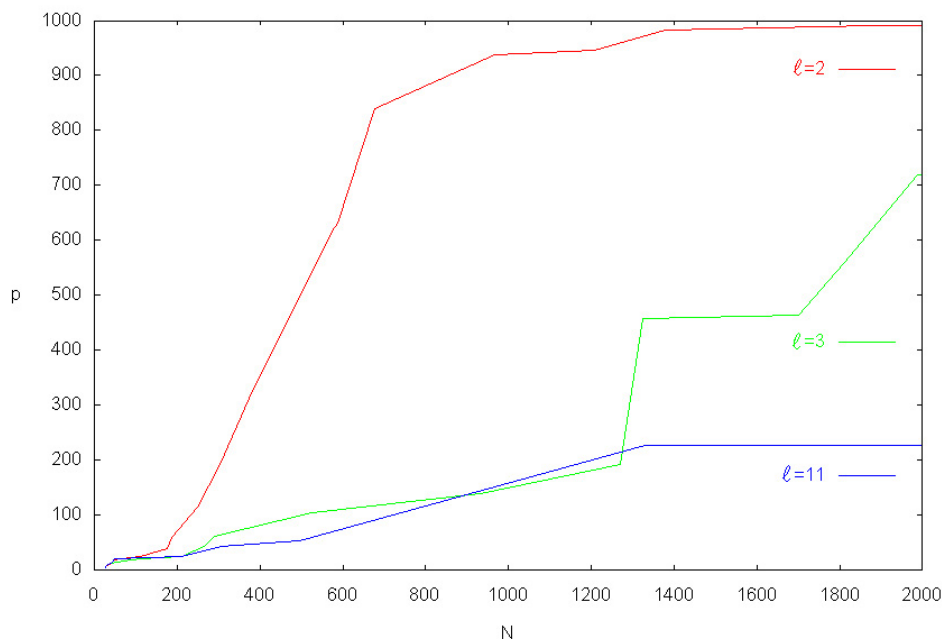


Figure 2.2: Maximal p with respect to N for the worst ℓ 's

we have some couples of newforms in which c^{PB} is not optimal; and at the same time, it seems that these cases will be quite isolated. Thus, we expect that, for $N \leq 2000$ and $\ell \neq 2$, $\text{pBound} = 1000$ gives already a fairly correct global upper bound, i.e. in most of the cases we will have $L^+ = c^{\text{PB}}$.

Remark 2.8.1. *An effective version of Chebotarev gives an explicit bound for p , but even under GHR, this is much too big.*

2.9 Description of UpperBound1.0

First step: Create a data base with all the characteristic polynomials $Q_{f,p}$ that we will use (in our case, $p < 1000$). For every newform (N, i_N) , we save the coefficients of the 168 polynomials in the files $\mathbf{N}-i_N.\text{txt}$.

We recall that $V_p(c) = |c|_p^{-1} = p^{v_p(c)}$.

Algorithm: UpperBound1.0

Input: Two different newforms $f = (qN, i_f)$ and $g = (N, i_g)$ ($q \in \mathbb{N}$) and

a bound **pBound**.

Output: L^+ such that if $\bar{\rho}_{f,\ell^n} \sim \bar{\rho}_{g,\ell^n}$, then $\ell^n \mid L^+$

i) p_1, p_2 minimal such that $p_i \nmid qN$, and $\gcd(Q_{f,p_i}, Q_{g,p_i}) = 1$.
 $c_{p_i} \leftarrow c(Q_{f,p_i}, Q_{g,p_i})$.

ii) $L^+ \leftarrow \gcd(c_{p_1} \cdot V_{p_1}(c_{p_2}), c_{p_2} \cdot V_{p_2}(c_{p_1}))$

iii) For every ℓ such that $\ell \mid q$ and $\ell^3 \mid qN$, $L^+ \leftarrow V_\ell(L^+)$.
 If L^+ is 1, **return** 1.

iv) For every $p \leq \mathbf{pBound}$ such that $p \nmid qN$ and $\gcd(Q_{f,p}, Q_{g,p}) = 1$:
 $L^+ \leftarrow \gcd(L^+, c(Q_{f,p}, Q_{g,p}) \cdot V_p(L^+))$.
 If L^+ is 1, **return** 1.

v) **return** L^+ .

The modified gcd from steps (ii) and (iv), in which we use $V_p(c)$ come from formulae (2.3) and (2.4). Step (iii) comes from Corollary 2.4.3.

In case we take a **pBound** so small that we do not find any p_1 and p_2 satisfying the conditions from step (i), we just have to take a bigger **pBound** to ensure that we find them.

In our case we applied this algorithm for all couples of newforms with levels $N_g \mid N_f \leq 2000$ and **pBound** = 1000 and we obtained a huge list with all couples such that $L^+ > 1$. The first elements of this list can be found in Appendix A and the complete table is in **UpperBound1.0.res**.

Let us remark that we also found the possible congruences for $\ell = 2$, even if we already saw that the computed bound might be not optimal. We also did not check if the corresponding residual representations are reducible or not, because we do not need this condition to compute an upper bound.

Let us recall that, if Ribet's Lowering the Level can be generalized modulo λ^n (as it is shown for some specific cases in the next chapter, and it is questioned later in Chapter "Further work"), the condition " N_g divides N_f " can be taken without loss of generality when we are comparing minimal newforms.

Table 2.1 shows some remarkable elements computed with **UpperBound1.0**. The first block corresponds to the elements we found with the biggest L^+ . The next block shows, for each exponent n , the elements that we found with biggest ℓ .

N_f	i_f	N_g	i_g	L^+
$1966 = 2 \cdot 983$	6	983	2	$53 \cdot 2917069273 \cdot 5098557521$
$1977 = 3 \cdot 659$	7	659	4	$2 \cdot 3 \cdot 17 \cdot 61 \cdot 6738359 \cdot 2454829873$
$1797 = 3 \cdot 599$	6	599	3	$5^3 \cdot 389 \cdot 779881437372101$
$1941 = 3 \cdot 647$	4	647	3	$2551 \cdot 5539230441648341$
$1822 = 2 \cdot 911$	4	911	3	$2364851 \cdot 3903737869711$
$1937 = 13 \cdot 149$	4	149	2	$405607581 = 3^{10} \cdot 6869$
$1475 = 5^2 \cdot 59$	18	$5^2 \cdot 59$	11	$512 = 2^9$
$1854 = 2 \cdot 3^2 \cdot 103$	20	$3^2 \cdot 103$	5	$256 = 2^8$
$1105 = 5 \cdot 13 \cdot 17$	7	$13 \cdot 17$	6	$256 = 2^8$
$618 = 2 \cdot 3 \cdot 103$	11	$3 \cdot 103$	3	$256 = 2^8$
$1622 = 2 \cdot 811$	4	811	2	$268635771 = 3^7 \cdot 122833$
$1686 = 2 \cdot 3 \cdot 281$	10	$2 \cdot 281$	4	$28561 = 13^4$
$1934 = 2 \cdot 967$	2	967	1	$12528300625 = 5^4 \cdot 20045281$
$1643 = 31 \cdot 53$	3	53	2	$1250 = 2 \cdot 5^4$
$1401 = 3 \cdot 467$	1	467	2	$2160625 = 5^4 \cdot 3457$
$1158 = 2 \cdot 3 \cdot 193$	13	$2 \cdot 193$	4	$1250 = 2 \cdot 5^4$
$1909 = 23 \cdot 83$	4	23	1	$1331 = 11^3$
$1959 = 3 \cdot 653$	3	653	3	$7627463529 = 3 \cdot 7^3 \cdot 229 \cdot 32369$
$1551 = 3 \cdot 11 \cdot 47$	7	$11 \cdot 47$	11	$53138 = 2 \cdot 163^2$
$1742 = 2 \cdot 13 \cdot 67$	9	$2 \cdot 67$	1	$5329 = 73^2$
$1491 = 3 \cdot 7 \cdot 71$	3	$7 \cdot 71$	3	$2209 = 47^2$
$1678 = 2 \cdot 839$	8	839	2	$2 \cdot 1750283935190857471$
$1707 = 3 \cdot 569$	4	569	2	$2 \cdot 122272440801294601$
$1941 = 3 \cdot 647$	4	647	3	$2551 \cdot 5539230441648341$
$1839 = 3 \cdot 613$	4	613	3	3726338419619653

Table 2.1: Remarkable elements of UpperBound1.0.res.

- The biggest L^+ obtained is as big as $L^+ = 7.88 \cdot 10^{20}$.
- The biggest n that appears is $n = 10$ for $\ell = 3$. Since this example corresponds to a big N (1937), Figure 2.2 suggests that in this case one should check for more p 's (i.e. pBound may be too small).
- The biggest n that appears for the “non reliable” case $\ell = 2$ is $n = 9$.

- For $\ell = 7$, we have one example with $n = 7$. In this case, $N = 1622$ and hence it seems to be small enough to consider it being reliable.
- For $n = 4$ it appear the first cases with $\ell = 5$ and $\ell = 13$.
- With $n = 3$ there are already $\ell = 11$ and 7 .
- For $n = 2$ we already find many different ℓ 's up to 163 .

2.10 Congruences between f and $\sigma(f)$

It is interesting also to determine when there are congruences between a newform and one of its Galois conjugates. An easy way to obtain an upper bound, consists on applying a similar algorithm from Section 2.2 (and therefore we can talk again about congruences modulo λ^n instead of ℓ^n) but this time changing the resultant for the discriminant. The following lemma justifies why we can make this change.

Lemma 2.10.1. *If there is a congruence between f and $\sigma(f)$ (modulo some λ^n) for an embedding $\sigma \neq Id$, then the discriminant D of $Q_{f,p}$ ($p \nmid \ell N$) is divisible by ℓ^n .*

Proof. First of all, if K_f is not Galois, we can not simply compare the coefficients $a_p(f)$ with $a_p(\sigma(f))$, because $a_p(\sigma(f))$ might not be in K_f . Hence, the congruences have to be made in the Galois completion \hat{K}_f of K_f .

Let $\ell = \lambda^e \cdot \lambda_1^e \cdot \dots \cdot \lambda_s^e$ be the decomposition of ℓ in \hat{K}_f . Let Σ be the set of embeddings of K_f in \mathbb{C} . Since $Q_{f,p} = \prod_{\sigma' \in \Sigma} (X - a_p(\sigma'(f)))$, if there exist two elements $\sigma', \sigma'' \in \Sigma$ such that $a_p(\sigma'(f)) = a_p(\sigma''(f))$, then $D = 0$.

Otherwise, let $\sigma_1 \dots \sigma_e$ be the e embeddings such that $\sigma(\lambda) = \lambda$. Since $a_p(\sigma_i(f)) \neq a_p(\sigma_j(f))$ for every $i \neq j \in \{1 \dots e\}$, we have e different tuples $(a_p(\sigma_i(f)), a_p(\sigma_i(\sigma(f))))$.

Since f and $\sigma(f)$ are congruent modulo λ^n , we have that $a_p(f) - a_p(\sigma(f)) = \lambda^n \alpha$, for one $\alpha \in \mathcal{O}$. Whence, for each tuple, we have that $a_p(\sigma_i(f)) - a_p(\sigma_i(\sigma(f))) = \lambda^n \sigma_i(\alpha)$ (because $\sigma_i(\lambda) = \lambda$). Therefore, we have e different elements $\lambda^n \sigma_i(\alpha)$ dividing D . Thence, λ^{en} must divide D .

Since \hat{K}_f is Galois, for every λ_i , there exists one σ'_i such that $\sigma'_i(\lambda) = \lambda_i$. We have that, if $D = \lambda^{en} \cdot \beta$, then

$$\sigma'_i(D) = \sigma'_i(\lambda^{en} \cdot \beta) = \lambda_i^{en} \sigma'_i(\beta).$$

Then, we have that, for every i , λ_i^{en} divides D . Therefore,

$$D = \lambda^{en} \cdot \lambda_1^{en} \cdot \dots \cdot \lambda_s^{en} \cdot \beta' = \ell^n \beta'$$

and hence ℓ^n divides D . □

In the same way as we did before, this bound can be reduced using the congruence number. This time, we have to take the polynomials $Q_{f,p}$ and its derivative $Q'_{f,p}$. Then, the analogous algorithm of `UpperBound1.0` follows (in case that for every prime p , $c(Q_{f,p}, Q'_{f,p}) = 0$ we can not discard any possible congruence and the algorithm returns 0).

Algorithm: `UpperBound1.1`

Input: A newform $f = (N, i_f)$ and a bound `pBound`.

Output: L^+ such that if $\bar{\rho}_{f,\ell^n} \sim \bar{\rho}_{\sigma(f),\ell^n}$, then $\ell^n \mid L^+$

- i) p_1, p_2 minimal such that $p_i \nmid N$, and $c(Q_{f,p_i}, Q'_{f,p_i}) \neq 0$.
 If $c(Q_{f,p}, Q'_{f,p}) = 0 \forall p \leq \text{pBound}$, **return** 0.
 $L_i \leftarrow c(Q_{f,p_i}, Q'_{f,p_i})$.
- ii) $L^+ \leftarrow \gcd(L_1 \cdot V_{p_1}(L_2), L_2 \cdot V_{p_2}(L_1))$
- iii) For every $p \leq \text{pBound}$, $p \nmid N$, $Q_{f,p}$ irreducible:
 $L^+ \leftarrow \gcd(L^+, c(Q_{f,p}, Q'_{f,p}) \cdot V_p(L^+))$.
 If L^+ is 1, **return** 1.
- iv) **return** L^+ .

We applied this algorithm to all forms with level $N \leq 2000$ and we stored the results in the file `N,i eq M,j.res`. In Appendix B we show the first elements of this list. It is remarkable to say that in some cases this bound is huge and it might be far from the reality. For example:

$$f = (1931, 2)$$

$$L^+ = 2^{1113} \cdot 5 \cdot 11 \cdot 4327 \cdot 17583293051 \cdot 221188513448417 = 102990589235232943$$

$$408337752832711913341450897876573336497366777834092065184012574274$$

$$203920494440055352682091440590466845686343036217737007310915086380$$

$$478559620613210798042891557146989243093226383181738610547147636533$$

$$596743361980310844147595603184757659840421229929405526190694856368$$

$$950511273336078540689071951302097801946327093281283247127892360862$$

$$020570193831395328 \approx 1.03 \cdot 10^{365}$$

or

$$f = (1979, 3)$$

$L^+ = 5814254014865651451202035635397258842607100459214961472869166$
 $183466323995187762575673735179435021599630812954839231709187702102$
 $614977309025528158485794489063674941476317861549257385743011960989$
 $231458675288997724169939545389491239021744686204379372408180244298$
 $710044591960348244641721024796722028115261123598255040931156960373$
 $97153890435072 \approx 5.81 \cdot 10^{338}, \dots$

2.11 Global lower bound I: Hecke Bound

Until now, for any couple of newforms, we can already determine one finite number L^+ such that these forms are not congruent outside L^+ . From now on, we want to determine a lower bound $L^-, L^-(f, g)$ such that for every prime power ℓ^n dividing L^- , we can ensure the existence of a congruence between the newforms modulo ℓ^n . To do it we will use the Hecke Bound.

Definition 2.11.1. *Let f be in $S_2(N)$. We define the (improved) **Hecke bound** of f (also called **Sturm bound**) as*

$$H_f := \frac{m}{6} - \frac{m-1}{N}$$

where $m = [SL_2(\mathbb{Z}) : \Gamma_0(N)]$ (the “improved” comes because the original bound was just $\frac{m}{6}$).

We denote H_f simply by H if f is clear by the context.

Theorem 2.11.2. *The Hecke algebra \mathbb{T} acting on the space $S_2(N)$ is generated as a \mathbb{Z} -module (resp. algebra) by the Hecke operators T_n for $n \leq H$ (resp. T_p for $p \leq H$, p prime).*

Proof. Theorem 9.23 and Remark 9.24 from [Ste07]. □

Theorem 2.11.3. *Let f and g be newforms of levels $N_g \mid N_f$ and let λ be a prime ideal in the ring of integers \mathcal{O} of a number field. Suppose that for all $i \leq H_f$*

$$a_i(f) \equiv a_i(g) \pmod{\lambda}.$$

Then $f \equiv g \pmod{\lambda}$.

Proof. Corollary 9.19 from [Ste07]. □

Theorem 2.11.4. *Let f and g be newforms of levels $N_g \mid N_f$ and let λ be a prime ideal in the ring of integers \mathcal{O} of a number field. Suppose that for all primes $p \leq H_f$*

$$a_p(f) \equiv a_p(g) \pmod{\lambda^n}.$$

Then $f \equiv g \pmod{\lambda^n}$.

Proof. For $n = 1$ this is Theorem 9.22 from [Ste07] with trivial character.

In general, \mathbb{T} is generated as a \mathbb{Z} -algebra by the Hecke operators T_p , for every p prime $p \leq H$ (Theorem 2.11.2). Then, $\mathbb{T}_{\mathcal{R}}$ is generated as an \mathcal{R} -algebra by the same generators. Taking $\mathcal{R} = \mathcal{O}_{\lambda}/\lambda^n$, if the coefficients $a_p(f)$ and $a_p(g)$ are congruent modulo λ^n for every prime until the Hecke bound, then $a_p(f)$ and $a_p(g)$ are congruent for every prime p . Therefore, f and g are congruent modulo λ^n . □

Given two newforms f and g and a prime p , using Corollary 2.5.5 we can find a local lower bound of congruence between $Q_{f,p}$ and $Q_{g,p}$. If we get that for every $p \leq H$ there is an ℓ^n dividing all the lower bounds, it seems that we could already guarantee that there is a congruence *mod* ℓ^n between f and g (*mod* ℓ^n and not *mod* λ^n because of the use of the local congruence number between $Q_{f,p}$ and $Q_{g,p}$).

However, let $\sigma(g)$ be a conjugate of g and suppose that, for example, the following case occurs: let \mathbb{P} be the set of prime numbers and let \mathbb{P}_1 and \mathbb{P}_2 be such that $\mathbb{P}_1 \cup \mathbb{P}_2 = \mathbb{P}$, $\#(\mathbb{P}_1 \cap \mathbb{P}_2) < \infty$ and $\#\mathbb{P}_1 = \#\mathbb{P}_2 = \infty$.

Let $Q'_{f,p} = X - a_p(f)$, as in Section 2.6. For every p , we have

$$\begin{aligned} Q'_{f,p} &\equiv Q'_{g,p} && \text{if } p \in \mathbb{P}_1 \\ Q'_{f,p} &\not\equiv Q'_{g,p} && \text{if } p \notin \mathbb{P}_1 \\ Q'_{f,p} &\equiv Q'_{\sigma(g),p} && \text{if } p \in \mathbb{P}_2 \\ Q'_{f,p} &\not\equiv Q'_{\sigma(g),p} && \text{if } p \notin \mathbb{P}_2. \end{aligned}$$

In this case, even though we can get that for every p , ℓ^n divides the local lower bound, we do not have a congruence modulo ℓ^n neither between f and g , nor between f and $\sigma(g)$. Nevertheless, we think that this situation actually never happens:

Conjecture 2.11.5. *Let f and g be newforms such that g is not in the conjugacy class of f (i.e., for every $\sigma \in \Sigma$, $g \neq \sigma(f)$). For a fixed prime*

power ℓ^n and every prime p , suppose that there exist $\sigma_{g,p} \in \Sigma_K$ such that $a_p(f) \equiv \sigma_{g,p}(a_p(g)) \pmod{\lambda^n}$. Then, there exists $\sigma_g \in \Sigma_K$ such that $f \equiv \sigma_g(g) \pmod{\lambda^n}$.

From now on in this chapter, we assume that Conjecture 2.11.5 is always satisfied.

Then, applying Theorem 2.11.4, we get the following algorithm. Given two newforms f and g and the upper bound L^+ obtained with `UpperBound1.0` we do the following.

For every $\ell \mid L^+$ and every prime $p \leq H$, let ℓ^{n_p} be the local lower bound between $Q_{f,p}$ and $Q_{g,p}$ obtained from Corollary 2.5.5 (b), (c) or (d). We compute

$$L_{1,\ell}^- = \ell^{\min_{p \leq H} (n_p)},$$

and we take the product $L_1^- = \prod_{\ell \mid L^+} L_{1,\ell}^-$.

2.12 Global lower bound II

Following ideas of G. Wiese one can hope to get milder conditions in Theorem 2.11.5 for the primes $p \mid N_f$. Let K be a number field with ring of integers \mathcal{O} and λ a place dividing ℓ . Given an integer n , let $\gamma(n)$ be as defined in equation (2.1) (Section 2.2).

Definition 2.12.1. *Let $N_g \mid N_f$ be two integers. For any positive divisor d of N_f/N_g , we define the degeneracy map*

$$\begin{aligned} \phi_d : (\mathcal{O}/\lambda^{\gamma(n)}\mathcal{O})[[q]] &\rightarrow (\mathcal{O}/\lambda^{\gamma(n)}\mathcal{O})[[q]] \\ q &\mapsto q^d. \end{aligned}$$

Let $g \in S_k(N_g)$ be a modular form. The old space of g modulo ℓ^n is defined as the $\mathcal{O}/\lambda^{\gamma(n)}\mathcal{O}$ -span of $\{\phi_d(g)\}$, where d runs through all the positive divisors of N_f/N_g and ϕ_d is applied to the standard q -expansion of g modulo ℓ^n .

Proposition 2.12.2. *Let f, g be as above and assume that the residual Galois representations at ℓ of f and g are absolutely irreducible. Let $\phi_d(g)$, $d \mid N_f/N_g$ be the finitely many Hecke eigenforms modulo ℓ^n in the oldspace of g modulo ℓ^n of level N_f .*

Then the reductions modulo ℓ^n of the ℓ -adic Galois representations attached to f and g are isomorphic if there is d_0 such that $a_p(f) \equiv a_p(\phi_{d_0}(g))$ modulo ℓ^n for p prime between 1 and H .

Proof. The assumptions imply that the coefficients satisfy $a_p(f) \equiv a_p(g) \pmod{\ell^n}$ for all primes p except possibly those with p dividing m . Thus, applying Corollary 1.2.5 the result follows. \square

Let $p \mid N_f$. In [Wie04] is described how the characteristic polynomial of the p -Hecke Operator on the old space of g in level N_f can be computed:

Let $m = N_f/N_g$ and let us suppose that r is the maximum exponent so that $p^r \mid m$. Let Q'_{g,p^r} denote the characteristic polynomial of the Hecke operator T_p acting on the old space of g in level $p^r N_g$. Then, Q'_{g,p^r} is the characteristic polynomial of the $(r+1) \times (r+1)$ matrix

$$\begin{pmatrix} a_p(g) & 1 & 0 & 0 & \dots & 0 \\ -\delta p & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & & \vdots \\ 0 & \dots & 0 & 0 & 0 & 1 \\ 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix} \quad (2.5)$$

where $\delta = 0$ if $p \mid N_g$ and $\delta = 1$ otherwise. Since r is the highest power dividing m , the characteristic polynomial Q'_{g,p,N_f} of the T_p acting on the space of level N_f will be just a power of Q'_{g,p^r} .

Let d_g be the dimension of K_g (the field generated by the coefficients of g). Now we want to compute the characteristic polynomial Q_{g,p,N_f} of T_p acting on the whole space of level N_f . As we did in Section 2.6, Q_{g,p,N_f} will be the product of all $Q'_{\sigma(g),p,N_f}$. This is equivalent to computing the characteristic polynomial of the $d_g \cdot (r+1) \times d_g \cdot (r+1)$ matrix resulting from (2.5), in which we substitute every 0 for the $d_g \times d_g$ dimensional 0_{d_g} matrix, 1 becomes the d_g -identity $\mathbf{1}_{d_g}$, $a_p(g)$ is the $d_g \times d_g$ matrix of the Hecke operator T_p on $S_2(N_g)$, and δ is either 0_{d_g} or $\mathbf{1}_{d_g}$.

Since all the elements under the diagonal are 0 for all the blocks under the second line of blocks, we already know that the characteristic polynomial of this big matrix will be the product of $X^{d_g(r-1)}$ and the characteristic polynomial of the block matrix

$$\left(\begin{array}{c|c} T_p & \mathbf{1}_{d_g} \\ \hline -\delta p^{k-1} \cdot \mathbf{1}_{d_g} & 0_{d_g} \end{array} \right). \quad (2.6)$$

If $Q_{g,p} = \sum_{i=0}^{d_g} c_i X^i$, the characteristic polynomial of (2.6) is

$$\sum_{i=0}^d \left(c_i X^{d_g-i} (X^2 - \delta p^{k-1})^i \right).$$

Hence, the characteristic polynomial Q_{g,p,N_f} of 2.5 is

$$Q_{g,p,N_f} = \sum_{i=0}^{d_g} \left(c_i X^{d_g r-i} (X^2 - \delta p^{k-1})^i \right), \quad (2.7)$$

which can be computed very quickly from $Q_{g,p}$. Let us remark that, if $p \mid N$, this polynomial is simply $X^{d_g r} \cdot Q_{g,p}$. Whence, we just have to compare $Q_{f,p}$ with $Q_{g,p}$ as usual, or with $X^{d_g r}$. On the other hand, it is interesting to see that if $p \nmid N$ and $d_g = 1$, then $Q_{g,p,N_f} = X^{r-1} \cdot P_{g,p}$ (where $P_{g,p}$ is the characteristic polynomial of the p -Frobenius element from Section 2.2).

The algorithm will run as follows. Assuming Conjecture 2.11.5 to be true, suppose that $\bar{\rho}_{f,\ell}$ and $\bar{\rho}_{g,\ell}$ are absolutely irreducible. Then, for every $\ell \mid L^+$ (such that $v_\ell(L^+) \neq v_\ell(L_1^-)$), we compute

$$L_{2,\ell}^- = \ell^{\min_{p \leq H}(\tilde{d}_p)}$$

with \tilde{d}_p defined as follows:

$$\begin{aligned} \text{If } p \nmid m, \quad \tilde{d}_p &= \text{local lower bound between } Q_{f,p} \text{ and } Q_{g,p} \\ \text{If } p \mid m, \quad \tilde{d}_p &= \text{local lower bound between } Q_{f,p} \text{ and } Q_{g,p,N_f}. \end{aligned}$$

The local lower bound is computed, as before, using Corollary 2.5.5.

Again, we compute $L_2^- = \prod_{\ell \mid L^+} L_{2,\ell}^-$.

2.13 Description of LowerBound1.0

Assume that Conjecture 2.11.5 is satisfied.

Algorithm: LowerBound1.0

Input: Two different newforms $f = (mN, i_f)$ and $g = (N, i_g)$ ($q \in \mathbb{N}$) and the upper bound L^+ from UpperBound1.0.

Output: An integer $L^- \leq L^+$ such that if ℓ^n divides L^- , there exist σ_1 and σ_2 such that $\bar{\rho}_{\sigma_1(f),\ell^n} \sim \bar{\rho}_{\sigma_2(g),\ell^n}$.

- i) $H \leftarrow$ Hecke Bound of f
- ii) $L^- \leftarrow 1$
- iii) For every ℓ prime dividing L^+
 - a) $L_1^-, L_2^- \leftarrow \ell^r$, where r is the maximal exponent such that $\ell^r \mid L^+$
 - b) if $\bar{\rho}_{g,\ell}$ is reducible, $L_2^- \leftarrow 1$
 - c) for every prime $p \leq H$ do
 - $d_p =$ local lower bound between $Q_{f,p}$ and $Q_{g,p}$
 - **if** $p \mid m$, $\tilde{d}_p =$ local lower bound between $Q_{f,p}$ and Q_{g,p,N_f}
else $\tilde{d}_p = d_p$
 - if d_p and \tilde{d}_p equal 0, next ℓ
 - $L_1^- \leftarrow \min(L_1^-, \ell^{d_p})$, $L_2^- \leftarrow \min(L_2^-, \ell^{\tilde{d}_p})$
 - d) $L^- \leftarrow L^- \cdot \max(L_1^-, L_2^-)$
 - e) next ℓ
- iv) **return** L^- .

Remark 2.13.1. *If we use this algorithm to find a congruence modulo ℓ^n between a newform f and an Eisenstein series, we can determine that the representation $\bar{\rho}_{f,\ell^n}$ is reducible.*

Remark 2.13.2. *Let f and g be such that $N_f = pN_g$, p prime. Let ℓ be such that $\ell \nmid L^-$ and $\ell \mid L^+$. Suppose that there is no newform f' of level N_f such that $\ell \mid L^+(f', g)$. We might think that in this case we could apply Ribet's Raising the Level to improve L^- .*

Definition 2.13.3. *Let $\bar{\rho}$ be an irreducible residual representation of conductor N . We say that $\bar{\rho}$ is p -new of level pN if there exists a newform f of level pN such that its associated residual representation $\bar{\rho}_f$ is equivalent to $\bar{\rho}$.*

Theorem 2.13.4 (Ribet). *Let $\bar{\rho}$ be modular, irreducible of level N , and $p \nmid \ell N$ a prime. Then, p satisfies one or both the identities*

$$\mathrm{tr}(\bar{\rho}(\mathrm{Frob}_p)) \equiv \pm(p+1) \pmod{\lambda}. \quad (2.8)$$

if and only if $\bar{\rho}$ is p -new of level pN .

Proof. [Rib90b]. □

However, Ribet's theorem does not bring better results as for each couple satisfying the conditions of Remark 2.13.2, the attached representations modulo ℓ are always reducible.

2.14 L^+ vs. L^- and other results

Table 2.2 shows some results comparing UpperBound and LowerBound.

N_f	i_f	N_g	i_g	L^-	L^+
1937	4	149	2	$3^9 \cdot 6869$	$3^{10} \cdot 6869$
866	5	433	3	$2 \cdot 89 \cdot 193 \cdot 787$	$2 \cdot 89 \cdot 193 \cdot 787$
626	6	313	2	$5^2 \cdot 37 \cdot 587$	$5^2 \cdot 37 \cdot 587$
982	6	491	2	$2 \cdot 29 \cdot 331$	$2^4 \cdot 29 \cdot 331$
613	1	613	2	$7 \cdot 47^2$	$7 \cdot 47^2$
1680	21	1680	14	2^3	2^3
1921	5	17	1	$2 \cdot 5^2$	$2^2 \cdot 5^2$
1986	10	562	4	13^4	13^4

Table 2.2: Comparing L^+ with L^- .

Notice that, in many cases, $L^+ = L^-$ and therefore all possible congruences are determined.

Remark 2.14.1. *We can find in our tables the following case: let $f = (N, i_f)$, $g = (N, i_g)$ and $h = (N \cdot M, i_h)$ be three newforms such that there is apparently one congruence between f and g modulo ℓ^n , there is also a congruence between f and h modulo ℓ^n , but if we look in the list there is no congruence between g and h , not even modulo ℓ . This can be explained with different places $\lambda_1, \lambda_2 \mid \ell$. f and g are congruent modulo λ_1 , f and h are congruent modulo a different λ_2 and this does not imply any congruence between g and h .*

Let us remark that even though Ribet's raising the level already determines in many cases the congruence between two newforms modulo ℓ (i.e, for the $n = 1$ case) this result does not work for couples of modular forms with exactly the same level. We show in Table 2.3 some of these examples.

N	i_f	i_g	L	d_f	d_g
$1241 = 17 \cdot 73$	2	1	$33684458 = 2 \cdot 1933 \cdot 8713$	17	11
$1719 = 3^2 \cdot 191$	9	8	$30955181 = 17 \cdot 487 \cdot 3739$	14	10
1249	2	1	$20685371 = 7 \cdot 2955053$	37	7
$1761 = 3 \cdot 587$	8	7	$17163962 = 2 \cdot 8581981$	18	9
$1939 = 7 \cdot 277$	4	3	$6055087 = 37^2 \cdot 4423$	23	7
$1773 = 3^2 \cdot 197$	8	6	$4146974 = 2 \cdot 13 \cdot 159499$	14	10
$1503 = 3^2 \cdot 167$	7	5	3699337	12	8
$1557 = 3^2 \cdot 173$	6	4	$2410477 = 1399 \cdot 1723$	12	10
1289	3	2	$444027 = 3 \cdot 283 \cdot 523$	39	6
1193	3	1	415577	55	3

Table 2.3: First 10 elements of the table of congruences for $N_f = N_g$ in which $L^+ = L^- = L$, ordered by L . The complete list can be found in the file `N1eqN2.res`.

This kind of examples play a very interesting rôle in Question 0.1.1 discussed in the introduction. We reformulate it here now as it is stated in [Fre01] (Question 3.5.16).

Question 2.14.2. *Let A_1 and A_2 be two abelian varieties defined over K with conductor N_1 and N_2 . Assume that for a number ℓ^n we find Galois invariant subgroups $C_i \subset A_i[\ell^n]$ with C_1 Galois-isomorphic to C_2 . How large (depending on K, N_i) has the order of C_1 to be in order to force A_1 and A_2 to have isogenous abelian subvarieties?*

In our case, we take A_f and A_g coming from two modular forms f and g both in a $\Gamma_0(N)$, with $d = \dim(A_g) \leq \dim(A_f)$. For each variety, we have the diagram as in Equation (1.1).

We suppose A_f^* and A_g^* have no isogenous abelian subvarieties ($A_f^* \not\approx A_g^*$). Then, if the question above can give us an explicit bound to compute the order of the biggest common subgroup of A_f^* and A_g^* , then it bounds also the maximal ℓ^n such that the representations attached to f and g can be congruent modulo ℓ^n .

It is possible to see, that the biggest ℓ is, the smaller is the dimension of $\hat{\rho}_{f,g,\ell}$ (see Definition 1.7.4). Therefore, we can conjecture that the cardinality of this intersection depends on N^d .

Conjecture 2.14.3. *Let K be a field. Given 2 abelian varieties as in Question 2.14.2, we have that $|C_i| < O(\max(N_1, N_2)^d)$. In our case, if the A_i are abelian varieties over \mathbb{Q} and they come from the modular forms f and g such that $N_g \mid N_f$, then $|A_f^* \cap A_g^*| < O(N_f^d)$.*

2.15 Heuristic realization of Galois Groups

One of the very interesting aspects about Galois representations is the realization of groups as Galois groups over a field K .

Definition 2.15.1. *Let G be a finite group and K a field. We say that G is **realizable** if there exists a Galois extension field $L \mid K$ such that G is isomorphic to the Galois group of this extension.*

For a given Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL_n(\mathcal{R})$, applying the isomorphism theorem we have that $\text{Im}(\rho) \simeq G_{\mathbb{Q}}/\text{Ker}(\rho)$, and since any quotient of $G_{\mathbb{Q}}$ by a closed normal group is a Galois group, we can realize the group $\text{Im}(\rho)$. This tool is used in [Die01], [DV00], [RV95], [Wieb] and in many other articles to realize infinitely many groups as Galois groups over \mathbb{Q} .

Now we will introduce two simple examples of realizations using this technique. First of all we will compute a large amount of gcd's of the characteristic polynomials of the Frobenius elements modulo a prime ℓ , and we compute the frequency in which each element appears. Then we consider all the possible subgroups of $GL_d(2)$ (where d is the dimension of $\hat{\rho}_{f,g,\ell}$, see Def. 1.7.4) and we discard all those who contain elements with characteristic polynomial different from the ones we computed; as well as the groups which do not contain at least one of our Frobenius. Then we compute the density of the characteristic polynomials for these groups, we compare with our group and we expect to find precisely one group with these densities. In this case, this procedure will have determined the structure of the image of our representation and therefore we have heuristically realized its associated group. But with this procedure we can determine not only the group we are realizing but also the polynomial having precisely this group as a Galois group. The way to do it is simply by searching in a database all possible polynomials with our Galois group, and then we compare the splitting of this polynomial modulo p with the p -Frobenius, until there is only one possibility left. However, this technique works only for small degrees, and hence it is would be very difficult to realize a new group.

Example 1: Let g be the 3rd eigenform of degree $N = 352$ (sorted as in Remark 1.1.7) and $f = (704, 10)$. If we take $\ell = 2$ and we compute the gcd's of $\hat{P}_{f,p,\ell}$ and $\hat{P}_{g,p,\ell}$ for all primes $p < 1000$, $(p, N) = 1$, we find that the different polynomials we get, have degree 2 and decompose always in factors $(X^2 + X + 1)$ or $(X + 1)^2$. If we look at the ratio in which each element appears, we get approximately $1/3$ and $2/3$, respectively. Chebotarev's Theorem ensures that the Frobenius elements are equally distributed, hence we have to look for the subgroups of $GL_2(2)$ satisfying this condition. An easy check shows that the only possible subgroup with this distribution is $GL_2(2)$ itself. In this way, we found a realization of the group $GL_2(2)$.

Now we are interested in determining explicitly the polynomial that generates this Galois group of order 6. We know by Remark 1.4.14 that this field must be unramified outside $2 \cdot 11$. Looking at [Klü] we get two candidates with these conditions: $X^3 - X^2 + X + 1$ and $X^3 - X^2 + 4X + 2$. The Galois group of both polynomials is $S_3 \simeq GL_2(2)$. In order to determine exactly which of these polynomials is the one generating our group, we simply compare their irreducibility modulo p for some different primes, with the irreducibility of the gcd of each p -Frobenius. We can see quickly that the first polynomial is the only one that satisfies this test and, therefore, is the polynomial we were looking for.

Example 2: Another example slightly more complicated is the following. If we take now the second and the third modular forms of level 353, we can see in our tables that they are congruent modulo 2. If we see which possible polynomials we get, they are the following: $(X + 1)^4$, $(X^2 + X + 1)^2$ and $X^4 + X^3 + X^2 + X + 1$. The distributions of the first 166 polynomials in this case are 40, 56 and 70 (24%, 34% and 42%) respectively. Since $X^4 + X^3 + X^2 + X + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$, the irreducible representation $\hat{\rho}_{f,g,2}$ has dimension 4. This increases a bit the difficulty because $GL_4(2)$ has 137 subgroups. Nevertheless, if we impose that the only possible characteristic polynomials are the ones we got and exactly those ones, we get only 2 possible subgroups. One has order 60 and the other 120. The distribution of the polynomials in each subgroup is 16, 20 and 24 (26%, 33% and 40%) in the first case and 56, 40 and 24 (46%, 33% and 20%) in the second one. Then it is clear that our group is the first one. More precisely, our Galois group is the subgroup of

$GL_4(2)$ generated by

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

If we work a bit with these generators, we can easily determine that this group is A_5 , the alternating group on 5 letters. Again, we can try to determine explicitly the polynomial that generates our group. With all these conditions, we look at [Klü] again, and we find 3 possible polynomials: $X^{10} + X^9 - 7X^7 - 14X^6 - 13X^5 - 7X^4 + 2X^3 - 6X^2 - 10X - 8$, $X^6 - X^5 - 3X^4 + X^3 + 4X + 4$ and $X^5 + X^3 - 5X^2 - 4X - 7$. Looking again the irreducibility of these elements modulo p , we determine that the polynomial we were looking for is the third one.

Chapter 3

Deformation Theory and lowering the level modulo ℓ^n

In this chapter we are interested in answering Question 0.1.3 we proposed in the introduction. That is, given two newforms f and g , a place $\lambda \mid \ell$ and an integer $n \geq 1$, let $\rho_{f,\lambda}$ and $\rho_{g,\lambda}$ be the two λ -adic associated representations described in Section 1.4. If $\rho_{f,\lambda}$ and $\rho_{g,\lambda}$ are equivalent modulo λ^n but not modulo λ^{n+1} , what forces these representations not being equivalent anymore?

I want to thank Gebhard Böckle for encouraging me, in a very interesting conversation, to study the behaviour of inertia groups as a possible reason to explain the situation mentioned above. Most of the content of this chapter was written in a joint paper with Luis Dieulefait in [DT09].

Given a prime p , let f and g be two modular forms of levels $N_f = pN_g$ and N_g , respectively. Let us suppose that there exists a $\lambda \mid \ell$ such that f and g are congruent modulo λ . By Theorem 1.4.10, we know that $\rho_{f,\lambda}$ can ramify only at the divisors of pN_g , and $\rho_{g,\lambda}$ just at the ones of N_g . On the other hand, by Remark 1.4.14, we know that the semi-simplification of the projection modulo λ of ρ_g is unramified outside ℓN_g . Since f and g are congruent modulo λ , it is clear that $\bar{\rho}_{f,\lambda}$ is unramified also outside ℓN_g .

If we raise now the power of λ to λ^2 , it is clear that some of the inertia groups that were killed before by λ , might now not disappear. So, increasing the exponent implies that this representation can have some ramification that the lower one did not have.

Then, we have two possibilities modulo λ^2 : either $\bar{\rho}_{f,\lambda^2}$ and $\bar{\rho}_{g,\lambda^2}$ continue being equivalent or not. In the former case, the only possible ramification for

$\bar{\rho}_{g,\lambda^2}$ continues being in ℓN_g , and thus, because of the congruence, it is also for $\bar{\rho}_{f,\lambda^2}$. In the latter case, if $\bar{\rho}_{f,\lambda^2}$ and $\bar{\rho}_{g,\lambda^2}$ are not equivalent anymore, the ramification of $\bar{\rho}_{f,\lambda^2}$ might have increased at p . The aim of this chapter is to study when can we say something about this increase.

3.1 Main results

During the whole chapter we will assume f and g are two eigenforms of weight 2 without nebentypus; $\ell \neq 2$ and that all the representations we use are irreducible modulo λ . In particular, this implies that all representations will be odd and absolutely irreducible.

Definition 3.1.1. *Let $L = \mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$. Then $\bar{\rho}_{g,\lambda}$ is **strongly irreducible** if $\bar{\rho}_{g,\lambda}|_{G_L}$ is irreducible.*

Proposition 3.1.2. *Let $\ell > 3$. Then $\bar{\rho}_{g,\lambda}$ is strongly irreducible.*

Proof. Assuming that $\bar{\rho}_{g,\lambda}$ is irreducible as in our case, if g is a newform of weight 2 and ℓ does not divide its level, clearly the residual representation $\bar{\rho}_{g,\lambda}$ has Serre's weight 2. Thus, this gives a precise information of the action of inertia at ℓ , and this is enough to show that $\bar{\rho}_{g,\lambda}|_{G_L}$ is irreducible if $\ell > 3$. This is proved in [Rib97] as part of the proof that the dihedral case can not occur for semistable weight 2 representations. \square

Let us remark that the condition of $\bar{\rho}|_{G_L}$ being irreducible for $\ell = 3$ is easily checked just by finding a prime $p \equiv 2 \pmod{3}$ such that $a_p(g) \not\equiv 0 \pmod{\lambda}$, $\lambda \mid 3$, or equivalently, such that $\text{Norm}(a_p(g)) \not\equiv 0 \pmod{3}$.

Theorem 3.1.3. *Let $\ell, p \nmid N_g$, $\ell > 2$ be two different prime numbers. Let f be in $S_2(p^k N_g)$, $k \geq 1$, and let $g \in S_2(N_g)$ be minimal with respect to λ . Suppose that $\bar{\rho}_{f,\lambda} \sim \bar{\rho}_{g,\lambda}$ and they are strongly irreducible, and assume that for any other $h \in S_2(N_g)$, $\bar{\rho}_{g,\lambda} \not\sim \bar{\rho}_{h,\lambda}$. Then,*

$$m := \min\{n \in \mathbb{N} : \bar{\rho}_{f,\lambda^n} \not\sim \bar{\rho}_{g,\lambda^n}\} = \min\{n \in \mathbb{N} : \bar{\rho}_{f,\lambda^n}|_{\mathcal{I}_p} \not\sim \bar{\rho}_{g,\lambda^n}|_{\mathcal{I}_p}\}.$$

Hence, what we show is that in many cases the cause of the break of the congruence when increasing the power of λ is due precisely to the non-triviality of the action of the inertia group at a prime in N_f/N_g . Let us remark that this is specific to the situation we are in, namely when N_g is

a proper divisor of N_f . If this were not the case, $N_f = N_g$ and ρ_f and ρ_g were congruent modulo some λ^n , it is clear that the reason of not being congruent anymore modulo λ^{n+1} can not be related to ramification at any place, because g is minimal at λ , and the congruence implies that f must be also minimal at λ .

When Theorem 3.1.3 can be applied, it can be reinterpreted as a generalization to higher exponents of Ribet's Lowering the Level [Rib90a].

Theorem 3.1.4 (Ribet's Lowering the Level modulo λ). *Let $\bar{\rho}$ be an irreducible mod λ modular representation of level pN , where p does not divide N . Assume that $\bar{\rho}$ is unramified at p . Then $\bar{\rho}$ is modular of level N .*

Proof. The proof is found in [Rib90a] together with [Rib94]. □

As a corollary of Theorem 3.1.3 and using Ribet's Lowering the Level, we obtain the following result.

Corollary 3.1.5 (Lowering the level modulo λ^n). *Let f be a newform of weight 2, trivial character and level $p^k N$ ($p \nmid N$) such that for a given $\lambda \nmid 2pN$ and an integer n , $\bar{\rho}_{f,\lambda^n}$ does not ramify at p . Let us suppose that there exists exactly one newform g of weight 2 and level N congruent to f modulo λ (Ribet's lowering the level provides **at least one**) satisfying the strong irreducibility condition. Then, lowering the level can be generalized modulo λ^n , i.e., f and g are congruent also modulo λ^n .*

In Corollary 2.4.3 we saw that there is no congruence between two newforms of levels N and $p^k N$ if $k > 2$. In the case $k = 1$, we can rewrite Theorem 3.1.3 as follows.

Corollary 3.1.6. *With the same conditions as in Theorem 3.1.3, let $k = 1$. Then*

$$\rho_{f,\lambda}|_{\mathcal{I}_p} = \left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right\rangle$$

where $v_p(a) = m - 1$. So, the image of the mod λ^m representation of f contains an ℓ -group.

Proof. It is well known that if a representation ρ is semi-stable at p , the restriction of ρ on the inertia at p is

$$\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

for some $* \neq 0$. Since we know that the inertia at p vanishes modulo λ^n exactly when $n < m$, then we know that $* \equiv 0 \pmod{\lambda^n}$ if and only if $n < m$. Then $v_\ell(*) = m - 1$. \square

In particular, when $\rho_{g,\lambda}$ has Complex Multiplication, we can bound the image of the $\text{mod } \lambda^m$ representation $\bar{\rho}_{f,\lambda^m}$.

For any two-dimensional Galois representation ρ , let us denote by ρ' its projectivization. Then we have the following:

Corollary 3.1.7. *With the same conditions as in Theorem 3.1.3, let $k = 1$. Let us suppose also that g has Complex Multiplication (in this case, $\text{Im}(\rho'_{g,\lambda})$ is a dihedral group). Then the image of $\rho'_{f,\lambda}$ is not dihedral and the number m of the Theorem is the smallest one such that the first of the following inclusions is not an equality:*

$$\text{Dihedral group} \subsetneq \bar{\rho}'_{f,\lambda^m}(G_{\mathbb{Q}}) \subsetneq PGL_2(\mathcal{O}_{f,\lambda}/\lambda^m \mathcal{O}_{f,\lambda}).$$

Proof. It is clear that for $m - 1$, $\bar{\rho}'_{g,\lambda^{m-1}} \sim \bar{\rho}'_{f,\lambda^{m-1}}$, and since g has Complex Multiplication, $\bar{\rho}'_{f,\lambda^{m-1}}(G_{\mathbb{Q}})$ must be a dihedral group. On the other hand, for m , since $\bar{\rho}'_{f,\lambda^m}(G_{\mathbb{Q}})$ contains an element provided by Theorem 3.1.3 which can not be contained in a dihedral group, it is clear that $\bar{\rho}'_{f,\lambda^m}(G_{\mathbb{Q}})$ is not a dihedral group anymore.

For the other inequality it is clear that it is never an equality, because if it were, $\bar{\rho}'_{f,\lambda^n}(G_{\mathbb{Q}})$ would always equal $PGL_2(\mathcal{O}_{f,\lambda}/\lambda^n \mathcal{O}_{f,\lambda})$, for every n . And this is impossible, since we know that for $n < m$, $\bar{\rho}'_{f,\lambda^n}(G_{\mathbb{Q}})$ is just a dihedral group. \square

As it can be observed, the results obtained describe some elements of the image of these representations. This can be applied to determine images of Galois representations and, therefore, realize some finite groups as Galois groups (see Remark 3.4.2).

Several examples of newforms satisfying the conditions of the Theorem and corollaries above can be found in Section 3.4.

Let us remark that the conditions in the Theorem are not too restrictive. For example, just by taking one modular form g of level N with residual $\text{mod } \lambda$ representation satisfying the strong irreducibility condition, minimal with respect to λ and not congruent to any other modular form of the same level, using Ribet's Raising the Level we can find infinitely many examples in which we can apply our results.

The conditions we are imposing on the pair (g, ℓ) are generic in the following sense: given g they are satisfied for almost every prime ℓ . In fact, given g it is well-known that for almost every prime ℓ the representation $\rho_{g, \lambda}$ is irreducible, as proved by Ribet in [Rib85] (see also [DV00] for an explicit determination of a finite set including all reducible primes), and as we have already explained the strong irreducibility condition is automatic if $\ell > 3$. It is also well-known that the number of primes giving congruences between modular forms of fixed (or bounded) level, called “congruence primes”, is finite because there are only finitely many newforms of bounded level, and two modular forms that are congruent modulo infinitely many primes must be equal. Also, the condition of being minimal with respect to λ is equivalent, by Ribet’s lowering the level, to the fact that g is not congruent to some modular form g' of level equal to a proper divisor of N , and so if this condition is not satisfied ℓ has to be a congruence prime and we know that there are only finitely many of them because the level of g and g' are both bounded by N . We conclude that for any level N there is constant C such that for any weight 2 modular form g of level N and any prime $\ell > C$ the pair (g, λ) satisfies the conditions of the Theorem.

3.2 Deformation theory

In this section we will give a very brief introduction to deformation theory, which is needed to prove the main result of this chapter. We will follow [Gou01] and [Maz97] to introduce the basic definitions and results.

Let k be a finite field and let \mathcal{R} , A , A_0 , A_1 and Λ be complete noetherian rings with residue field k .

Definition 3.2.1. *Let Π be a profinite group and h a continuous ring homomorphism*

$$h : A_1 \rightarrow A_0$$

Let n be a positive integer and denote also by h the induced homomorphism

$$h : GL_n(A_1) \rightarrow GL_n(A_0)$$

of groups. If

$$\bar{\rho} : \Pi \rightarrow GL_n(A_0)$$

is a representation, a **deformation** of $\bar{\rho}$ to the ring A_1 is a strict equivalence class of liftings

$$\begin{array}{ccc} \Pi & \xrightarrow{\rho} & GL_n(A_1) \\ & \searrow \bar{\rho} & \downarrow h \\ & & GL_n(A_0) \end{array}$$

where two liftings ρ and ρ' are called **strictly equivalent** if they can be brought one into another by conjugation by elements of $GL_n(A_1)$ which lie in the kernel of h .

Let K be a number field and S a finite set of non-archimedean places of K . Let $G_{K,S}$ denote the Galois group

$$G_{K,S} := \text{Gal}(\bar{K}_S/K),$$

where \bar{K}_S is the maximal algebraic extension of K in \bar{K} unramified outside S . The first basic result is the following

Proposition 3.2.2. *If n is a positive integer and*

$$\bar{\rho} : G_{K,S} \rightarrow GL_n(k)$$

*is absolutely irreducible, then there is a **universal ring** $\mathcal{R} = \mathcal{R}(\bar{\rho})$ with residue field k , and a **universal deformation**,*

$$\rho^{\text{univ}} : G_{K,S} \rightarrow GL_n(\mathcal{R}),$$

of $\bar{\rho}$ to \mathcal{R} ; it is universal in the sense that given any ring A with residue field k , and any deformation

$$\rho : G_{K,S} \rightarrow GL_n(A),$$

of $\bar{\rho}$ to A , there is one and only one homomorphism $h : \mathcal{R} \rightarrow A$ inducing the identity isomorphism on residue fields for which the composition of the universal deformation ρ^{univ} with the homomorphism $GL_n(\mathcal{R}) \rightarrow GL_n(A)$ coming from h is equal to the deformation ρ .

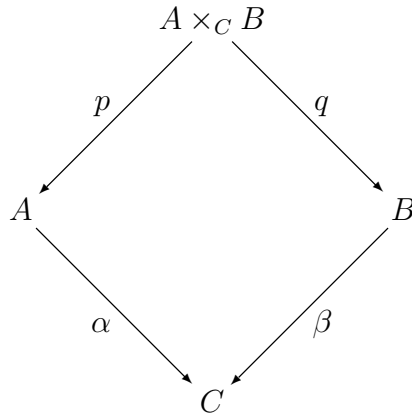
Proof. [Maz97], p.261. □

Now we will introduce the representations with prescribed conditions as in [Gou01].

Definition 3.2.3. Let A, A_1 , a representation $\rho : G_{\mathbb{Q}} \rightarrow GL_n(A)$ and a homomorphism $\alpha : A \rightarrow A_1$ be given. The **push-forward** $\alpha_*\rho : G_{\mathbb{Q}} \rightarrow GL_n(A_1)$ of ρ by α is the composition of ρ with the homomorphism $GL_n(A) \rightarrow GL_n(A_1)$ induced by α .

Definition 3.2.4. We suppose $\bar{\rho}$ is a residual representation of dimension n . A **deformation condition** on deformations of $\bar{\rho}$ is a property \mathcal{Q} of n -dimensional representations of $G_{\mathbb{Q}}$ defined over artinian Λ -algebras which satisfies the following conditions

- i) The residual representation $\bar{\rho}$ has property \mathcal{Q} .
- ii) Given a deformation $\rho : G_{\mathbb{Q}} \rightarrow GL_n(A)$ of $\bar{\rho}$ and a homomorphism of Λ -algebras $\alpha : A \rightarrow A_1$, if ρ has property \mathcal{Q} then so does the push-forward $\alpha_*\rho$.
- iii) Let



be a fiber product diagram in \mathcal{C}_{Λ}^0 , and let

$$\rho : G_{\mathbb{Q}} \rightarrow GL_n(A \times_C B)$$

be a deformation of $\bar{\rho}$. Then ρ has property \mathcal{Q} if and only if both $p_*\rho$ and $q_*\rho$ have property \mathcal{Q} .

iv) Let $\alpha : A \rightarrow A_1$ be an injective homomorphism of Λ -algebras and let $\rho : G_{\mathbb{Q}} \rightarrow GL_n(A)$ be a deformation of $\bar{\rho}$. If $\alpha_*\rho$ has property \mathcal{Q} then so does ρ .

3.3 Proof of Theorem 3.1.3

We will need first to introduce two auxiliary results.

Proposition 3.3.1. *Let $\bar{\rho}$ be a mod λ strongly irreducible representation of conductor N , with $\ell > 2$. Let us suppose that there exists only one modular form g of weight 2, trivial character, and level N such that $\bar{\rho} = \bar{\rho}_{g,\lambda}$. Let \mathcal{Q} be the following set of deformation conditions:*

- *The deformations are unramified outside ℓN .*
- *The deformations are minimally ramified everywhere.*
- *The determinant of the deformations is the cyclotomic character.*
- *The deformations are flat (locally at ℓ).*

Then, the deformation ring $\mathcal{R}_{\mathcal{Q}}$ is the ring of integers $\mathcal{O}_{g,\lambda}$.

Proof. If we apply an extended version of the famous Theorem of Taylor-Wiles ([TW95], [dS97] and [Dia97]), we obtain that the universal deformation ring $R_{\mathcal{Q}}$ must be isomorphic to $\mathbb{T}_{\mathcal{Q}}$. By hypothesis, there is only one $\overline{\mathbb{Q}}_{\ell}$ -point in $\mathbb{T}_{\mathcal{Q}}$. Then $\mathcal{R}_{\mathcal{Q}}$ must be $\mathcal{O}_{g,\lambda}$ itself. \square

Lemma 3.3.2. *Let ρ_1 and ρ_2 be two representations, both deforming $\bar{\rho}$*

$$\rho_1, \rho_2 : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{\lambda}/\lambda^n\mathcal{O}_{\lambda})$$

satisfying the same deformation conditions \mathcal{Q} , such that for these conditions the universal deformation ring is \mathcal{O}_{λ} . Then, ρ_1 is equivalent to ρ_2 .

Proof. We suppose they are different. The universal deformation (under conditions \mathcal{Q}) is

$$\rho^{univ} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{\lambda}).$$

By hypothesis, there exist two homomorphisms h_1 and h_2

$$h_1, h_2 : \mathcal{O}_{\lambda} \rightarrow \mathcal{O}_{\lambda}/\lambda^n\mathcal{O}_{\lambda}$$

such that they induce the identity in the residue fields and also $h_i \circ \rho^{univ} = \rho_i$. Then h_1 and h_2 must be different homomorphisms, but since there exists only one natural projection from \mathcal{O}_λ to $\mathcal{O}_\lambda/\lambda^n\mathcal{O}_\lambda$ fixing the residue fields, we arrive at a contradiction. \square

Proof of Theorem 3.1.3. We consider the same set of deformation conditions \mathcal{Q} as in Proposition 3.3.1. We consider also the set of conditions \mathcal{Q}' as follows:

- The deformations are unramified outside ℓpN .
- The deformations are minimally ramified locally at every place $q \neq p$.
- The determinant of the deformations is the cyclotomic character.
- The deformations are flat locally at ℓ .

So, the set of conditions \mathcal{Q}' is different from the set of conditions \mathcal{Q} only because now we allow ramification at p .

Obviously $\bar{\rho}_{g,\lambda^{m-1}}$ and $\bar{\rho}_{g,\lambda^m}$ satisfy conditions \mathcal{Q} and \mathcal{Q}' . Since $\bar{\rho}_{g,\lambda^{m-1}} \sim \bar{\rho}_{f,\lambda^{m-1}}$, $\bar{\rho}_{f,\lambda^{m-1}}$ satisfies also \mathcal{Q} and \mathcal{Q}' .

By Proposition 3.3.1, $\mathcal{R}_{\mathcal{Q}} = \mathcal{O}_{g,\lambda}$. This means, by Lemma 3.3.2, that if two *mod* λ^n deformations satisfy deformation conditions \mathcal{Q} they must be the same. By hypothesis we know that $\bar{\rho}_{f,\lambda^m} \not\sim \bar{\rho}_{g,\lambda^m}$. This means that $\bar{\rho}_{f,\lambda^m}$ can not satisfy conditions \mathcal{Q} . Nevertheless, $\bar{\rho}_{f,\lambda^m}$ clearly satisfies conditions \mathcal{Q}' . Since the only difference between both conditions is the ramification at p , the reason for $\bar{\rho}_{f,\lambda^m}$ not to satisfy \mathcal{Q} must be precisely that $\bar{\rho}_{f,\lambda^m}$ ramifies at p , as we wanted to prove. \square

3.4 Examples

In this section we give a table showing some interesting examples of couples of newforms satisfying Theorem 3.1.3 and Corollary 3.1.6. They have been computed with the algorithm `UpperBound1.0` and `LowerBound1.0` from the preceding chapter.

Elements in Table 3.1 satisfy the conditions from Theorem 3.1.3. All but one of them (the one with $p = 13^2$) satisfy also the conditions from Corollary 3.1.6. More extended lists can be found in Appendix C, and the complete list is in `Theorem.res`.

N_f	i	N_g	j	ℓ^{m-1}	p^k	m
$1678 = 2 \cdot 839$	8	839	2	1750283935190857471	2	2
$1707 = 3 \cdot 569$	4	569	2	122272440801294601	3	2
$1941 = 3 \cdot 647$	4	647	3	5539230441648341	3	2
$1839 = 3 \cdot 613$	4	613	3	3726338419619653	3	2
$1757 = 7 \cdot 251$	5	251	2	902088490528867	7	2
$1797 = 3 \cdot 599$	6	599	3	779881437372101	3	2
$1941 = 3 \cdot 647$	3	647	3	665741756680589	3	2
$1945 = 5 \cdot 389$	5	389	5	571255479184807	5	2
$1754 = 2 \cdot 877$	4	877	3	551522526259063	2	2
$1706 = 2 \cdot 853$	5	853	2	372293980443053	2	2
$1906 = 2 \cdot 953$	6	953	2	303408887531093	2	2
$1851 = 3 \cdot 617$	7	617	2	286866593268389	3	2
$1991 = 11 \cdot 181$	4	11	1	$3^2 \leq \ell^{m-1} \leq 3^3$	181	$3 \leq m \leq 4$
$1969 = 11 \cdot 179$	4	11	1	3	179	2
$1903 = 11 \cdot 173$	4	11	1	7	173	2
$1859 = 11 \cdot 13^2$	8	11	1	3	13^2	2
$1837 = 11 \cdot 167$	5	11	1	13	167	2
$1937 = 13 \cdot 149$	4	149	2	$3^9 \leq \ell^{m-1} \leq 3^{10}$	13	$10 \leq m \leq 11$
$1934 = 2 \cdot 967$	2	967	1	$625 = 5^4$	2	5
$1708 = 2^2 \cdot 7 \cdot 61$	6	$2^2 \cdot 61$	2	$3^3 \leq \ell^{m-1} \leq 3^4$	7	$4 \leq m \leq 5$
$1643 = 31 \cdot 53$	3	53	2	$5^3 \leq \ell^{m-1} \leq 5^4$	31	$4 \leq m \leq 5$
$1426 = 2 \cdot 23 \cdot 31$	13	$23 \cdot 31$	5	$81 = 3^4$	2	5
$1401 = 3 \cdot 467$	1	467	2	$625 = 5^4$	3	5
$1298 = 2 \cdot 11 \cdot 59$	11	$11 \cdot 59$	4	$81 = 3^4$	2	5
$1158 = 2 \cdot 3 \cdot 193$	13	$2 \cdot 193$	4	$625 = 5^4$	3	5
$1115 = 5 \cdot 223$	8	223	2	$81 = 3^4$	5	5

Table 3.1: Some examples satisfying Theorem 3.1.3

We divided the table in 3 different parts: the first one has some of the elements with the biggest ℓ 's that we found. The greatest one is as big as $1.75 \cdot 10^{18}$. The next part includes the elements with a big p . Since we are working with elements with $N \leq 2000$ and the smallest level appearing is $N = 11$, we know that p can not be bigger than 181. We have actually precisely one example with this p . Finally, in the last section we have the

couples with the biggest m 's. It is remarkable to see that there is one element in which m is between 10 and 11 (as we saw in Table 2.2, these bounds come from L^- and L^+).

As we mentioned in the last chapter, working with polynomials with integer coefficients instead of going to extension fields, has the disadvantage concerning the conjugate forms. Whence, it might be difficult to check if the condition of unique congruent element in $S_2(N_g)$ from Theorem 3.1.3 is satisfied, as it was mentioned in Remark 2.14.1.

Let us suppose that we have two newforms $f \in S_2(p^k N)$ and $g \in S_2(N)$ and a $\lambda \mid \ell$ such that f and g are congruent modulo λ . If we check in our list of congruences, we can see if there is another $g' \in S_2(N)$ congruent to g for some (other) $\lambda' \mid \ell$. In this case, if $\lambda = \lambda'$, g' is congruent to f and therefore they have to appear also in our list. If we do not find it, we can already determine that $\lambda \neq \lambda'$ and we solved our problem.

However, it could be the case that f and g were congruent modulo λ_1 , f and g' modulo λ_2 and the same could happen with a λ_3 for g' and g , $(\lambda_1, \lambda_2, \lambda_3) = 1$. In this case, the three couples would appear in our lists without being congruent all together.

One way to solve this problem is by computing the gcd's of the Hecke Operators as it is shown in Remark 2.5.6. In this case, however, the gcd will not be of 2 polynomials but 3. Using the notation of §2.6, if $\gcd(\hat{Q}_{f,p,\ell}, \hat{Q}_{g,p,\ell}, \hat{Q}_{g',p,\ell})$ is not trivial for every $p \nmid N_f$, we have big chances that these three newforms are congruent all together modulo one λ and thence we can not apply the Theorem.

Remark 3.4.1. *To compute this uniqueness' condition, we used both methods described above. For every couple of newforms f and g with $N \leq 2000$ with $N_f = pN_g$, $p \nmid N_g$, and for every prime ℓ from our list of congruences such that $\ell \nmid 2pN_g$ and with g minimal in ℓ , we found just one triple such that these two different systems gave different answer. In particular, for $f = (1948, 2)$, $g = (487, 2)$, $g' = (487, 4)$ and $\ell = 3$, there exist three places dividing ℓ such that they are congruent two to two and they are not congruent all together (for $p < 5000$ there are just 16 over 666 primes –2,40%– with trivial gcd). Nonetheless, these newforms seem to be reducible modulo some place dividing ℓ . So, until $N = 2000$ we did not find any triple satisfying **all** the conditions of the Theorem except the one about uniqueness.*

Remark 3.4.2. *As it has already been mentioned, one of the most interesting applications of the results obtained in this chapter can have is precisely to*

determine images of Galois representations and thence, being able to realize finite groups with controlled ramification.

If we look at Table 3.1, we can find many examples in which we get a determined element in the image of the Galois representation. Since we can determine that the images must have elements with order e.g. 3^{10} , 5^4 or 13^4 , we have already a very restricted amount of possibilities for the images of the representations.

Further work

After having answered some questions (or some cases of some questions) we had proposed at the starting point of this travel, it seems thus far we have found more new questions than the ones we had at the beginning. Some of the next natural problems are the following.

- First of all, in this thesis we have restricted all our work to the weight 2 and trivial nebentypus case. Most of the results we obtained, however, do not seem to depend strictly on these conditions and, therefore, it would be very interesting to study those more general cases.
- Looking `UpperBound1.0.res`, for $\ell = 43$ we see that there are 4 couples such that $43^2 \mid L^+$:

N_f	i_f	N_g	i_g	L^+
1243	3	113	3	43^2
895	6	179	3	$3 \cdot 43^2 \cdot 14947$
838	1	419	2	$37 \cdot 43^2$
662	5	331	3	43^2

However, most of prime numbers ℓ do not appear in our lists with $n_\ell > 1$. Why? are there some primes which are more likely to appear? Are there primes which will never appear with exponent bigger than 1?

- Is Conjecture 2.11.5 true?
- We have in mind to relax the assumptions of Theorem 3.1.3 by considering relative deformations. For example, one should consider in which cases it is possible to change the condition “for any other $h \in S_2(N_g)$, $\bar{\rho}_{g,\lambda} \not\sim \bar{\rho}_{h,\lambda}$ ” with “for any other $h \in S_2(N_g)$, $\bar{\rho}_{g,\lambda^n} \not\sim \bar{\rho}_{h,\lambda^n}$ ”.

Another possibility would be to study in which situation this condition can be completely eliminated. In this more general case, the minimal universal deformation ring will be more complicated, though it is known to be *finite flat complete intersections* by the result of Taylor-Wiles.

There are examples showing that this condition can not be simply removed in general for any couple of modular forms. Even in the simplest case when we have a $g' \in S_k(N)$ such that $\bar{\rho}_g \equiv \bar{\rho}_{g'} \pmod{\lambda^m}$, we can not say anything yet about the ramification of $f \in S_k(pN)$ because then, the dimension of the tangent space t_D of the functor D (which controls the dimension of the deformation ring) is not necessarily 0. In such a case, we can have infinite different morphisms from $GL_2(\mathcal{R}_{\mathcal{O}})$ to $GL_2(\mathcal{O}_{\lambda}/\lambda^n \mathcal{O}_{\lambda})$ and we can not apply Lemma 3.3.2.

- Applying new developments in the Taylor-Wiles Theorem and some recent works on characteristic two, we wonder if it could be possible also to extend Theorem 3.1.3 for $\ell = 2$; and remove the “strong irreducibility” condition for $\ell = 3$.
- In Remark 3.4.1 we saw that in the examples we computed, we did not find any triple of modular forms satisfying all the conditions from Theorem 3.1.3 but the uniqueness one. This leads us to the following question.

Question 4.1.1. *Let $\ell, p \nmid N_g$, $\ell > 2$ be two different prime numbers. Let $f \in S_2(p^k N)$ ($k \geq 1$), $g, g' \in S_2(N)$ be three different newforms of weight 2 and trivial character. Let g be minimal in ℓ . In which cases can $\lambda_1, \lambda_2, \lambda_3 \mid \ell$ exist, with $(\lambda_1, \lambda_2, \lambda_3) = 1$ and such that*

- $\bar{\rho}_{f, \lambda_1} \sim \bar{\rho}_{g, \lambda_1}$ *irreducible*
- $\bar{\rho}_{f, \lambda_2} \sim \bar{\rho}_{g', \lambda_2}$
- $\bar{\rho}_{g, \lambda_3} \sim \bar{\rho}_{g', \lambda_3}$?

- Looking the results we obtained with Theorem 3.1.3, we also wondered the following question.

Question 4.1.2. *In Table 3.1 we saw that ℓ and p seem not to be bounded (p is clear). However, given any couple of newforms, is there any global bound for m ?*

-
- As we already mentioned in Remark 3.4.2, it would be very a nice study to apply Theorem 3.1.3 explicitly to realize Galois groups.
 - Another interesting thing would be to generalize Ribet's Raising the Level for higher powers of λ . If we look in our lists, we see that in many cases, given a newform $\rho \in S_2(N)$ irreducible modulo λ , we have

$$\mathrm{tr}\rho(\mathrm{Frob}_p) \equiv \pm(p+1) \pmod{\lambda^n}$$

if and only if there exists one newform of level pN congruent to ρ modulo λ^n . But this is not always the case. In particular (as expected), for $\ell = 2$ it works really bad. Then, could we say something for $\ell > 2$?

- In the same fashion, as we saw in Section 1.7, it would be very valuable extend the lowering the level theorem for λ^n , with $n > 1$.

Question 4.1.3. *Let f in $S_2(qN)$, for a $q \in \mathbb{N}$ such that $N(\bar{\rho}_{f,\lambda^n}) = N$. Is there a modular form $g \in S_2(N)$ such that $f \equiv g \pmod{\lambda^n}$?*

In fact, in our case, just the following particular case would be already enough:

Question 4.1.4. *Let $f \in S_2(k_1N)$ and $g \in S_2(k_2N)$ such that $(k_1, k_2) = 1$. Suppose that $f \equiv g \pmod{\lambda^n}$. Is there a modular form $h \in S_2(N)$ such that $f \equiv g \equiv h \pmod{\lambda^n}$?*

It is remarkable to mention the still non published work of I. Chen, I. Kiming and J. Rasmussen in which indeed, it seems they can reduce the level precisely in the prime ℓ (they need, however, a weight change). In some sense, it complements the work we developed in this thesis.

Appendix A

UpperBound1.0.res

List of results of UpperBound1.0 (Chapter 2) for all couples of newforms with $N < 90$ and `pBound = 1000`. A list for all couples with $N \leq 2000$ (204.438 lines) can be found in `UpperBound1.0.res` and the \LaTeX version in `UpperBound1.0.tex.res`. This list has been created with the file `UpperBound1.0`.

N_f	i_f	N_g	i_g	L^+
$26 = 2 \cdot 13$	2	$26 = 2 \cdot 13$	1	2
$30 = 2 \cdot 3 \cdot 5$	1	$15 = 3 \cdot 5$	1	$4 = 2^2$
$33 = 3 \cdot 11$	1	11	1	3
$34 = 2 \cdot 17$	1	17	1	2
$35 = 5 \cdot 7$	2	$35 = 5 \cdot 7$	1	2
37	2	37	1	2
$38 = 2 \cdot 19$	1	19	1	3
$38 = 2 \cdot 19$	2	$38 = 2 \cdot 19$	1	2
$39 = 3 \cdot 13$	2	$39 = 3 \cdot 13$	1	$4 = 2^2$
$40 = 2^3 \cdot 5$	1	$20 = 2^2 \cdot 5$	1	2
$42 = 2 \cdot 3 \cdot 7$	1	$14 = 2 \cdot 7$	1	2
$42 = 2 \cdot 3 \cdot 7$	1	$21 = 3 \cdot 7$	1	$8 = 2^3$
43	2	43	1	2
$44 = 2^2 \cdot 11$	1	11	1	2
$45 = 3^2 \cdot 5$	1	$15 = 3 \cdot 5$	1	$4 = 2^2$
$46 = 2 \cdot 23$	1	23	1	5
$48 = 2^4 \cdot 3$	1	$24 = 2^3 \cdot 3$	1	$8 = 2^3$
$50 = 2 \cdot 5^2$	2	$50 = 2 \cdot 5^2$	1	2

N_f	i_f	N_g	i_g	L^+
$51 = 3 \cdot 17$	2	17	1	$4 = 2^2$
$51 = 3 \cdot 17$	2	$51 = 3 \cdot 17$	1	2
$52 = 2^2 \cdot 13$	1	$26 = 2 \cdot 13$	2	3
53	2	53	1	2
$54 = 2 \cdot 3^3$	1	$27 = 3^3$	1	3
$54 = 2 \cdot 3^3$	2	$27 = 3^3$	1	3
$54 = 2 \cdot 3^3$	2	$54 = 2 \cdot 3^3$	1	$6 = 2 \cdot 3$
$55 = 5 \cdot 11$	2	11	1	7
$55 = 5 \cdot 11$	2	$55 = 5 \cdot 11$	1	$4 = 2^2$
$56 = 2^3 \cdot 7$	1	$14 = 2 \cdot 7$	1	$4 = 2^2$
$56 = 2^3 \cdot 7$	2	$14 = 2 \cdot 7$	1	2
$56 = 2^3 \cdot 7$	2	$56 = 2^3 \cdot 7$	1	2
$57 = 3 \cdot 19$	1	19	1	2
$57 = 3 \cdot 19$	3	19	1	2
$57 = 3 \cdot 19$	3	$57 = 3 \cdot 19$	1	$4 = 2^2$
$57 = 3 \cdot 19$	3	$57 = 3 \cdot 19$	2	3
$58 = 2 \cdot 29$	1	29	1	2
$58 = 2 \cdot 29$	2	29	1	2
$58 = 2 \cdot 29$	2	$58 = 2 \cdot 29$	1	2
61	2	61	1	2
$62 = 2 \cdot 31$	2	31	1	11
$62 = 2 \cdot 31$	2	$62 = 2 \cdot 31$	1	2
$63 = 3^2 \cdot 7$	1	$21 = 3 \cdot 7$	1	$4 = 2^2$
$63 = 3^2 \cdot 7$	2	$21 = 3 \cdot 7$	1	$4 = 2^2$
$63 = 3^2 \cdot 7$	2	$63 = 3^2 \cdot 7$	1	$4 = 2^2$
$64 = 2^6$	1	$32 = 2^5$	1	$4 = 2^2$
$65 = 5 \cdot 13$	2	$65 = 5 \cdot 13$	1	2
$65 = 5 \cdot 13$	3	$65 = 5 \cdot 13$	1	2
$65 = 5 \cdot 13$	3	$65 = 5 \cdot 13$	2	$4 = 2^2$
$66 = 2 \cdot 3 \cdot 11$	1	$33 = 3 \cdot 11$	1	2
$66 = 2 \cdot 3 \cdot 11$	2	$33 = 3 \cdot 11$	1	$4 = 2^2$
$66 = 2 \cdot 3 \cdot 11$	2	$66 = 2 \cdot 3 \cdot 11$	1	2
$66 = 2 \cdot 3 \cdot 11$	3	11	1	5
$66 = 2 \cdot 3 \cdot 11$	3	$33 = 3 \cdot 11$	1	2
$66 = 2 \cdot 3 \cdot 11$	3	$66 = 2 \cdot 3 \cdot 11$	1	$4 = 2^2$
$66 = 2 \cdot 3 \cdot 11$	3	$66 = 2 \cdot 3 \cdot 11$	2	2

N_f	i_f	N_g	i_g	L^+
67	3	67	1	5
67	3	67	2	2
$68 = 2^2 \cdot 17$	1	17	1	2
$68 = 2^2 \cdot 17$	1	$34 = 2 \cdot 17$	1	$6 = 2 \cdot 3$
$69 = 3 \cdot 23$	2	23	1	11
$69 = 3 \cdot 23$	2	$69 = 3 \cdot 23$	1	$4 = 2^2$
$70 = 2 \cdot 5 \cdot 7$	1	$14 = 2 \cdot 7$	1	2
$70 = 2 \cdot 5 \cdot 7$	1	$35 = 5 \cdot 7$	2	$4 = 2^2$
71	2	71	1	$18 = 2 \cdot 3^2$
$72 = 2^3 \cdot 3^2$	1	$24 = 2^3 \cdot 3$	1	$4 = 2^2$
$72 = 2^3 \cdot 3^2$	1	$36 = 2^2 \cdot 3^2$	1	2
73	3	73	1	3
73	3	73	2	2
$74 = 2 \cdot 37$	1	37	2	3
$74 = 2 \cdot 37$	2	37	1	5
$74 = 2 \cdot 37$	2	$74 = 2 \cdot 37$	1	2
$75 = 3 \cdot 5^2$	1	$15 = 3 \cdot 5$	1	3
$75 = 3 \cdot 5^2$	2	$15 = 3 \cdot 5$	1	$4 = 2^2$
$75 = 3 \cdot 5^2$	3	$75 = 3 \cdot 5^2$	1	2
$75 = 3 \cdot 5^2$	3	$75 = 3 \cdot 5^2$	2	3
$76 = 2^2 \cdot 19$	1	19	1	2
$76 = 2^2 \cdot 19$	1	$38 = 2 \cdot 19$	2	3
$77 = 7 \cdot 11$	1	11	1	2
$77 = 7 \cdot 11$	2	11	1	3
$77 = 7 \cdot 11$	3	11	1	2
$77 = 7 \cdot 11$	3	$77 = 7 \cdot 11$	1	$4 = 2^2$
$77 = 7 \cdot 11$	4	$77 = 7 \cdot 11$	2	$4 = 2^2$
$77 = 7 \cdot 11$	4	$77 = 7 \cdot 11$	3	5
$78 = 2 \cdot 3 \cdot 13$	1	$26 = 2 \cdot 13$	1	5
$78 = 2 \cdot 3 \cdot 13$	1	$39 = 3 \cdot 13$	1	$8 = 2^3$
$78 = 2 \cdot 3 \cdot 13$	1	$39 = 3 \cdot 13$	2	$4 = 2^2$
79	2	79	1	2

N_f	i_f	N_g	i_g	L^+
$80 = 2^4 \cdot 5$	1	$20 = 2^2 \cdot 5$	1	2
$80 = 2^4 \cdot 5$	1	$40 = 2^3 \cdot 5$	1	$8 = 2^3$
$80 = 2^4 \cdot 5$	2	$20 = 2^2 \cdot 5$	1	$4 = 2^2$
$80 = 2^4 \cdot 5$	2	$40 = 2^3 \cdot 5$	1	2
$80 = 2^4 \cdot 5$	2	$80 = 2^4 \cdot 5$	1	2
$81 = 3^4$	1	$27 = 3^3$	1	3
$82 = 2 \cdot 41$	1	41	1	2
$82 = 2 \cdot 41$	2	41	1	2
$82 = 2 \cdot 41$	2	$82 = 2 \cdot 41$	1	2
83	2	83	1	$4 = 2^2$
$84 = 2^2 \cdot 3 \cdot 7$	1	$14 = 2 \cdot 7$	1	2
$84 = 2^2 \cdot 3 \cdot 7$	1	$21 = 3 \cdot 7$	1	2
$84 = 2^2 \cdot 3 \cdot 7$	1	$42 = 2 \cdot 3 \cdot 7$	1	$6 = 2 \cdot 3$
$84 = 2^2 \cdot 3 \cdot 7$	2	$14 = 2 \cdot 7$	1	$6 = 2 \cdot 3$
$84 = 2^2 \cdot 3 \cdot 7$	2	$21 = 3 \cdot 7$	1	2
$84 = 2^2 \cdot 3 \cdot 7$	2	$42 = 2 \cdot 3 \cdot 7$	1	2
$84 = 2^2 \cdot 3 \cdot 7$	2	$84 = 2^2 \cdot 3 \cdot 7$	1	$4 = 2^2$
$85 = 5 \cdot 17$	1	17	1	2
$85 = 5 \cdot 17$	2	17	1	2
$85 = 5 \cdot 17$	2	$85 = 5 \cdot 17$	1	2
$85 = 5 \cdot 17$	3	17	1	2
$85 = 5 \cdot 17$	3	$85 = 5 \cdot 17$	1	2
$85 = 5 \cdot 17$	3	$85 = 5 \cdot 17$	2	$4 = 2^2$
$86 = 2 \cdot 43$	1	43	2	7
$86 = 2 \cdot 43$	2	43	1	5
$86 = 2 \cdot 43$	2	$86 = 2 \cdot 43$	1	2
$87 = 3 \cdot 29$	2	29	1	23
$87 = 3 \cdot 29$	2	$87 = 3 \cdot 29$	1	$4 = 2^2$
$88 = 2^3 \cdot 11$	1	11	1	2
$88 = 2^3 \cdot 11$	1	$44 = 2^2 \cdot 11$	1	$4 = 2^2$
$88 = 2^3 \cdot 11$	2	11	1	2
$88 = 2^3 \cdot 11$	2	$44 = 2^2 \cdot 11$	1	$4 = 2^2$
$88 = 2^3 \cdot 11$	2	$88 = 2^3 \cdot 11$	1	$8 = 2^3$
89	3	89	1	2
89	3	89	2	5

Appendix B

Congruences with conjugates

List of results of `UpperBound1.1` (Chapter 2) for $N_f = N_g$ and $i_f = i_g$, for all couples of newforms with $N < 159$ and `pBound` = 1000. A list for all couples with $N \leq 2000$ (10.045 lines) can be found in `N,i eq M,j.res` and the L^AT_EX version in `N,i eq M,j.tex.res`. Due to the very big results for ℓ , this value has not been factorized here. $\ell = 0$ means that for every prime smaller than `pBound`, the polynomial we want to work with is a square. This list has been created with the file `UpperBound1.0`.

N_f	i_f	N_g	i_g	ℓ
23	1	23	1	20
29	1	29	1	8
31	1	31	1	20
$35 = 5 \cdot 7$	2	$35 = 5 \cdot 7$	2	17
$39 = 3 \cdot 13$	2	$39 = 3 \cdot 13$	2	32
41	1	41	1	148
43	2	43	2	8
47	1	47	1	31312
$51 = 3 \cdot 17$	2	$51 = 3 \cdot 17$	2	17
53	2	53	2	148
$55 = 5 \cdot 11$	2	$55 = 5 \cdot 11$	2	32
59	1	59	1	2210176
61	2	61	2	148
$62 = 2 \cdot 31$	2	$62 = 2 \cdot 31$	2	12
$63 = 3^2 \cdot 7$	2	$63 = 3^2 \cdot 7$	2	48

B Congruences with conjugates

N_f	i_f	N_g	i_g	ℓ
$65 = 5 \cdot 13$	2	$65 = 5 \cdot 13$	2	12
$65 = 5 \cdot 13$	3	$65 = 5 \cdot 13$	3	8
67	2	67	2	5
67	3	67	3	5
$68 = 2^2 \cdot 17$	1	$68 = 2^2 \cdot 17$	1	12
$69 = 3 \cdot 23$	2	$69 = 3 \cdot 23$	2	20
71	1	71	1	257
71	2	71	2	257
73	2	73	2	5
73	3	73	3	13
$74 = 2 \cdot 37$	1	$74 = 2 \cdot 37$	1	13
$74 = 2 \cdot 37$	2	$74 = 2 \cdot 37$	2	5
$77 = 7 \cdot 11$	4	$77 = 7 \cdot 11$	4	20
79	2	79	2	1305424
$81 = 3^4$	1	$81 = 3^4$	1	12
$82 = 2 \cdot 41$	2	$82 = 2 \cdot 41$	2	8
83	2	83	2	36238544
$85 = 5 \cdot 17$	2	$85 = 5 \cdot 17$	2	8
$85 = 5 \cdot 17$	3	$85 = 5 \cdot 17$	3	12
$86 = 2 \cdot 43$	1	$86 = 2 \cdot 43$	1	21
$86 = 2 \cdot 43$	2	$86 = 2 \cdot 43$	2	5
$87 = 3 \cdot 29$	1	$87 = 3 \cdot 29$	1	20
$87 = 3 \cdot 29$	2	$87 = 3 \cdot 29$	2	916
$88 = 2^3 \cdot 11$	2	$88 = 2^3 \cdot 11$	2	17
89	3	89	3	535120
$91 = 7 \cdot 13$	3	$91 = 7 \cdot 13$	3	8
$91 = 7 \cdot 13$	4	$91 = 7 \cdot 13$	4	316
$93 = 3 \cdot 31$	1	$93 = 3 \cdot 31$	1	20
$93 = 3 \cdot 31$	2	$93 = 3 \cdot 31$	2	916
$94 = 2 \cdot 47$	2	$94 = 2 \cdot 47$	2	8
$95 = 5 \cdot 19$	1	$95 = 5 \cdot 19$	1	592
$95 = 5 \cdot 19$	2	$95 = 5 \cdot 19$	2	181504
97	1	97	1	49
97	2	97	2	2777
$98 = 2 \cdot 7^2$	2	$98 = 2 \cdot 7^2$	2	8
101	2	101	2	1124401088

N_f	i_f	N_g	i_g	ℓ
103	1	103	1	5
103	2	103	2	447952448
$104 = 2^3 \cdot 13$	2	$104 = 2^3 \cdot 13$	2	17
$105 = 3 \cdot 5 \cdot 7$	2	$105 = 3 \cdot 5 \cdot 7$	2	80
107	1	107	1	5
107	2	107	2	14248502464
109	2	109	2	49
109	3	109	3	7537
$110 = 2 \cdot 5 \cdot 11$	4	$110 = 2 \cdot 5 \cdot 11$	4	33
$111 = 3 \cdot 37$	1	$111 = 3 \cdot 37$	1	592
$111 = 3 \cdot 37$	2	$111 = 3 \cdot 37$	2	99584
113	2	113	2	12
113	3	113	3	49
113	4	113	4	321
$115 = 5 \cdot 23$	2	$115 = 5 \cdot 23$	2	20
$115 = 5 \cdot 23$	3	$115 = 5 \cdot 23$	3	245072
$117 = 3^2 \cdot 13$	2	$117 = 3^2 \cdot 13$	2	48
$117 = 3^2 \cdot 13$	3	$117 = 3^2 \cdot 13$	3	32
$119 = 7 \cdot 17$	1	$119 = 7 \cdot 17$	1	148816
$119 = 7 \cdot 17$	2	$119 = 7 \cdot 17$	2	7259984
$122 = 2 \cdot 61$	2	$122 = 2 \cdot 61$	2	13
$122 = 2 \cdot 61$	3	$122 = 2 \cdot 61$	3	229
$123 = 3 \cdot 41$	3	$123 = 3 \cdot 41$	3	8
$123 = 3 \cdot 41$	4	$123 = 3 \cdot 41$	4	316
$125 = 5^3$	1	$125 = 5^3$	1	5
$125 = 5^3$	2	$125 = 5^3$	2	5
$125 = 5^3$	3	$125 = 5^3$	3	4400
127	1	127	1	81
127	2	127	2	9658420688
$129 = 3 \cdot 43$	3	$129 = 3 \cdot 43$	3	8
$129 = 3 \cdot 43$	4	$129 = 3 \cdot 43$	4	568
131	2	131	2	142916104920801280
$133 = 7 \cdot 19$	1	$133 = 7 \cdot 19$	1	5
$133 = 7 \cdot 19$	2	$133 = 7 \cdot 19$	2	5
$133 = 7 \cdot 19$	3	$133 = 7 \cdot 19$	3	13
$133 = 7 \cdot 19$	4	$133 = 7 \cdot 19$	4	229

B Congruences with conjugates

N_f	i_f	N_g	i_g	ℓ
$134 = 2 \cdot 67$	1	$134 = 2 \cdot 67$	1	473
$134 = 2 \cdot 67$	2	$134 = 2 \cdot 67$	2	81
$135 = 3^3 \cdot 5$	3	$135 = 3^3 \cdot 5$	3	52
$135 = 3^3 \cdot 5$	4	$135 = 3^3 \cdot 5$	4	52
$136 = 2^3 \cdot 17$	3	$136 = 2^3 \cdot 17$	3	20
137	1	137	1	725
137	2	137	2	1435966564
$138 = 2 \cdot 3 \cdot 23$	4	$138 = 2 \cdot 3 \cdot 23$	4	20
139	2	139	2	49
139	3	139	3	2145245897
$141 = 3 \cdot 47$	6	$141 = 3 \cdot 47$	6	17
$143 = 11 \cdot 13$	2	$143 = 11 \cdot 13$	2	31312
$143 = 11 \cdot 13$	3	$143 = 11 \cdot 13$	3	3113859280
$145 = 5 \cdot 29$	2	$145 = 5 \cdot 29$	2	32
$145 = 5 \cdot 29$	3	$145 = 5 \cdot 29$	3	592
$145 = 5 \cdot 29$	4	$145 = 5 \cdot 29$	4	592
$146 = 2 \cdot 73$	1	$146 = 2 \cdot 73$	1	404
$146 = 2 \cdot 73$	2	$146 = 2 \cdot 73$	2	6224
$147 = 3 \cdot 7^2$	4	$147 = 3 \cdot 7^2$	4	8
$147 = 3 \cdot 7^2$	5	$147 = 3 \cdot 7^2$	5	8
$148 = 2^2 \cdot 37$	2	$148 = 2^2 \cdot 37$	2	17
149	1	149	1	49
149	2	149	2	18822062530624
151	1	151	1	49
151	2	151	2	257
151	3	151	3	4838537
$152 = 2^3 \cdot 19$	3	$152 = 2^3 \cdot 19$	3	3844
$153 = 3^2 \cdot 17$	5	$153 = 3^2 \cdot 17$	5	17
$154 = 2 \cdot 7 \cdot 11$	4	$154 = 2 \cdot 7 \cdot 11$	4	20
$155 = 5 \cdot 31$	4	$155 = 5 \cdot 31$	4	20308
$155 = 5 \cdot 31$	5	$155 = 5 \cdot 31$	5	8468
157	1	157	1	24217
157	2	157	2	390366232
$158 = 2 \cdot 79$	6	$158 = 2 \cdot 79$	6	24
$159 = 3 \cdot 53$	1	$159 = 3 \cdot 53$	1	31312
$159 = 3 \cdot 53$	2	$159 = 3 \cdot 53$	2	16864208

Appendix C

Theorem 3.1.3

List of couples from `UpperBound1.0.res` satisfying the conditions of Theorem 3.1.3. Here we show all elements with $N \leq 266$. The complete list for all couples with $N \leq 2000$ (8.746 examples) can be found in `Theorem.res` and the \LaTeX version in `Theorem.tex.res`. The magma code to create this list can be found in the file `Theorem`.

N_f	i_f	N_g	i_g	L^-	L^+
$55 = 5 \cdot 11$	2	11	1	7	7
$62 = 2 \cdot 31$	2	31	1	11	11
$74 = 2 \cdot 37$	1	37	2	3	3
$74 = 2 \cdot 37$	2	37	1	5	5
$77 = 7 \cdot 11$	2	11	1	3	3
$78 = 2 \cdot 3 \cdot 13$	1	$26 = 2 \cdot 13$	1	5	5
$86 = 2 \cdot 43$	2	43	1	5	5
$87 = 3 \cdot 29$	2	29	1	23	23
$106 = 2 \cdot 53$	2	53	2	5	5
$111 = 3 \cdot 37$	1	37	2	5	5
$111 = 3 \cdot 37$	2	37	1	7	7
$114 = 2 \cdot 3 \cdot 19$	2	$57 = 3 \cdot 19$	1	5	5
$118 = 2 \cdot 59$	2	59	1	19	19
$119 = 7 \cdot 17$	2	17	1	3	3
$122 = 2 \cdot 61$	2	61	2	13	13
$123 = 3 \cdot 41$	4	41	1	23	23
$130 = 2 \cdot 5 \cdot 13$	1	$26 = 2 \cdot 13$	1	3	3

C Theorem 3.1.3

N_f	i_f	N_g	i_g	L^-	L^+
$132 = 2^2 \cdot 3 \cdot 11$	1	$44 = 2^2 \cdot 11$	1	5	5
$134 = 2 \cdot 67$	2	67	2	19	19
$141 = 3 \cdot 47$	5	47	1	7	7
$141 = 3 \cdot 47$	6	47	1	43	43
$143 = 11 \cdot 13$	2	11	1	3	$9 = 3^2$
$146 = 2 \cdot 73$	2	73	2	19	19
$154 = 2 \cdot 7 \cdot 11$	1	$77 = 7 \cdot 11$	1	3	3
$154 = 2 \cdot 7 \cdot 11$	3	$77 = 7 \cdot 11$	1	3	3
$155 = 5 \cdot 31$	4	31	1	7	7
$158 = 2 \cdot 79$	6	79	2	53	53
$159 = 3 \cdot 53$	1	53	1	7	7
$159 = 3 \cdot 53$	2	53	2	107	107
$161 = 7 \cdot 23$	3	23	1	19	19
$166 = 2 \cdot 83$	2	83	2	131	131
$170 = 2 \cdot 5 \cdot 17$	3	$85 = 5 \cdot 17$	3	3	3
$170 = 2 \cdot 5 \cdot 17$	5	$85 = 5 \cdot 17$	2	7	7
$174 = 2 \cdot 3 \cdot 29$	3	$58 = 2 \cdot 29$	1	7	7
$174 = 2 \cdot 3 \cdot 29$	1	$87 = 3 \cdot 29$	2	13	13
$174 = 2 \cdot 3 \cdot 29$	3	$87 = 3 \cdot 29$	1	11	11
$177 = 3 \cdot 59$	4	59	1	229	229
$178 = 2 \cdot 89$	1	89	3	7	7
$182 = 2 \cdot 7 \cdot 13$	2	$14 = 2 \cdot 7$	1	5	5
$182 = 2 \cdot 7 \cdot 13$	1	$91 = 7 \cdot 13$	4	11	11
$182 = 2 \cdot 7 \cdot 13$	3	$91 = 7 \cdot 13$	1	5	5
$183 = 3 \cdot 61$	2	61	2	19	19
$185 = 5 \cdot 37$	4	37	2	3	3
$186 = 2 \cdot 3 \cdot 31$	2	$93 = 3 \cdot 31$	2	7	7
$186 = 2 \cdot 3 \cdot 31$	4	$93 = 3 \cdot 31$	1	19	19
$187 = 11 \cdot 17$	1	17	1	3	3
$187 = 11 \cdot 17$	4	17	1	3	3
$190 = 2 \cdot 5 \cdot 19$	2	$95 = 5 \cdot 19$	2	11	11
$190 = 2 \cdot 5 \cdot 19$	4	$95 = 5 \cdot 19$	1	13	13
$194 = 2 \cdot 97$	2	97	2	67	67
$194 = 2 \cdot 97$	3	97	1	71	71
$195 = 3 \cdot 5 \cdot 13$	1	$65 = 5 \cdot 13$	3	7	7
$195 = 3 \cdot 5 \cdot 13$	5	$65 = 5 \cdot 13$	2	11	11

N_f	i_f	N_g	i_g	L^-	L^+
$198 = 2 \cdot 3^2 \cdot 11$	2	$99 = 3^2 \cdot 11$	4	5	5
$201 = 3 \cdot 67$	4	67	3	19	19
$201 = 3 \cdot 67$	5	67	2	29	29
$202 = 2 \cdot 101$	1	101	2	17	17
$202 = 2 \cdot 101$	2	101	1	3	3
$202 = 2 \cdot 101$	3	101	1	3	3
$204 = 2^2 \cdot 3 \cdot 17$	1	$68 = 2^2 \cdot 17$	1	11	11
$205 = 5 \cdot 41$	5	41	1	13	13
$205 = 5 \cdot 41$	6	41	1	31	31
$206 = 2 \cdot 103$	2	103	2	67	67
$206 = 2 \cdot 103$	4	103	1	19	19
$209 = 11 \cdot 19$	4	19	1	5	5
$213 = 3 \cdot 71$	5	71	1	19	19
$213 = 3 \cdot 71$	5	71	2	61	61
$214 = 2 \cdot 107$	5	107	2	109	109
$214 = 2 \cdot 107$	6	107	1	11	11
$215 = 5 \cdot 43$	4	43	2	31	31
$217 = 7 \cdot 31$	2	31	1	19	19
$218 = 2 \cdot 109$	4	109	2	41	41
$219 = 3 \cdot 73$	4	73	3	17	17
$219 = 3 \cdot 73$	5	73	2	29	29
$221 = 13 \cdot 17$	2	17	1	3	3
$222 = 2 \cdot 3 \cdot 37$	4	$74 = 2 \cdot 37$	2	11	11
$222 = 2 \cdot 3 \cdot 37$	2	$111 = 3 \cdot 37$	1	23	23
$222 = 2 \cdot 3 \cdot 37$	3	$111 = 3 \cdot 37$	2	13	13
$226 = 2 \cdot 113$	1	113	4	3	3
$226 = 2 \cdot 113$	3	113	4	3	3
$226 = 2 \cdot 113$	4	113	3	41	41
$230 = 2 \cdot 5 \cdot 23$	2	$115 = 5 \cdot 23$	3	43	43
$230 = 2 \cdot 5 \cdot 23$	4	$115 = 5 \cdot 23$	2	19	19
$231 = 3 \cdot 7 \cdot 11$	2	$77 = 7 \cdot 11$	3	5	5
$234 = 2 \cdot 3^2 \cdot 13$	2	$117 = 3^2 \cdot 13$	3	7	7
$235 = 5 \cdot 47$	1	47	1	$9 = 3^2$	$9 = 3^2$
$235 = 5 \cdot 47$	2	47	1	3	3
$235 = 5 \cdot 47$	3	47	1	3	3
$237 = 3 \cdot 79$	1	79	2	31	31

C Theorem 3.1.3

N_f	i_f	N_g	i_g	L^-	L^+
$237 = 3 \cdot 79$	3	79	1	5	5
$238 = 2 \cdot 7 \cdot 17$	2	$119 = 7 \cdot 17$	1	5	5
$238 = 2 \cdot 7 \cdot 17$	6	$119 = 7 \cdot 17$	2	61	61
$242 = 2 \cdot 11^2$	3	$121 = 11^2$	1	3	3
$242 = 2 \cdot 11^2$	4	$121 = 11^2$	4	5	5
$242 = 2 \cdot 11^2$	5	$121 = 11^2$	1	3	3
$245 = 5 \cdot 7^2$	1	$49 = 7^2$	1	3	3
$245 = 5 \cdot 7^2$	3	$49 = 7^2$	1	3	3
$246 = 2 \cdot 3 \cdot 41$	2	$123 = 3 \cdot 41$	4	11	11
$247 = 13 \cdot 19$	4	19	1	5	5
$249 = 3 \cdot 83$	3	83	2	31	31
$249 = 3 \cdot 83$	4	83	1	5	5
$249 = 3 \cdot 83$	5	83	2	2711	2711
$250 = 2 \cdot 5^3$	2	$125 = 5^3$	2	11	11
$250 = 2 \cdot 5^3$	3	$125 = 5^3$	1	11	11
$253 = 11 \cdot 23$	1	23	1	19	19
$254 = 2 \cdot 127$	5	127	1	17	17
$254 = 2 \cdot 127$	6	127	2	383	383
$255 = 3 \cdot 5 \cdot 17$	1	$51 = 3 \cdot 17$	2	13	13
$255 = 3 \cdot 5 \cdot 17$	2	$85 = 5 \cdot 17$	3	11	11
$258 = 2 \cdot 3 \cdot 43$	5	$86 = 2 \cdot 43$	2	19	19
$259 = 7 \cdot 37$	5	37	2	3	3
$262 = 2 \cdot 131$	2	131	2	11	11
$262 = 2 \cdot 131$	3	131	1	3	3
$262 = 2 \cdot 131$	4	131	2	313	313
$262 = 2 \cdot 131$	5	131	1	3	3
$264 = 2^3 \cdot 3 \cdot 11$	3	$88 = 2^3 \cdot 11$	1	7	7
$265 = 5 \cdot 53$	1	53	1	3	3
$265 = 5 \cdot 53$	5	53	2	31	31
$265 = 5 \cdot 53$	6	53	1	3	3
$266 = 2 \cdot 7 \cdot 19$	2	$14 = 2 \cdot 7$	1	11	11
$266 = 2 \cdot 7 \cdot 19$	4	$38 = 2 \cdot 19$	2	11	11
$266 = 2 \cdot 7 \cdot 19$	1	$133 = 7 \cdot 19$	4	13	13
$266 = 2 \cdot 7 \cdot 19$	2	$133 = 7 \cdot 19$	2	11	11

Bibliography

- [Bas96] Jacques Basmaji, *Ein Algorithmus zur Berechnung von Hecke-Operatoren und Anwendungen auf modulare Kurven*, Ph.D. thesis, Institut für Experimentelle Mathematik (Universität Essen), 1996, <http://modular.math.washington.edu/scans/papers/basmaji/>.
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993) <http://www.maths.usyd.edu.au:8000/u/magma/>.
- [Bla07] Guido Blady, *Punktezählalgorithmen für den Hecke-Operator und Anwendungen auf Modulkurven von Geschlecht 4*, Ph.D. thesis, Institut für Experimentelle Mathematik (Universität Duisburg-Essen), 2007.
- [Car89] Herni Carayol, *Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires*, Duke mathematical journal **59** (1989), no. 3, 785–801.
- [Car94] ———, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, Contemporary Mathematics **165** (1994), 213–237.
- [CR62] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Wiley Interscience, New York, 1962.
- [DDT97] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's Last Theorem*. In: *Elliptic Curves and Modular Forms*, Current

- Development in Mathematics, 1995, International Press, 1997,
www.math.mcgill.ca/darmon/pub/Articles/Expository/05.DDT/paper.pdf.
- [Del73] Pierre Deligne, *Formes modulaires et représentations de $GL(2)$* , Modular functions of one variable II, Springer, Berlin, 1973, pp. 55–105. Lecture Notes in Math., Vol. 349.
- [Dia97] Fred Diamond, *An extension of Wiles' results*, Modular Forms and Fermat's last Theorem, Tata Institute of Fundamental Research Studies in Mathematics, Springer, New York, 1997.
- [Die01] Luis Dieulefait, *Newforms, inner twists, and the inverse Galois problem for projective linear groups*, Journal de théorie des nombres de Bordeaux **13** (2001), no. 2, 395–411,
http://www.numdam.org/numdam-bin/item?id=JTNB_2001__13_2_395_0.
- [Die06] ———, *Remarks on Serre's modularity conjecture*, Preprint (2006), [arXiv:math/0603439v9](https://arxiv.org/abs/math/0603439v9).
- [DR73] Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable II, Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.
- [dS97] Ehud de Shalit, *Hecke rings and universal deformation rings*, Modular Forms and Fermat's last Theorem, Tata Institute of Fundamental Research Studies in Mathematics, Springer, New York, 1997.
- [DT09] Luis Dieulefait and Xavier Taixés i Ventosa, *Congruences between modular forms and lowering the level mod ℓ^n* , Journal de Théorie des Nombres de Bordeaux **21** (2009), no. 1, 83–92,
http://jtnb.cedram.org/item?id=JTNB_2009__21_1_83_0.
- [DV00] Luis Dieulefait and Núria Vila, *Projective linear groups as Galois groups over \mathbb{Q} via modular representations*, Symbolic Computation **30** (2000), 799–810.
- [Fre94] Gerhard Frey, *Construction and arithmetical applications of modular forms of low weight*, C.R.M. Proc. and Lecture Notes **4** (1994), 1–21.

-
- [Fre01] ———, *Galois representations attached to elliptic curves and diophantine problems*, Number Theory, eds. M. Juila and T. Metsänkylä, De Gruyter, Berlin (2001), 71–104,
<http://www.exp-math.uni-essen.de/zahlentheorie/preprints/turku.ps>.
- [Gou01] Fernando Q. Gouvêa, *Deformations of Galois representations*, Arithmetic Algebraic Geometry, IAS/Park City Mathematics Series, vol. 9, American Mathematical Society, 2001.
- [Kis] Mark Kisin, *Modularity of 2-adic barsotti-tate representations*, Preprint,
<http://www.math.uchicago.edu/~kisin/dvifiles/serre2.dvi>.
- [Klü] Jürgen Klüners, *A database for number fields*,
www.math.uni-duesseldorf.de/~klueners/minimum/minimum.html.
- [KWa] Chandrashekar Khare and Jean-Pierre Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$* , To appear in Annals of Math.,
<http://www.math.utah.edu/~shekhar/serre.pdf>.
- [KWb] ———, *Serre's modularity conjecture (I)*, Unpublished preprint,
<http://www.math.utah.edu/~shekhar/results.pdf>.
- [KWc] ———, *Serre's modularity conjecture (II)*, Unpublished preprint,
<http://www.math.utah.edu/~shekhar/proofs.pdf>.
- [KW07] Lloyd James Peter Kilford and Gabor Wiese, *On the failure of the gorenstein property for hecke algebras of prime weight*, Preprint (2007), [arXiv:math/0612317v1](https://arxiv.org/abs/math/0612317v1).
- [Lan84] Serge Lang, *Algebra, 2nd edition*, Addison-Wesley, 1984.
- [Maz77] Barry Mazur, *Modular curves and the Eisenstein ideal*, Publications mathématiques de l'I.H.É.S. **47** (1977), 33–186,
http://www.numdam.org/item?id=PMIHES_1977__47__33_0.
- [Maz97] ———, *An introduction to the deformation theory of Galois representations*, Modular Forms and Fermat's Last Theorem, Tata Institute of Fundamental Research Studies in Mathematics, Springer, New York, 1997.

- [Mum74] David Mumford, *Abelian varieties*, second ed., Tata Institute of Fundamental Research Studies in Mathematics, no. 5, Oxford University Press, 1974.
- [MW06] Jean-François Mestre and Gabor Wiese, Appendices to “*Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one*”, *J. Inst. Math. Jussieu* **5** (2006), no. 1, 1–34, [arXiv:math/0312019v1](https://arxiv.org/abs/math/0312019v1).
- [Oes88] Joseph Oesterlé, *Nouvelles approches du “Théorème” de Fermat*, *Séminaire Bourbaki* **30** (1987–1988), 165–186, http://www.numdam.org/item?id=SB_1987-1988__30__165_0.
- [Pau01] Sebastian Pauli, *Efficient enumeration of extensions of local fields with bounded discriminant*, Ph.D. thesis, Concordia University, 2001, <http://www.math.tu-berlin.de/~pauli/papers/phd.pdf>.
- [Rib85] Kenneth A. Ribet, *On ℓ -adic representations attached to modular forms II*, *Glasgow Math.* **27** (1985), 185–194, <http://math.berkeley.edu/~ribet/Articles/rankin.pdf>.
- [Rib90a] ———, *On modular representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms*, *Invent. Math.* **100** (1990), 431–476, http://math.berkeley.edu/~ribet/Articles/invent_100.pdf.
- [Rib90b] ———, *Raising the levels of modular representations*, *Séminaire de Théorie des Nombres, Paris 1987–88*, *Progress in Mathematics* **81** (1990), 259–271, <http://math.berkeley.edu/~ribet/Articles/dpp.pdf>.
- [Rib92] ———, *Abelian varieties over \mathbf{Q} and modular forms*, *Proc. KAIST Mathematics Workshop*, Korea Adv. Inst. Sci. Tech., Taejon (1992), 53–79, <http://math.berkeley.edu/~ribet/Articles/korea.pdf>.
- [Rib94] ———, *Report on mod ℓ representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$* , *Motives* (Seattle, WA, 1991). Providence, RI: Amer. Math. Soc. Proc. Sympos. Pure Math. **55** (1994), 639–676, <http://math.berkeley.edu/~ribet/Articles/motives.pdf>.

-
- [Rib97] ———, *Images of semistable Galois representations*, Olga Taussky-Todd: in memoriam, Pacific J. Math. **Special Issue** (1997), 277–297,
<http://nyjm.albany.edu:8000/PacJ/1997/181-3-16.pdf>.
- [RV95] Alfons Reverter and Núria Vila, *Some projective linear groups over finite fields as Galois groups over \mathbb{Q}* , Contemporary Mathematics **186** (1995), 51–63.
- [Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
- [Ser79] ———, *Local fields*, Springer Verlag, 1979.
- [Ser87] ———, *Sur les représentations modulaires de degré 2 de $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$* , Duke Mathematical Journal **54** (1987), no. 1, 179–230.
- [Shi73] Goro Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544.
- [ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.
- [Ste07] William A. Stein, *Explicitly computing with modular forms*, Graduate Studies in Mathematics, American Math Society, 2007,
<http://modular.math.washington.edu/msri06/refs/stein-book-on-modular-forms.pdf>.
- [TW95] Richard Taylor and Andrew J. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572,
<http://math.stanford.edu/~lekheng/flt/taylor-wiles.pdf>.
- [TW09] Xavier Taixés i Ventosa and Gabor Wiese, *Computing congruences of modular forms and Galois representations modulo prime powers*, In preparation (2009).
- [Wiea] Gabor Wiese, *Heckealgebra*,
<http://www.uni-due.de/~hx0037/programs/HeckeAlgebra>.
- [Wieb] ———, *On projective linear groups over finite fields as Galois groups over the rational numbers*, in “Modular Forms on Schiermonnikoog”, edited by Gerard van der Geer, Ben Moonen and Bas

Bibliography

- Edixhoven, Cambridge University Press, to appear.,
[arXiv:math/0606732v4](https://arxiv.org/abs/math/0606732v4).
- [Wie04] ———, *Dihedral galois representations and Katz modular forms*,
Documenta Math. **9** (2004), 123–133,
<http://www.emis.de/journals/DMJDMV/vol-09/07.pdf>.
- [Wie06] ———, *Multiplicities of Galois representations of weight one*,
Preprint (2006), [arXiv:math/0612318v1](https://arxiv.org/abs/math/0612318v1).
- [Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*,
Annals of Mathematics **141** (1995), no. 3, 443–551,
<http://math.stanford.edu/~lekheng/flt/wiles.pdf>.

Glossary of Notations

(N_f, i_f)	$(N_f, i_{N_f}), 10$
(N, i_N)	i_N -th newform of level N , 10
1	identity matrix, 12
A	Abelian variety, 16
A	complete noetherian local ring, 13, 61
A_f	abelian variety coming from f , 11, 53
A_f^*	dual variety of A_f , 12
$A[m]$	m -torsion subgroup of A , 16
$\text{Aut}(\mathcal{R})$	automorphisms of \mathcal{R} , 16
$a_n, a_n(f)$	n -th coefficient of the modular form f , 9
α_n	map from $X_0(nN)$ to $X_0(N)$, 8
α_n^*	Pic functoriality, 8
β_n	map from $X_0(nN)$ to $X_0(N)$, 8
$(\beta_n)_*$	Albanese functoriality, 8
C_N	cyclic group of order N , 8
$c^{(p_i)}$	$\gcd(c^{(p(i-1))}, c_{p_i} \cdot V_{p_i}(c^{(p(i-1))}))$, 38
$c(P, Q), c_p(P, Q)$	local congruence number at p , 35
\mathbb{C}	complex numbers, 8
d_f	degree of K_f over \mathbb{Q} , 52
\det	determinant, 18
E	elliptic curve, 8, 12
E_{tors}	torsion subgroup of E , 17

$e_{L/K}$	ramification index of L/K , 30
Frob_p	p -Frobenius element, 12
f	modular form, 8, 30
$\mathbb{F}_{f,\lambda}$	the residue field of $\mathcal{O}_{f,\lambda}$, 19
φ_f	morphism from $\mathbb{T}_{\mathbb{Q}}$ to \mathbb{C} , 11, 22
$\bar{\varphi}_f$	reduction of φ_f to $\bar{\mathbb{F}}_{\ell}$, 22
G	$\bar{\rho}(G_{\mathbb{Q}})$, 14
G_i	ramification group of G , 14
$G_{K,S}$	$\text{Gal}(\bar{K}_S/K)$, 62
$G_{\mathbb{Q}}$	absolute Galois group, 12
\mathcal{G}	topological group, 12
$\Gamma_0(N)$	subgroup of $SL_2(\mathbb{Z})$ such that each element reduces modulo N to an upper triangular matrix, 7
$\gamma(n), \gamma_{L/K}(n)$	$(n-1)e_{L/K} + 1$, 30
H, H_f	Hecke Bound of f , 46
\mathcal{H}	upper half plane $\{z \in \mathbb{C} \mid \Im(z) > 0\}$, 7
\mathcal{H}^*	completed complex upper half plane, 7
I_f	ideal $\ker(\varphi_f) \cap \mathbb{T}$, 11
\mathcal{I}_p	inertia group at p , 12
$J_0(N)$	Jacobian of $X_0(N)$, 8
$J_0^{\text{Tor}}(N)$	Torsion points of $J_0(N)$, 27
K	a field, usually an ℓ -adic field extension, 13, 30
K_f	field generated by the coefficients of f , 11, 30
$K_{f,\ell}$	$K_f \otimes \mathbb{Q}_{\ell}$, 17
\bar{K}_S	maximal algebraic extension unramified outside S , 62
k	weight of a modular form, 8
$k_{\mathcal{R}}$	residue field of \mathcal{R} , 13
L	global congruence number, 32

$L^+, L^+(f, g)$	upper bound of congruence between f and g , 32
$L^-, L^-(f, g)$	lower bound of congruence between f and g , 32, 46, 50
ℓ	a prime, 30
λ	a place dividing ℓ , 30
$M_k(N)$	modular forms of weight k and level N , 9
\mathfrak{m}_f	$\text{Ker}(\overline{\varphi}_f)$, 22
N	positive integer, generally representing the level of a modular form or the conductor of a representation, 7
\overline{N}	Serre conductor of $\overline{\rho}$, 15
N_f	level of the form f , 30
$n_p, n_{\overline{\rho}, p}, n_{\rho, p}$	exponent of the Serre conductor, 14
\mathcal{O}	ring of integers of K , 30
\mathcal{O}_f	ring of integers of K_f , 18, 30
$\mathcal{O}_{f, \ell}$	$\mathcal{O}_f \otimes \mathbb{Z}_\ell$, 18
$\mathcal{O}_{f, \lambda}$	$\mathcal{O}_{f, \ell} = \prod_{\lambda \ell} \mathcal{O}_{f, \lambda}$, 18
\overline{P}	reduction of the polynomial P modulo ℓ , 36
$P_{f, p}$	$\prod_{\sigma} P'_{\sigma(f), p}$, 31
$P'_{f, p}(X)$	characteristic polynomial of $\overline{\rho}_{f, \lambda}(\text{Frob}_p)$, 31
$P_{\rho, p}(X)$	characteristic polynomial of $\rho(\text{Frob}_p)$, 13
p	prime, 9
\mathfrak{p}	place in $\overline{\mathbb{Q}}$ dividing p , 12
\mathbb{P}	set of prime numbers, 17
Π	profinite group, 13, 61
$Q_{f, p}$	$\prod_{\sigma} Q'_{\sigma(f), p}$, 37
$Q'_{f, p}$	minimal polynomial of the eigenvalue of the p -Hecke Operator on f , 37
\mathcal{Q}	deformation conditions, 63
\mathbb{Q}	rational numbers, 7

$\overline{\mathbb{Q}}$	algebraic closure of \mathbb{Q} , 12
\mathcal{R}	an arbitrary ring, a \mathcal{G} -module, 9
\mathcal{R}	universal ring, 62
ρ	linear representation, 12
ρ^{univ}	universal deformation, 62
$\overline{\rho}$	residual representation, 13
$\rho_{f,\ell}$	ℓ -adic representation attached to f , 17
$\overline{\rho}_{f,\ell}, \overline{\rho}_{f,\ell}^{ss}$	$mod \ell$ representation attached to f , 19
$\overline{\rho}_{f,\ell^n}$	$mod \ell^n$ representation attached to f , 20, 31
$\rho_{f,\lambda}$	λ -adic representation attached to f , 18
$\overline{\rho}_{f,\lambda}$	$mod \lambda$ representation attached to f , 19
$\overline{\rho}_{f,\lambda^n}$	$mod \lambda^n$ representation attached to f , 21
$\overline{\rho}_{f,\mathfrak{m}^n}$	representation on $\mathbb{T}_{\lambda,\mathfrak{m}}/\mathfrak{m}^n$, 23
$\overline{\rho}_{\mathfrak{m}}$	representation attached to \mathfrak{m} , 22
$S_k(N)$	cuspidal forms of weight k and level N , 9
$S_k(\Gamma, \mathcal{R})$	$S_k(\Gamma, \mathbb{Z}) \otimes \mathcal{R}$, 9
$S_k(\Gamma, \mathbb{Z})$	elements of $S_k(N)$ with integral coefficients, 9
$S_k^{\text{new}}, S_k^{\text{new}}(N)$	new space of $S_k(N)$, 10
$S_k^{\text{old}}, S_k^{\text{old}}(N)$	space of old forms of $S_k(N)$, 10
$SL_2(\mathcal{R})$	2×2 matrices γ with $\det(\gamma) = 1$ and coefficients in \mathcal{R} , 7
Σ_f	set of embeddings of K_f in \mathbb{C} , 30
Σ_K	set of embeddings of K in \mathbb{C} , 25, 30
σ	element in $G_{\mathbb{Q}}$, 16
T_n	n -th Hecke operator, 8
$\mathcal{T}_{\ell}(A)$	Tate module of A , 17
$\mathcal{T}_{\lambda,\mathfrak{m}}$	localisation of \mathcal{T}_{λ} in \mathfrak{m} , 24
tr	trace, 13
$\mathbb{T}, \mathbb{T}(N)$	Hecke algebra of level N , 9
\mathbb{T}_{ℓ}	$\mathbb{T}_{\mathbb{Z}_{\ell}}$, 9
\mathbb{T}_{λ}	$\mathbb{T}_{\mathcal{O}_{\lambda}}$, 9
$\mathbb{T}_{\lambda,\mathfrak{m}}$	localisation of \mathbb{T}_{λ} in \mathfrak{m} , 23
$\mathbb{T}_{\mathcal{R}}$	$\mathbb{T} \otimes \mathcal{R}$, 9

V	free \mathcal{R} -module, 12
$V_p(c)$	inverse of the p absolute value of c , 38
Ver_p	p -Verschiebung element, 18
v	discrete valuation of K , 17
W	$J_0(N)[\mathfrak{m}]$, 22
W^n	$J_0(N)[\mathfrak{m}^n]$, 22
$X_0(N)$	modular curve, 8
\mathbb{Z}	integers, 7
$\overline{\mathbb{Z}}$	algebraic integers, 32, 36
$\overline{\mathbb{Z}}_\ell$	algebraic ℓ -adic integers, 36
$\hat{\mathbb{Z}}$	$\varprojlim_m \mathbb{Z}/m\mathbb{Z}$, 16

Index

- Abelian variety of GL_2 -type, 25
- Artin representation, 13
- Brauer-Nesbitt Theorem, 12
- Chebotarev's density theorem, 14
- Conductor
 - Serre, 15
- Congruence number, 35
 - global, 33
 - local, 35
- Congruence of modular forms, 26, 31
- Conjecture
 - Serre, 25
 - Shimura-Taniyama-Weil, 25
- Criterion of Néron-Ogg-Shafarevich, 17
- Cusp, 7
 - form, 9
- Deformation, 62
 - condition, 63
 - universal, 62
- Eigenform, 10
- Elliptic curve, 12
- Galois representation, 12
- GL_2 -type Abelian variety, 25
- Global congruence number, 33
- Hecke
 - algebra, 9
 - bound, 46
 - operator, 8
- Irreducible representation, 12
- ℓ -adic representation, 13
- Linear representation, 12
- Local congruence number, 35
- LowerBound1.0, 50
- Lowering the Level, 59
- Minimal at ℓ
 - modular form, 18
 - representation, 15
- $\text{mod } \ell^n$ representation, 13, 31
- Modular
 - curve, 8
 - form, 9
 - group, 8
- Néron-Ogg-Shafarevich Criterion, 17
- New space, 10
- Newform, 10
- Normalized form, 10
- Odd representation, 12
- Old
 - form, 10
 - space, 10
 - space modulo ℓ^n , 48
- p -new representation, 51

- pBound, 39
- Petersson scalar product, 10
- Prime of congruence, 26
- Push-forward, 63
- Realization of groups, 54
- Representation, 12
 - mod* ℓ^n , 13, 31
 - Artin, 13
 - Galois, 12
 - irreducible, 12
 - ℓ -adic, 13
 - minimal, 15
 - odd, 12
 - p -new, 51
 - residual, 13
 - semi-simple, 12
 - simple, 12
 - strongly irreducible, 58
 - unramified, 13
- Residual representation, 13
- Ribet's Lowering the Level, 59
- Semi-simple representation, 12
- Serre
 - conductor, 15
 - Conjecture, 25
- Shimura's theorem, 11
- Shimura-Taniyama-Weil Conjecture, 25
- Simple representation, 12
- Strict equivalence of reprs., 62
- Strongly irreducible representation, 58
- Sturm bound, 46
- Sylvestrer matrix, 35
- Tate module, 17
- Theorem
 - Brauer-Nesbitt, 12
 - Chebotarev, 14
 - Raising the Level, 51
 - Shimura, 11
- Torsion subgroup, 16
- Universal
 - deformation, 62
 - ring, 62
- UpperBound1.0, 41
- UpperBound1.1, 45