UNIVERSITAT DE
BARCELONA

New results on modular forms and Fermat-type equations

Eduardo Soto Ballesteros

UNIVERSITAT DE BARCELONA

New results on modular forms and Fermat-type equations

Eduardo Soto Ballesteros

Programa de Doctorat de Matemàtiques i Informàtica
Universitat de Barcelona
Juliol de 2019

2010 Mathematics subject Classification: 11F33, 11F80, 11D41, 11G05.
Descriptors o paraules clau: pujada de nivell, representacions de Galois, cadenes segures, primers de Steinberg, congrüències de formes modulars, equacions de tipus Fermat.

Amb el finançament parcial d?una beca FPI del *Ministerio de Ciencia, Innovación y Universidades* i dels projectes MTM2013-45075-P, MTM2016-78623-P.

New results on modular forms and Fermat-type equations.

Programa de Doctorat de Matemàtiques i Informàtica.
Memòria presentada per aspirar al grau de Doctor en Matemàtiques per la Universitat de Barcelona.

Certifiquem que la present memòria ha estat realitzada per Eduardo Soto Ballesteros i dirigida per nosaltres.
Barcelona, Juliol 2019.

Luis Dieulefait

Rosa Maria Miró-Roig

A mis abuelos Isabel y Manolo,
a mis padres Paqui y Edu,
a mi hermano Beto.

Proemium

Let $\mathbb{Q}$ be the field of rational numbers and let $\bar{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$. The absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is profinite with the Krull topology. In general it is a hard problem to prove or disprove the existence of a continuous quotient $G_{\mathbb{Q}} \twoheadrightarrow P$ for a fixed profinite group P. One says that P is Galois over $\mathbb{Q}$ if there is such a morphism. Equivalently the problem consists in proving or disproving the existence of a Galois extension $L/\mathbb{Q}$ with Galois group isomorphic to P. This is the so-called inverse Galois problem for P. A classical conjecture states that every finite group P is a Galois group over $\mathbb{Q}$. It is worth noting that the infinite case is false in general; e.g. it is a consequence of the Kronecker-Weber theorem that the profinite group $\mathbb{Z}_p^2$ is not Galois over $\mathbb{Q}$.

Let $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ denote the ring of profinite integers, that is the profinite completion of the ring $\mathbb{Z}$ of integers. The theory of abelian varieties or even algebraic groups provides continuous morphisms $G_{\mathbb{Q}} \to \mathrm{GL}_n(\hat{\mathbb{Z}})$. As a consequence, one can realize many linear groups as Galois groups over $\mathbb{Q}$. Let us see three examples.

1. The group $\mathrm{GL}_1(\hat{\mathbb{Z}}) = \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ is a Galois group over $\mathbb{Q}$. Indeed, one can take the infinite cyclotomic extension $L = \mathbb{Q}(\mu_n)_{n\geq 1}/\mathbb{Q}$ where μ_n denotes the group of nth roots of unity in $\bar{\mathbb{Q}}^\times$. Hence
$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^\times.$$
This is the Galois representation attached to the algebraic group $\mathbb{G}_m$.

2. The extension $\mathbb{Q}(E(\bar{\mathbb{Q}})[n])_{n\geq 1}/\mathbb{Q}$ is a natural generalization of the cyclotomic case, where $E(\bar{\mathbb{Q}})[n]$ denotes the group of n-

torsion points for a rational elliptic curve E. The linear action of $G_{\mathbb{Q}}$ on $E(\bar{\mathbb{Q}})[n]$ induces a morphism

$$\rho_E : G_{\mathbb{Q}} \to \prod_p \mathrm{Aut}_{\mathbb{Z}_p} \mathcal{T}_p E \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

where $\mathcal{T}_p E$ denotes the p-adic Tate module of E.

Theorem (Serre [48]). *With the notation above ρ_E is never surjective. Moreover,*

(a) either E has complex multiplication,

(b) or the image of ρ_E has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

3. Let f be a weight 2, level N newform with trivial character, let K denote the number field generated by its Fourier coefficients and $\mathcal{O}$ the ring of integers of K. The existence of an abelian variety A_f over $\mathbb{Q}$ attached to f is due to Shimura. The group of torsion points of A_f induces a morphism

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathcal{O}}) = \prod_{\mathfrak{p}} \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$$

where $\hat{\mathcal{O}}$ denotes the profinite completion of $\mathcal{O}$. See [34] for a description of the image of ρ_f.

These examples are strongly related. The first one $G_{\mathbb{Q}} \twoheadrightarrow \hat{\mathbb{Z}}^\times$ arises as the determinant of the others. One also has the highly non trivial

Theorem (Modularity, Wiles, Breuil-Conrad-Diamond-Taylor). *Every elliptic curve over $\mathbb{Q}$ is (in the isogeny class of) an abelian variety A_f for some newform f of weight 2.*

As a consequence, ρ_E arises as the Galois representation ρ_f for some newform f up to isogeny.

The purpose of this thesis is to study these Galois representations attached to newforms.

Let $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathcal{O}})$ be the morphism attached to f and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$. The projection $\hat{\mathcal{O}} \to \mathcal{O}_{\mathfrak{p}} \to \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ induces a morphism

$$\bar{\rho}_{\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}).$$

This is the so-called mod $\mathfrak{p}$ Galois representation attached to f.

Different newforms f, g define non isomorphic representations ρ_f, ρ_g. Nevertheless, they may share some residual Galois representations. To be more precise, let f,g be newforms and let $\mathfrak{p}$, $\mathfrak{p}'$ be maximal ideals of $\mathcal{O}_f$ and $\mathcal{O}_g$. We say that $\bar{\rho}_{f,\mathfrak{p}}$ and $\bar{\rho}_{g,\mathfrak{p}'}$ are isomorphic if there is a maximal ideal $\mathfrak{q}$ in the compositum field $K_f K_g$ containing $\mathfrak{p}, \mathfrak{p}'$ such that $\bar{\rho}_{f,\mathfrak{p}}$, $\bar{\rho}_{g,\mathfrak{p}'}$ are isomorphic as representations mod $\mathfrak{q}$. In this case we say that f, g are congruent mod $\mathfrak{q}$. A natural question arises:

What can be said about newforms g congruent to a fixed newform f?

This question has many answers due to the work of Hida, Kisin, Mazur, Ribet, Serre, Taylor or Wiles. Ribet's level raising [45] and level lowering [46] theorems are prototypical examples in this topic since they describe some changes of level through congruences. It is worth mentioning that the Modularity Theorem proved by Wiles combined with the Level Lowering Theorem proved by Ribet provides striking applications to the theory of Diophantine equations such as Fermat's Last Theorem.

The content of our work is divided in 2 parts: we give new answers to the question arisen above in Chapters 2 and 3 and we solve new cases of Fermat-type diophantine equations in Chapter 4. Chapters 2 and 3 have been accepted for publication in prestigious journals, see [17], [18]. We now briefly describe the content.

- Chapter 1 is a chapter of preliminary topics in which we recall to the reader the Galois theory of $\bar{\mathbb{Q}}/\mathbb{Q}$, Galois representations, modular forms and elliptic curves. Therein, we consider the special case of Frey curves. The last section is devoted to the study of cyclotomic polynomials used in Chapter 4 to solve some S-unit equations.

- In Chapter 2 we describe the phenomenon of sign change at a Steinberg prime. Newforms with Steinberg prime p, i.e. such that p divides the level once, admit one of two possible behaviors at p, depending on the sign $a_p \in \{\pm 1\}$. We describe the case where two congruent newforms with common Steinberg prime p may have different sign at the pth coefficient a_p. Furthermore, if f is a newform with a Steinberg prime p we find necessary and

sufficient conditions on $\bar{\rho}_{f,\mathfrak{p}}$ to ensure the existence of a newform g congruent to f with different sign at the Steinberg prime p. Our strategy is as follows: we remove p from the level of f by a level lowering theorem. Then we add p to the level with a level raising theorem that allows us to choose the sign a_p. We prove that the level lowering theorem applies to f if and only if such a g exists. We restrict to the irreductible case with residual odd characteristic

- Chapter 3 is devoted to level raising at an arbitrary prime. Let f be a (weight 2) newform such that the mod $\mathfrak{p}$ Galois representation $\bar{\rho}_{f,\mathfrak{p}}$ is irreducible for every $\mathfrak{p}$ and let p be a prime not in the level of N. We prove that $a_p^2 - (p+1)^2$ is not a unit in $\mathcal{O}_f$. We combine this with a theorem of Ribet to ensure the existence of a newform g congruent to f with p in the level. We also prove some variants of this statement where one can choose the sign a_p of g.

- In Chapter 4 we solve new cases of the Asymptotic Fermat Conjecture (AFC) with coefficients. This conjecture is connected with Galois representations due to the work of Frey and Mazur. We follow here the effective approach of Kraus so that we can give explicit bounds. The exposure of some local obstructions to S-unit equations allows us to solve $ax^p + by^p = cz^p$ asymptotically on p with abc containing an arbitrary number of prime factors. We shall point out that all the instances infinite families of AFC solved previous to our work consider only the case $\mathrm{rad}(abc) \mid 2p$.

Acknowledgments

Quiero dar las gracias a Luis Dieulefait por sus ideas y generosidad durante todos estos años, espero que evidentes en el presente texto. Gràcies a la Rosa Maria Miró-Roig i a la Laura Costa pel seu suport en aquest projecte i per pensar en mi en un primer moment. Amb aquest escrit acaba una etapa que he tingut la sort de compartir amb moltes i enriquidores persones.

Gràcies als professors Carlos d'Andrea, Sara Arias-de-Reyna, Pilar Bayer Isant, Nicolas Billerey, María J. Carro, Carles Casacuberta Vergés, Eduard Casas Alvero, Carme Cascante Canut, Teresa Crespo, Juan Elias, Olga Lavila-Vidal, Xavier Massaneda, Ignasi Mundet i Riera, Joan Carles Naranjo del Val, Joaquim Ortega Cerdà, Ariel Pacetti, Victor Rotger, Martín Sombra, Javier Soria, Artur Travesa, Núria Vila i Xavier Xarles, Santiago Zarzuela Armengou per les múltiples discussions i caliu. María Jesús y Javier os deseo toda la suerte y éxitos en vuestro nuevo proyecto.

Thanks to the research group Laia Amoros, Jasper Van Hirtum, Chun Yin Hui, Marigiulia De Maria, Alexander de Rham, Panagiotis Tsaknias, Katharina Heil and Marie Leblanc leaded by Gabor Wiese for the warm reception during my stay in Luxembourg.

Thanks to professor Jacques Tilouine for the warm reception during my stay in Paris. Thanks to professor Benoît Stroh for his courses.

Als companys Yairon Cid, Roberto Gualdi, Roser Homs, Mikel Lluvia i Fatmanur Yıldırım del seminari DATGA amb qui he crescut matemàticament. Gràcies Roser, amb tu he après àlgebra commutativa. Grazie Roberto, le molteplici discussioni che abbiamo avuto mi hanno portato sempre nuovi punti di vista. Spero che continui così per molti anni. Als participants del seminari de teoria de cossos de classe Alex Cebrian, Mar Curcó, Giancarlo Gebbia, Bruno Mazorra, Piermarco Milione i Anna Somoza. A los participantes del seminari de formes automorfes Daniele Casazza, Francesca Gatti, Daniel Gil y Óscar Rivero. Gràcies Eduard Roure per ajudar-me en l'organització. Als participants del seminari de prehistòria de Fermat Marc Adillon, Guillem Garcia-Tarrach, Enric Florit, Andriana Karuk i Adriana Moya. Gràcies Bruno i Andriana per la vostra confiança.

Gràcies a l'Alberto Cámara, Gemma Colomé Nin, Alberto F. Boix, Elisa Lorenzo Garcia, Piermarco, Marta Narváez, Joan Nualart i Adrián Zenteno per acompanyar-me durant els primers anys de tesi i a en Xevi Guitart i Carlos de Vera Piquero per fer-ho en els darrers. Als participants i organitzadors del STNB Montserrat Alsina Aubach, Francesc Bars, Marc Masdeu, Santiago Molina, Bernat Plans Berenguer. Obrigado Nuno Freitas. Grazie Samuele Anni.

Als meus companys Marta Bofill Roig, Pau, Gemma Colldeforns Papiol, Alberto Debernardi, Victòria Gras Andreu, Adrià, Jordina i

Francesc Pons Llopis.

Moltíssimes gràcies al personal de secretaria del departament, molt especialment al Víctor i a la Montse.

Gracias Alberto, Anna, Arià, Francesc, Mariagiulia, Merce, Roberto, Samuele, Sergi y Tania por todos los puntos de apoyo. Gràcies Joana, gràcies Èric i gràcies Joima. Als meus amics els Autobuseros i a les seves famílies. A mis primos y tíos. Gracias a los Collbareños Alejandro, Alex (Yarza), Alicia, David, Gustavo, Marc, Mateus y Victòria.

Al Colegio de España y mis amigos Fer, Jorge, Mario. Als companys de CDLD i Golois. A les Terres de Marca de la Concepció, a Brevis et Solemnis del Josep, a la Xalest del Pol i a l'Albada de l'Esteve. Al Lozano i a l'Andreu-Manel. A tots moltes gràcies,

Edu

Contents

Chapter 1

Preliminary topics

Rings are assumed to be commutative and unitary unless the contrary is said.

1.1 Galois theory

In this section we recall some classic Galois theory. See [59, Chapter 1] for a concise exposition.

1.1.1 Algebraic extensions

Let K be a *field*, that is, a ring whose group of units $K^\times$ equals $K \setminus \{0\}$.[1] By an *extension* L of K, also written as L/K, we mean a K-algebra L which is a field.[2]

The *degree* of L/K is

$$[L : K] := \dim_K L$$

as a K-module. Thus $1 \leq [L : K] \leq \infty$ and L/K is *finite* if

$$\dim_K L < \infty.$$

Let L/E, E/K be algebraic extensions, let $\{\alpha_i\}_i$, $\{\beta_j\}_j$ be bases of L/E and E/K respectively then $\{\alpha_i\beta_j\}_{i,j}$ is a basis of L/K. In

[1] In particular the **0** ring is not a field.

[2] The structural map $\iota : K \to L$ is a monomorphism of rings since K has no non-trivial proper ideals. We shall identify K with the image $\iota(K)$.

particular one obtains the so-called *product formula*

$$[L : K] = [L : E] \cdot [E : K].$$

for finite extensions L/E, E/K. Let $K[X]$ be the ring of polynomials in one variable over K and let $x \in L$. The evaluation map

$$\begin{array}{rccc} e_x : & K[X] & \longrightarrow & L \\ & P(X) & \longmapsto & P(x) \end{array}$$

is a homomorphism of K-algebras. The image of e_x is a quotient of $K[X]$ usually denoted by $K[x]$. The ring $K[X]$ is Euclidean, hence it is a principal ideal domain and non-zero prime ideals are maximal. The following conditions are equivalent

(i) e_x has non trivial kernel,

(ii) the kernel of e_x is a maximal ideal of $K[X]$,

(iii) $K[x]$ is a K-module of finite rank,

(iv) $K[x]$ is a field.

If that is the case then x is *algebraic over* K and there is a unique monic polynomial $Irr(x, K)$ generating the ideal $\ker e_x$. The polynomial $Irr(x, K)$ is known as the *irreducible polynomial* of x over K.[3] Similarly, $K(x)$ denotes the field of fractions of $K[x]$. Notice that $K(x) = K[x]$ if and only if x is algebraic. As a matter of taste we shall avoid square brackets when possible.

An extension L/K is *algebraic* if every element $x \in L$ is algebraic over K. Equivalently one has the

Proposition 1.1.1. *Let L be a K-algebra. Then, L is an algebraic extension of K if and only if every K-subalgebra E of L is a field.*

Proof. Let E be a K-subalgebra of L and let $x \in E \setminus \{0\}$. Since L is algebraic then $K[x]$ is a subfield of E. Hence $x^{-1} \in K[x] \subseteq E$. Reciprocally, L and $K[x]$ are fields for every $x \in L$, by hypothesis. □

Proposition 1.1.2. *Finite extensions are algebraic.*

[3] It is certainly irreducible in $K[X]$ since $K[x]$ is a subring of L.

Proof. L is a K-module of finite rank hence $K[x] \subseteq L$ is a K-submodule of finite rank. □

A field K is *algebraically closed* if every algebraic extension L/K is trivial. An *algebraic closure* of K is an algebraic extension of K that is algebraically closed. One generally needs the Axiom of Choice to prove the existence of algebraic closures of K.

Theorem 1.1.3. *Let K be a field.*

(i) There exists an algebraic closure $\bar{K}$ of K. If $\bar{K}, \bar{K}'$ are algebraic closures of K then they are (non-canonically) isomorphic as K-algebras.

(ii) Let L/K be an algebraic extension. Then there is an embedding $\theta : L \to \bar{K}$ of K-algebras.

(iii) With the notation above assume that L is algebraically closed. Then any such θ is an isomorphism.

See [28, V.2.6 and V.2.8] for a proof.

Notice that a field K is algebraically closed if every polynomial in $K[X]$ splits into linear factors in $K[X]$.

1.1.2 Simple extensions

Simple extensions are central in the theory of number fields. We shall summarize some of their properties.

An algebraic extension L/K is *simple* if there is $x \in L$ such that $L = K[x]$. In this case $L \simeq K[X]/(Irr(x, K))$ and $n := [L : K] = \deg Irr(x, K)$ since $1, x, \ldots, x^{n-1}$ is a K-basis of $K[x]$. Hence simple extensions are finite.

Proposition 1.1.4. *Let L/K be an extension of finite fields. Then L/K is simple.*

Proof. The abelian group $L^\times$ is cyclic since the ℓ-torsion $\{x \in L^\times : x^\ell = 1\}$ of $L^\times$ has either order 1 or ℓ for every prime ℓ. Let x be a generator of $L^\times$ then $L = L^\times \cup \{0\} \subseteq K[x]$ □

Let $L = K[x]/K$ be a simple extension. One can describe some intermediate K-algebras of L in an elementary manner. Let $P = Irr(x, K)$ and let Q be a monic divisor of P in $L[X]$, $Q = X^n + \sum_{0 \leq i \leq n-1} a_i X^i$. Then $K_Q := K[a_0, \ldots, a_{n-1}]$ is a K-subalgebra of L.

Lemma 1.1.5. *Let L be a simple extension of K, $L = K[x]/K$. Then the previous construction describes all K-subalgebras of L, that is,*

$$\{K_Q : Q \text{ is a monic divisor of } Irr(x, L) \text{ in } L[X]\}$$

is the set of K-subalgebras of L.

Proof. Let E be a K-subalgebra of L and let $Q = Irr(x, E)$. Let us see that $E = K_Q$. By construction $K_Q \subseteq E$ and $L = E[x] = K_Q[x]$. By the product formula it is enough to see that $Irr(x, E) = Irr(x, K_Q)$. Since $Irr(x, E)$ is a monic irreducible polynomial of $K_Q[X]$ and lies in the kernel $e_x : K_Q[X] \mapsto L$ then $Irr(x, E) = Irr(x, K_Q)$. □

By Proposition 1.1.1, the algebraic hypothesis can be read in terms of subalgebras. Emil Artin proved that it is also the case for the simple hypothesis.

Theorem 1.1.6 (E. Artin)**.** *Let L/K be a finite extension. Then L/K is simple if and only if L has finitely many K-subalgebras.*

Proof. If K is finite, then L is finite and both are true so we assume that K is infinite. Let $L = K[x]$ be a simple extension of K and let P be the irreducible polynomial $Irr(x, K)$. By the previous lemma all K-subalgebras of L arise as K_Q for some monic divisor Q of P in $L[X]$. A polynomial in $L[X]$ has finitely many monic divisors in $L[X]$ thus L has finitely many K-subalgebras.

Let L/K be a finite extension with finitely many K-subalgebras. We say that a finite set S in L generates L/K if $K[S] = L$. For example, a basis of L as K-module generates L/K. Let $S = \{x_1, \ldots, x_m\}$ be a set generating L/K with minimal cardinality $|S| = m$. If $0 \leq m \leq 1$ we are done. Otherwise, consider the subalgebra $E := K(x_1, x_2)$. The field $K_a = K(x_1 + ax_2)$ is a K-subalgebra of E for every $a \in K$. Since K is infinite and L has finitely many K-subalgebras there are $a, b \in K$, $a \neq b$ so that $K_a = K_b$. One can use some elementary linear algebra to prove that $x_1, x_2 \in K_a$. Hence $L = K(x_1, x_2, x_3, \ldots, x_m) =$

$K(x_1 + ax_2, x_3, \dots x_m)$, that is $\{x_1 + ax_2, x_3, \dots, x_m\}$ is a set of cardinality $m-1$ generating L/K. □

In particular, if L/K is simple and E is a K-subalgebra of L then E/K is simple.

1.1.3 Galois extensions

Let L/K be an algebraic extension, L/K is *separable* if for every $x \in L$ the polynomial $Irr(x, K)$ has no multiple roots in an algebraic closure of K. This does not depend on the choice of $\bar{K}$ by Theorem 1.1.3.

Lemma 1.1.7. *Let L/K be a finite separable extension and let $\bar{K}$ be an algebraic closure of K. Then $\mathrm{Hom}_K(L, \bar{K})$ has $\leq [L : K]$ embeddings. The equality is satisfied if and only if L/K is separable.*

Proof. Let $x_1, \dots, x_n$ be a K-basis of L, then $L = K(x_1, \dots, x_n)$. This defines a tower

$$L/K(x_1, \dots x_{n-1})/ \cdots /K(x_1)/K$$

of simple field extensions. It is enough to prove the case $K(x)/K$ of simple extensions due to the product formula. The set of K-homomorphisms $\theta : K(x) = K[X]/Irr(x, K) \to \bar{K}$ is in bijection with the set of roots of $Irr(x, K)$ in $\bar{K}$. The bijection is given by $\theta \mapsto \theta(x)$. Thus, $\mathrm{Hom}_K(K(x), \bar{K}) \leq \deg Irr(x, K) = [K(x) : K]$. Reciprocally, let us assume that $Irr(x, K)$ has multiple roots for some $x \in L$. The surjection $\mathrm{Hom}_K(L, \bar{K}) \to \mathrm{Hom}_K(K(x), \bar{K})$ given by restriction $\theta \mapsto \theta|_{K(x)}$ is $|\mathrm{Hom}_{K(x)}(L, \bar{K})|$-to-1. Thus

$$\begin{aligned} |\mathrm{Hom}_K(L, \bar{K})| &= |\mathrm{Hom}_{K(x)}(L, \bar{K})| \cdot |\mathrm{Hom}_K(K(x), \bar{K})| \\ &< [L : K(x)] \cdot [K(x) : K] = [L : K]. \quad \square \end{aligned}$$

Let $L/E/K$ be extensions. Then L/K is separable if and only if L/E, E/K are separable. We will see below that finite separable extensions contain finitely many subalgebras. This together with Artin's Theorem says that finite separable extensions are simple.

The separability condition is necessary in order to define the classical Galois group. It is not hard to prove that every algebraic closure $\bar{K}$ of K contains a *maximal* separable extension K^s, see [59, 1.1.9].

In the present text we will consider *perfect* fields, that is fields whose algebraic closure is separable.

Lemma 1.1.8. *Characteristic* 0 *fields and finite fields are perfect.*

Proof. Recall that a polynomial in $\bar{K}[X]$ has no multiple roots if and only if f, f' are coprime, where f' denotes the formal derivative. For the characteristic 0 case, if f is irreducible in $K[X]$ then f' is non-zero and f, f' are coprime since $\deg f' < \deg f$ and f is irreducible. Let K be a finite field and let $\bar{K}$ be an algebraic closure. Then K contains $\mathbb{F}_p$ for some prime p and $|K| = p^r$ for some r. Similarly if $x \in \bar{K}$ then $K(x)$ contains $\mathbb{F}_p$ and has cardinal p^s for some s. If $x = 0$ we are done. If $x \neq 0$ then $x^n = 1$ for some $n \mid \#K(x)^\times = p^r - 1$. Notice that $f = X^n - 1$ has no multiple roots since $f' = nX^{n-1}$, $n \neq 0$ in $\mathbb{F}_p$ and 0 is not a root of f. Thus $Irr(x, K) \mid x^n - 1$ has no multiple roots. □

Let L/K be a field extension and let $\mathrm{Aut}(L/K)$ denote the group of K-automorphisms of L. For a subgroup H of $\mathrm{Aut}(L/K)$ the set $L^H = \{x \in L : Hx = x\}$ is a K-subalgebra of L.

Example 1.1.9. *Let $K(x)/K$ be a simple algebraic extension. The map $\mathrm{Aut}(K(x)/K) \to \{$roots of $Irr(x, K)$ in $K(x)\}$, $\sigma \mapsto \sigma(x)$ is a bijection.*

Proposition 1.1.10. *Let L/K be a separable extension. The following are equivalent*

(i) $L^{\mathrm{Aut}(L/K)} = K$,

(ii) The polynomial $Irr(x, K)$ splits into linear factors in $L[X]$ for every $x \in L$.

(iii) Let $\bar{K}$ be an algebraically closed field containing L. Then every $\theta \in \mathrm{Hom}_K(L, \bar{K})$ satisfies $\theta(L) \subseteq L$.

Proof. Let $x \in L$. The orbit $O_x = \mathrm{Aut}(L/K)x$ is a finite set consisting in roots of $Irr(x, K)$. Let $\sigma \in \mathrm{Aut}(L/K)$, the natural automorphism $\sigma : L[X] \to L[X]$ acts trivially on $g_x = \prod_{\alpha \in O_x}(X - \alpha)$ since $\sigma(O_x) = O_x$; i.e. $g_x \in L[X]^{\mathrm{Aut}(L/K)}$. If $L^{\mathrm{Aut}(L/K)} = K$ then $g_x \in K[X]$. Since $\deg g_x \leq \deg Irr(x, K)$ and $g_x(x) = 0$ one deduces

$g_x = Irr(x, K)$. This proves $(i) \Rightarrow (ii)$. To prove $(ii) \Rightarrow (iii)$ notice that an embedding $L \to \bar{L}$ maps x to a root of $Irr(x, K)$. Finally, let $x \in L \setminus K$. The polynomial $Irr(x, K)$ has at least two roots x, x' in $\bar{L}$. The isomorphism of K-algebras $K(x) \to K(x')$, $x \mapsto x'$ extends to an automorphism σ of $\bar{L}$ by Theorem 1.1.3. The restriction $\theta|_L \in \mathrm{Aut}(L/K)$ is an automorphism of L since $\theta(L) \subseteq L$, It does not fix x. □

If all the conditions in the previous proposition are satisfied we say that L/K is a *Galois* extension and the *Galois group* of L/K is $\mathrm{Gal}(L/K) := \mathrm{Aut}(L/K)$. If K is a perfect field and $\bar{K}$ is an algebraic closure then $\bar{K}/K$ is Galois.

Corollary 1.1.11. *A finite extension L/K is Galois if and only if $[L : K] = |\mathrm{Aut}(L/K)|$.*

Proof. Let $\bar{K}$ be an algebraic closure of K containing L. If L/K is Galois then it is separable and $[L : K] = |\mathrm{Hom}_K(L, \bar{K})|$. Moreover, every $\theta \in \mathrm{Hom}_K(L, \bar{K})$ has image in L, thus lies in $\mathrm{Gal}(L/K)$. Reciprocally, every automorphism of L defines an element in $\mathrm{Hom}_K(L, \bar{K})$ via $L \subseteq \bar{K}$. Thus, $|\mathrm{Hom}_K(L, \bar{K})| \geq |\mathrm{Aut}(L/K)| = [L : K]$ and L/K is separable. In particular $|\mathrm{Hom}_K(L, \bar{K})| = |\mathrm{Aut}(L/K)|$ and every element of $\mathrm{Hom}_K(L, \bar{K})$ arises in this manner. Thus $\sigma(L) \subseteq L$ for every $\sigma \in \mathrm{Hom}_K(L, \bar{K})$. □

If L/K is Galois and E is a K-subalgebra of L then L/E is Galois. This follows from the inclusion $\mathrm{Hom}_E(L, \bar{K}) \subseteq \mathrm{Hom}_K(L, \bar{K})$.

We will assume the following well-known lemma.

Lemma 1.1.12 (E. Artin)**.** *Let G be a finite group of automorphisms of a field L. Then $[L : L^G] \leq |G|$.*

See [40, 3.4, 3.5] for a proof.

Theorem 1.1.13. *Let L/K be a finite Galois extension. The map*

$$\begin{array}{ccc} \{H \text{ subgroup of } \mathrm{Gal}(L/K)\} & \to & \{K\text{-subalgebras of } L\} \\ H & \mapsto & L^H \end{array}$$

is a bijection. The inverse is given by $E \mapsto \mathrm{Gal}(L/E)$. Moreover E/K is Galois if and only if $\mathrm{Gal}(L/E)$ is a normal subgroup of $\mathrm{Gal}(L/K)$.

In this case the restriction map

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(E/K) \\ \sigma & \mapsto & \sigma|_E \end{array}$$

induces an isomorphism $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \simeq \mathrm{Gal}(E/K)$.

Proof. Let H be a subgroup of $G = \mathrm{Gal}(L/K)$. Notice that $\mathrm{Gal}(L/L^H) = H$ since L/L^H is Galois. Hence, the map $E/K \mapsto \mathrm{Gal}(L/E)$ is onto the set of subgroups of G. Let E a K-subalgebra of L and let $H = \mathrm{Gal}(L/E)$. Let us see that $E = L^H$. Notice that $E \subseteq L^H$, hence it is enough to prove that $[L : L^H] \leq [L : E]$ due to the product formula. This follos from Artin's lemma since $|\mathrm{Gal}(L/E)| \leq [L : E]$. Let $\sigma \in \mathrm{Gal}(L/K)$, let E/K be a subalgebra and let $E' = \sigma E$, then $\mathrm{Gal}(L/E') = \sigma \,\mathrm{Gal}(L/E)\sigma^{-1}$. The last statement follows. □

Thus, a finite Galois extension L/K is simple by Theorem 1.1.6 since $\mathrm{Gal}(L/K)$ has finitely many subgroups. It is worth noting that if L/K is finite separable extension, then there is a Galois finite extension L'/K containing L. It can be described as the compositum $L' := \prod_\theta \theta(L)$ where θ ranges over the set of embeddings $S = \mathrm{Hom}_K(L, \bar{K})$. Notice that L'/K is finite since S is so. Thus, finite separable extensions are also simple by 1.1.6.

1.1.4 Infinite Galois theory

The fundamental theorem of Galois theory admits a generalization to infinite Galois extensions. Let L/K be a Galois extension and let $\sigma \in \mathrm{Gal}(L/K)$. Then σ is determined by its restrictions $\{\sigma_E\}_E$ where E ranges over all finite Galois extensions E/K contained in L. Indeed, if $x \in L$ then $\sigma(x) = \sigma|_E(x)$ where $E \subseteq L$ is a finite Galois extension of K containing x. Hence, the lemma.

Lemma 1.1.14. *Let L/K be a Galois extension. The map*

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \to & \varprojlim_E \mathrm{Gal}(E/K) \\ \sigma & \mapsto & (\sigma|_E)_E \end{array}$$

is an isomorphism of groups. The projective limit is taken over the finite Galois extensions $E \subseteq L$ of K.

The isomorphism induces a structure of profinite topological group on $\mathrm{Gal}(L/K)$, the so-called Krull topology. Thus, $\mathrm{Gal}(L/K)$ is a Hausdorff, compact, totally disconnected topological group, [51, Proposition 0]. The set of groups $\{\mathrm{Gal}(L/E)\}_E$ is a basis of open neighborhoods of the identity.

The fundamental theorem fails to be true in the infinite case.

Example 1.1.15. *Let p be a prime and let $\mathbb{F}_p$ be the field of p elements. Let $\bar{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. The group $G = \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is the projective limit $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$ since every finite extension of a finite field is cyclic, thus $G \simeq \hat{\mathbb{Z}} \supsetneq \mathbb{Z}$. Let H be the group consisting in powers $Frob^n \in G$ of the Frobenius map $Frob_p : x \mapsto x^p$, $n \in \mathbb{Z}$. Then $\bar{\mathbb{F}}_p^H = \bar{\mathbb{F}}_p^G$.*

This an example of the following fact. Let L/K be a Galois extension, let H be a subgroup of $\mathrm{Gal}(L/K)$ and let $\bar{H}$ its topological closure. Then $\bar{H}$ is a subgroup of $\mathrm{Gal}(L/K)$ and $L^H = L^{\bar{H}}$.

Theorem 1.1.16. *Let L/K be a Galois extension. Let F be a K-subalgebra of L. Then $\mathrm{Gal}(L/F)$ is closed in $\mathrm{Gal}(L/K)$. Moreover, the map*

$$\begin{array}{ccc} \{H \text{ closed subgroup of } \mathrm{Gal}(L/K)\} & \to & \{K\text{-subalgebras of } L\} \\ H & \mapsto & L^H \end{array}$$

is a bijection. The inverse is given by $E \mapsto \mathrm{Gal}(L/E)$. Moreover E/K is Galois if and only if $\mathrm{Gal}(L/E)$ is normal subgroup of $\mathrm{Gal}(L/K)$. In this case the restriction map

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(E/K) \\ \sigma & \mapsto & \sigma|_E \end{array}$$

induces an isomorphism $\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \simeq \mathrm{Gal}(E/K)$ of topological groups.

See [59, Theorem 1.3.11] for a proof.

A further study of the profinite topology shows that a closed subgroup $\mathrm{Gal}(L/E)$ is open if and only if it is of finite index, if and only if E/K is finite.

1.1.5 Analysis and field theory

The methods described above allow us to build algebraic extensions via some quotient of the polynomial ring $K[X]$. Some analytical methods also provide a framework where one can consider extensions.

Lemma 1.1.17. *Let L/K be a field extension. The set*

$$A = \{x \in L : \ x \text{ is algebraic over } K \ \}$$

is a subfield of L containing K. In particular A/K is an algebraic extension. An automorphism $L \to L$ of K-algebras restricts to an automorphism $A \to A$ of K-algebras.

Proof. The field K is contained in A by definition. To see that A is closed under addition and product let $x, y \in A$. The rings $K[x+y]$, $K[xy]$ are K-submodules of $K[x][y]$ and by the product formula

$$[K[x][y] : K] = [K[x][y] : K[x]] \cdot [K[x] : K] < \infty$$

thus $K[x+y]$ and $K[xy]$ have finite rank over K. That is, A a K-subalgebra of L. If $x \in A \setminus \{0\}$, then A contains the field $K[x]$ and hence x^{-1}. Let $\sigma : L \to L$ be an automorphism of K-algebras. If $x \in A$ and $P \in K[X]$ so that $P(x) = 0$ then $P(\sigma(x)) = \sigma(P(x)) = 0$. Hence $\sigma(x) \in A$. The map $(\sigma^{-1})_{|A}$ is the inverse of $\sigma_{|A}$. □

Examples 1.1.18.

1. *An algebraic closure of $\mathbb{Q}$:*
   The fundamental theorem of algebra states that $\mathbb{C}$ is algebraically closed, that is $\bar{\mathbb{C}} = \mathbb{C}$. In particular, the set $\bar{\mathbb{Q}}$ of algebraic elements in $\mathbb{C}/\mathbb{Q}$ is an algebraic closure of $\mathbb{Q}$.

2. *The real part of $\bar{\mathbb{Q}}$:*
   The restriction map $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \to \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ induces a complex conjugation σ over $\bar{\mathbb{Q}}$. The field $\mathbb{A} := \bar{\mathbb{Q}}^{\sigma}$ is the field of algebraic elements in $\mathbb{R}/\mathbb{Q}$ and the previous map induces an isomorphism $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{A})$.

3. *The p-adic counterpart of the above example is considered in Theorem 1.2.4.*

4. *Let $K = \mathbb{Q}(X)$ denote the field of fractions of the polynomial ring $\mathbb{Q}[X]$. The completion L of K along (X) is the field of fractions of $\mathbb{Q}[[X]]$. The field $A = \{x \in L : x \text{ is algebraic over } K\}$ contains n^{th}-roots of $X+1$, the formal Taylor series of $\sqrt[n]{X+1}$ along 0. Hence A/K is an infinite algebraic extension.*

5. *When considering $K = \mathbb{Q}$ it is common to built roots of polynomials through analysis. For example the notation $\sqrt[3]{2}$ usually refers to the unique real $\theta \in \mathbb{R}$ satisfying $\theta^3 = 2$ and one writes $\mathbb{Q}(\sqrt[3]{2})$ to refer to the smallest field in $\mathbb{R}$ containing it. The roots of $X^3 - 2 = Irr(\theta, \mathbb{Q})$ in $\mathbb{C}$ are $\theta, \theta\zeta_3, \theta\zeta_3^2$ where $\zeta_3 = e^{2\pi i/3} = (-1 + i\sqrt{3})/2$. Hence $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois since $\zeta_3\theta \in \mathbb{C} \setminus \mathbb{R}$.*

   Similarly, one can use 5-adic analysis (Hensel Lemma) to prove that $X^3 - 2$ has a unique root in $\mathbb{Q}_5$ and that $\mathbb{Q}_5$ has no thirds roots of unity. Mainly, $X^3 - 2$ factors as $(X-3)(x^2-2x+4)$ in $\mathbb{F}_5[X]$. Again, this proves that $\mathbb{Q}[X]/(X^3-2)$ is not Galois over $\mathbb{Q}$.

1.2 Galois representations of $G_{\mathbb{Q}}$

The profinite structure of Galois groups with the classical inverse Galois problem in mind makes one wonder about examples of prototypical profinite groups. The topological group $\mathrm{GL}_n(\mathbb{Z}_\ell)$ is a profinite group. The product of profinite groups is also profinite. The Galois group $\mathrm{Gal}(\mathbb{Q}(\{\sqrt{p}\}_p)/\mathbb{Q})$ is isomorphic to the profinite group $\prod_p \mathbb{F}_2$ where p ranges over the set of prime numbers, just to give an example.

The problem of describing subgroups of $\mathrm{GL}_n(\mathbb{Z}_\ell)$ as Galois groups over $\mathbb{Q}$ has received great attention during the last half century. The realm of ℓ-adic Galois representations provides a natural framework for this problem.

A rank n *$\mathfrak{l}$-adic Galois representation* of a Galois group G is a continuous group homomorphism[4]

$$G \to \mathrm{GL}_n(\mathcal{O}_\mathfrak{l}),$$

[4]The continuous morphisms $G \to \mathrm{GL}_n(K_\mathfrak{l})$ are also known as $\mathfrak{l}$-adic representations.

here $\mathfrak{l}$ is a maximal ideal in the ring of integers of a number field K and $\mathcal{O}_{\mathfrak{l}}$ is the corresponding complete valuation ring attached to $\mathfrak{l}$.

A rank n *mod* $\mathfrak{l}$ *Galois representation* of a Galois group G is a continuous group homomorphism

$$G \to \mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}}/\mathfrak{l}).$$

The natural projection $\pi : \mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}}) \to \mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}}/\mathfrak{l})$ is a homomorphism of profinite groups. Let $\rho : G \to \mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}})$ be a Galois representation. The mod $\mathfrak{l}$ representation $\bar{\rho} = \pi \circ \rho$ is the *residual representation attached to* ρ.

Let us fix once and for all algebraic closures $\bar{\mathbb{Q}}$ and $\bar{\mathbb{Q}}_p$ of $\mathbb{Q}$ and $\mathbb{Q}_p$ respectively. We use $G_{\mathbb{Q}}$ to denote the absolute Galois group of $\mathbb{Q}$, that is

$$G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}).$$

Similarly, we use G_p to denote the absolute Galois group of $\mathbb{Q}_p$. In the present text we consider rank 2 Galois representations attached to $G_{\mathbb{Q}}$ and G_p. These groups are strongly related.

1.2.1 Decomposition group

Let $\bar{\mathbb{Z}}$ denote the integral closure of $\mathbb{Z}$ in $\bar{\mathbb{Q}}$.

Lemma 1.2.1. *The ring* $\bar{\mathbb{Z}}$ *is a domain with Krull dimension* 1. *Its maximal ideals have positive residue characteristic.*

Proof. The inclusion map $\mathbb{Z} \hookrightarrow \bar{\mathbb{Z}}$ induces an embedding $\mathbb{Z}/(m) \hookrightarrow \bar{\mathbb{Z}}/\mathfrak{p}$ where $(m) = \mathfrak{p} \cap \mathbb{Z}$ is a possibly zero prime ideal. Let $x \in \mathfrak{p} \setminus \{0\}$. The constant term n of $Irr(x, \mathbb{Q})$ is a non-zero integer, otherwise $X = Irr(x, \mathbb{Q})$ and $x = 0$. Hence $n \in \mathfrak{p} \cap \mathbb{Z}$ and m is non-zero, $p := m$. The domain $\bar{\mathbb{Z}}/\mathfrak{p}$ is a field since $\bar{\mathbb{Z}}/\mathfrak{p}$ is algebraic over $\mathbb{F}_p$. Thus, $\mathfrak{p}$ is maximal. □

For every maximal ideal $\mathfrak{p}$ of $\bar{\mathbb{Z}}$ the residue field $\mathbb{F}_{\mathfrak{p}} = \bar{\mathbb{Z}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$, where $p = \mathrm{char}\, \mathbb{F}_{\mathfrak{p}}$.

The map $G_{\mathbb{Q}} \times Spec(\bar{\mathbb{Z}}) \to Spec(\bar{\mathbb{Z}})$, $(\sigma, \mathfrak{p}) \mapsto \sigma(\mathfrak{p})$ defines an action of $G_{\mathbb{Q}}$ on the spectrum of $\bar{\mathbb{Z}}$. For a prime ideal $\mathfrak{p}$ the isotropy group

$$D_{\mathfrak{p}} = \{\sigma \in G_{\mathbb{Q}} : \sigma(\mathfrak{p}) = \mathfrak{p}\}$$

is known as the *decomposition group* of $\mathfrak{p}$.

Theorem 1.2.2. *Let p is a prime integer then $G_{\mathbb{Q}}$ acts transitively on $\{\mathfrak{p} : p \in \mathfrak{p}\}$.*

See [62, Appendix, Lemma]. The proof therein is a natural generalization of the finite Galois case L/K. Let $\mathfrak{p}$, $\mathfrak{p}'$ be two maximal ideals containing p and let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that $\sigma(\mathfrak{p}) = \mathfrak{p}'$. Then $D_{\mathfrak{p}} = \sigma^{-1} D_{\mathfrak{p}'} \sigma$ and they are isomorphic.

Lemma 1.2.3. *The group $D_{\mathfrak{p}}$ is closed in* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Proof. The following claim is clear and central: the ideal $\mathfrak{p}$ is the union of $\mathfrak{p}_L := \mathfrak{p} \cap \mathcal{O}_L$, where L ranges over the set of number fields and $\mathcal{O}_L$ denotes the ring of integers of L.

Now one can either prove that the complement S of $D_{\mathfrak{p}}$ is open by exhibiting a finite Galois extension $L_\sigma/\mathbb{Q}$ for every $\sigma \in S$ such that

$$\sigma \,\mathrm{Gal}(\bar{\mathbb{Q}}/L_\sigma) \cap D_{\mathfrak{p}} = \emptyset$$

or one can describe $D_{\mathfrak{p}}$ as an intersection of closed subgroups.

For the first assertion notice $\sigma(\mathfrak{p}) \neq \mathfrak{p}$ implies that $\sigma(\mathfrak{p}_{L_0}) \neq \mathfrak{p}_{L_0}$ for some L_0. Hence $\tau(\mathfrak{p}_{L_0}) = \mathfrak{p}_{L_0}$ for every $\tau \in \mathrm{Gal}(\bar{\mathbb{Q}}/L_0)$ and $\sigma \,\mathrm{Gal}(\bar{\mathbb{Q}}/L_0) \cap D_{\mathfrak{p}}$ is empty.

For the second assertion notice that $\sigma(\mathfrak{p}) = \mathfrak{p}$ if and only if $\sigma|_L(\mathfrak{p}_L) = \mathfrak{p}_L$ for every finite Galois extension $L/\mathbb{Q}$. The isotropy group $D_{\mathfrak{p}_L} \subseteq \mathrm{Gal}(L/\mathbb{Q})$ is closed and so is

$$D_{\mathfrak{p}} = \bigcap_L \pi_L^{-1}(D_{\mathfrak{p}_L})$$

where $\pi_L : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(L/\mathbb{Q})$ is the continuous projection given by restriction. □

Hence $D_{\mathfrak{p}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{A}_{\mathfrak{p}})$ for some extension $\bar{\mathbb{Q}}/\mathbb{A}_p/\mathbb{Q}$.

Theorem 1.2.4. *Let $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ be an embedding such that $\iota_p(\mathfrak{p})$ lies in the maximal ideal of $\bar{\mathbb{Q}}_p$. The restriction map*

$$\iota_p : \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$$

is continuous and has image in $D_{\mathfrak{p}}$. The map $G_p \to D_{\mathfrak{p}}$ is an isomorphism of profinite groups.

Proof. The elements in $\bar{\mathbb{Q}}_p$ are limit of sequences in $\bar{\mathbb{Q}}$ and the elements in G_p are continuous thus the injectivity. The ring $\bar{\mathbb{Z}}_p$ has a unique maximal ideal $\mathfrak{m}$. Thus Galois automorphisms σ in G_p preserve the maximal ideal and $\mathfrak{p} = \bar{\mathbb{Z}} \cap \mathfrak{m}$. Hence $\mathrm{Im}(\iota_p) \subseteq D_{\mathfrak{p}}$. A usual manner to see that $\mathrm{Im}(\iota_p) = D_{\mathfrak{p}}$ is dealing with the completion $\mathbb{C}_p$ of $\bar{\mathbb{Q}}_p$. Let us check that ι_p is continuous. It is enough to prove that $\iota^{-1}\,\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{A}_{\mathfrak{p}}(\theta))$ contains $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p(\theta))$ for every θ in $\bar{\mathbb{Q}}$. Since $\mathbb{Q} \subseteq \mathbb{A}_{\mathfrak{p}} = \bar{\mathbb{Q}} \cap \mathbb{Q}_p$ is dense in $\mathbb{Q}_p$ every automorphism in G_p acting trivially on $\mathbb{A}_{\mathfrak{p}}(\theta)$ also acts trivially on its completion $\mathbb{Q}_p(\theta)$.

□

The decomposition group $D_{\mathfrak{p}}$ has a natural action on $\mathbb{F}_{\mathfrak{p}}$. Indeed, an automorphism $\sigma : \bar{\mathbb{Z}} \to \bar{\mathbb{Z}}$ induces an isomorphism in residue fields $(\sigma \mod \mathfrak{p}) : \mathbb{F}_{\mathfrak{p}} \to \mathbb{F}_{\sigma(\mathfrak{p})}$.

The structure of $D_{\mathfrak{p}}$ is reduced to that of G_p. One deduces some useful properties.

Lemma 1.2.5. *The map*

$$\begin{array}{ccc} D_{\mathfrak{p}} & \longrightarrow & \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) \\ \sigma & \longmapsto & \sigma \mod \mathfrak{p} \end{array}$$

is a continuous group epimorphism.

Hence, the kernel of the previous map is a closed subgroup $I_{\mathfrak{p}}$ of $D_{\mathfrak{p}}$, the so-called *inertia group*. Again, if $\sigma \in G_{\mathbb{Q}}$ then $I_{\mathfrak{p}} = \sigma^1 I_{\sigma(\mathfrak{p})}\sigma$. We will denote the corresponding subgroup of G_p by I_p.

1.2.2 Conductor

In this paragraph we recall some properties of higher ramification groups and conductor. The standard reference is [49, Chapter IV]. See also the survey [61] by Douglas Ulmer.

The group G_p is filtered by the so-called higher ramification subgroups

$$G_p \supseteq G_p^s$$

$s \in [0, +\infty]$. It consists in a decreasing filtration of subgroups, that is $I_p^r \supseteq I_p^s$ if $r \leq s$. We take the convention that $G_p^{-1} = G_p$, and $G_p^0 = I_p$.

Let $\rho_{\mathfrak{l}} : G_p \to \mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}})$ be an $\mathfrak{l}$-adic Galois representation of G_p, with $p \neq \ell$. The *conductor* of $\rho_{\mathfrak{l}}$ is defined by

$$a(\rho_{\mathfrak{l}}) = \int_{-1}^{\infty} \operatorname{codim} V_{\ell}^{G^s},$$

where $V_{\mathfrak{l}}^{G^s}$ denotes the $K_{\mathfrak{l}}$-module $K_{\mathfrak{l}}^n$ whose action by G_p is given by $\mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}}) \subset \mathrm{GL}_n(K_{\mathfrak{l}})$. Notice that $\operatorname{codim} V_{\ell}^{G^s}$ is a decreasing function of s with values in $[0, n]$. The cases we will consider (modular representations) satisfy that $a(\rho_{\mathfrak{l}})$ is an integer. In this setting it is a useful technique to relate $a(\rho_{\mathfrak{l}})$ with usual Artin conductor of the residual representation $\bar{\rho}_{\mathfrak{l}}$, see [8] or [32].

The conductor $a(\rho_{\mathfrak{l}})$ is 0 if and only if I_p acts trivially. That is, if and only if $G_p \to GL_n(\mathcal{O}_{\mathfrak{l}})$ factors through $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. The group $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is topologically generated by the Frobenius map $\varphi_p : x \to x^p$. In this context, the characteristic polynomial of $\rho_{\mathfrak{l}}(\varphi)$ will play an important role.

Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}})$ be a Galois representations and let p be a prime number different from the residue characteristic of $\mathcal{O}_{\mathfrak{l}}$. The embedding $G_p \to G_{\mathbb{Q}}$ defines by restriction a continuous morphism

$$\rho|_{G_p} : G_p \to \mathrm{GL}_n(\mathcal{O}_{\mathfrak{l}}).$$

The *conductor exponent* of ρ at p is defined by $a(\rho|_{G_p})$. Notice that $a(\rho|_{G_p})$ does not depend on the choice of $\bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$. We will only deal with Galois representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_{\mathfrak{l}})$ ramified at finitely many prime numbers p. In those cases the prime-to-$\mathfrak{l}$ conductor of ρ will be a positive integer defined by

$$\mathrm{cond}(\rho) = \prod_{p \neq \ell} p^{a(\rho|_{G_p})}.$$

1.2.3 Example: Hecke eigenforms

Let N be a positive integer. The congruence subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ is the group of matrices whose mod N reduction is upper triangular. The space $S_2(N) := S_2(\Gamma_0(N))$ of weight 2, level N cusp forms is a finite $\mathbb{C}$-vector space consisting in holomorphic functions on the complex upper half plane vanishing at all cusps $\mathbb{P}_1(\mathbb{Q})$. See

[15, Definition 1.2.3] for a classical treatment of the topic and [41] for a geometrical one. Let us identify $S_2(N)$ with the subspace of $\mathbb{C}[[q]]$ given by the Fourier expansion at infinity

$$f = a_1 q + \sum_{n \geq 2} a_n q,$$

for $f \in S_2(N)$. The ring

$$\mathbb{T}_N = \mathbb{Z}[\ \{T_p\}_p]$$

of Hecke operators is a $\mathbb{Z}$-algebra generated by the so-called Hecke operators T_p, where p ranges over the set of prime numbers. The Hecke operator T_p acts linearly on $S_2(N)$ thus, $\mathbb{T}_N \otimes \mathbb{C}$ is a finite $\mathbb{C}$-vector subspace of $\mathrm{End}_{\mathbb{C}}(S_2(N))$. The Hecke algebra is a commutative ring with unit. A non-zero cusp form $f \in S_2(N)$ is a Hecke eigenform if it is an eigenvector for all Hecke operators T_p. Let $f = a_1 q + \sum_n a_n q^n$ a Hecke eigenform, then

$$a_1 = 0 \qquad \text{if and only if} \qquad f = 0.$$

An eigenform f is normalized if $a_1 = 1$. Let f be a normalized eigenform, notice that the restriction $\lambda_f : \mathbb{T}_N \otimes \mathbb{C} \to \mathrm{End}(f\mathbb{C}) = \mathbb{C}$ is a ring homomorphism. The map $f \mapsto \ker \lambda_f$ defines a bijection between the set of normalized Hecke eigenforms and the set of closed points of $\mathrm{Spec}\, \mathbb{T}_N \otimes \mathbb{C}$. The pth coefficient a_p of f is recovered from λ_f by the equation

$$\lambda_f(T_p) = a_p.$$

There is a hermitian scalar product on $S_2(N)$, the so-called Peterson scalar product, for which T_p is a Hermitian operator for every p coprime to N. By a classical result on Hermitian operators one deduces that T_p are semi-simple for every $p \nmid N$. Since $\mathbb{T}_N$ is commutative there is a basis $\mathcal{B} = \{f\}$ of cusp forms that are eigenforms of T_p for every $p \nmid N$. The existence of a basis of Hecke eigenforms (for all Hecke operators) is more subtle. The theory of newforms gives an answer to this problem, see [15, 5.8.3].

Let f be a normalized Hecke eigenform in $S_2(N)$. The field $\mathbb{Q}_f$ generated by the Fourier coefficients of f is a number field. Let $\mathfrak{l}$ a maximal ideal of residue characteristic ℓ in the ring of integers $\mathcal{O}$ of

$\mathbb{Q}_f$ and let $\mathcal{O}_\mathfrak{l}$ be the completion of $\mathcal{O}$ with respect to $\mathfrak{l}$. There is a Galois representation

$$\rho_{f,\mathfrak{l}} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathcal{O}_\mathfrak{l})$$

such that

- $\det \rho_{f,\mathfrak{l}}$ is the cyclotomic character,
- $\rho_{f,\mathfrak{l}}$ is unramified at every $p \nmid N\ell$ and
- the characteristic polynomial of $\rho_{f,\mathfrak{l}}(Frob_p)$ is $X^2 - a_p X + p$ for every $p \nmid N\ell$.

Remark 1.2.6. *If we assume that f is a newform (see section 3.2 for the definition) then the largest prime-to-ℓ divisor of N equals the conductor* $\mathrm{cond}(\rho_{f,\mathfrak{l}})$.

The construction of $\rho_{f,\mathfrak{p}}$ is due to Eichler-Shimura and Deligne. See [12, §3.1] for further details of $\rho_{f,\mathfrak{l}}$. See also [15, 5.8.4].

1.3 Elliptic curves

In this section we present some well-known statements on elliptic curves. Some background on algebraic geometry might be useful to the reader. The canonical introductory reference is Silverman's book [53].

An *elliptic curve* over K is a pair $(E, \mathcal{O}_E)$, where E is a genus one smooth projective algebraic curve over K and $\mathcal{O}_E$ is a K-rational point of E. By a *morphism* of elliptic curves $(E, \mathcal{O}_E) \to (E', \mathcal{O}_{E'})$ we mean a morphism $\phi : E \to E'$ of algebraic varieties over K such that $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$. This defines the category of elliptic curves over K.

Riemann-Roch Theorem is quite powerful in this setting. For instance, one has Proposition 3.1 in [53] that states that every elliptic curve E is plane. More precisely, E is isomorphic over K to a plane curve given by a *Weierstrass equation*

$$ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with $a_i \in K$ such that $\mathcal{O}_E$ maps to $[0 : 1 : 0]$. Reciprocally, a plane curve E given by a Weierstrass equation with coefficients in K defines

an elliptic curve $(E, [0:1:0])$ over K if and only if it is non-singular. The following consequence of Riemann-Roch describes isomorphisms between elliptic curves in Weierstrass form.

Proposition 1.3.1. *Any two Weierstrass equations for an elliptic curve $(E, \mathcal{O}_E)$ are related by a linear change of variables of the form*

$$\begin{aligned} X &= u^2X' + rZ' \\ Y &= u^3Y' + su^2X' + tZ' \\ Z &= Z' \end{aligned}$$

with $u, r, s, t \in K$, $u \neq 0$.

Proof. See [53, Chapter 3, Proposition 3.1]. □

1.3.1 The group law

Let $(W, \mathcal{O} = [0:1:0])$ be an elliptic curve over K in Weierstrass form and let $\bar{K}/K$ be an algebraic closure. A line ℓ in $\mathbb{P}_2/\bar{K}$ defines a multiset $\{P, Q, R\}$ of points in $W(\bar{K})$ corresponding to the intersection $\ell \cap W$ with intersection multiplicity. This follows from Bézout's Theorem, see [25, I.7.8].

Theorem 1.3.2. *There is a unique group structure $+$ on $W(\bar{K})$ such that $\mathcal{O} = [0:1:0]$ is the unit element and*

$$P + Q + R = \mathcal{O}$$

for every line ℓ, where $\{P, Q, R\}$ is the multiset attached to $\ell \cap W$. In particular $(W(\bar{K}), +)$ is abelian.

See [53, Proposition 2.2] for a proof. Let $(W_1, [0:1:0])$, $(W_2, [0:1:0])$ be elliptic curves in Weierstrass form and assume that they are isomorphic $W_1 \overset{\phi}{\simeq} W_2$ as elliptic curves. Then the bijection $W_1(\bar{K}) \overset{\phi}{\simeq} W_2(\bar{K})$ is an isomorphism of abelian groups. This follows from Proposition 1.3.1 since the linear isomorphism

$$\begin{aligned} X &= u^2X' + rZ' \\ Y &= u^3Y' + su^2X' + tZ' \\ Z &= Z'. \end{aligned}$$

extends to a linear automorphism of $\mathbb{P}_2$. In particular a line in $\mathbb{P}_2$ maps to a line in $\mathbb{P}_2$ Hence, $P+Q+R=\mathcal{O}_1$ if and only if $\phi(P)+\phi(Q)+\phi(R)=\mathcal{O}_2$.

The Galois group $\mathrm{Gal}(\bar{K}/K)$ acts on $E(\bar{K})$ linearly. That is

Theorem 1.3.3. *Let $P,Q\in E(\bar{K})$ and $\sigma\in\mathrm{Gal}(\bar{K}/K)$. Then*

$$\sigma(P+Q)=\sigma(P)+\sigma(Q).$$

In particular $E(L)=\{P\in E(\bar{K}):\mathrm{Gal}(\bar{K}/L)P=P\}=E(\bar{K})^{\mathrm{Gal}(\bar{K}/L)}$ is a subgroup of $E(\bar{K})$.

1.3.2 Tate module

Let $m\geq 1$ be an integer. We use $E(\bar{K})[m]$ to denote the m-torsion of $E(\bar{K})$, i.e. the kernel of $[m]:E(\bar{K})\to E(\bar{K})$ $P\mapsto mP$. Notice that $E(\bar{K})[m]$ is stable under the action of $\mathrm{Gal}(\bar{K}/K)$. Indeed $m\sigma(P)=\sigma(mP)=\sigma(\mathcal{O})=\mathcal{O}$ for every $\sigma\in\mathrm{Gal}(\bar{K}/K)$, $P\in E(\bar{K})$.

Example 1.3.4. *Consider the plane Weierstrass curve*

$$E: Y^2Z=X^3+a_2X^2Z+a_4XZ^2+a_6Z^3 \qquad a_2,a_4,a_6\in\mathbb{Q},$$

over $\mathbb{Q}$ and let $\gamma_1,\gamma_2,\gamma_3$ be the roots of $P(X)=X^3+a_2X^2+a_4X+a_6$ in $\bar{\mathbb{Q}}$ with multiplicities. Then $(E,[0:1:0])$ is an elliptic curve if, and only if, E is non-singular if, and only if, $\gamma_1,\gamma_2,\gamma_3$ are pairwise different. If that is the case then

$$E(\bar{\mathbb{Q}})[2]=\{[\gamma_i:0:1]\}_i\cup\{[0:1:0]\}.$$

Theorem 1.3.5. *Let K be a field of characteristic 0 and let $\bar{K}$ be an algebraic closure of K. Then the m-torsion $E(\bar{K})[m]$ of $(E(\bar{K}),+)$ is a free $\mathbb{Z}/m\mathbb{Z}$-module of rank 2.*

Let K be a characteristic 0 field, $\bar{K}$ an algebraic closure of K and let E an elliptic curve over K. This induces the so-called *mod m Galois representation attached to E*

$$\bar{\rho}_m:\mathrm{Gal}(\bar{K}/K)\to Aut(E(\bar{K})[m])\simeq \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

which is a continuous Galois representation.

Let ℓ be prime. The set

$$\{E(\bar{K})[\ell^n]\}_{n\geq 1}$$

together with morphisms $\varphi_{n+1} : E(\bar{K})[\ell^{n+1}] \to E(\bar{K})[\ell^n]$, $P \mapsto \ell P$ defines a projective system. The ℓ-adic Tate module $\mathcal{T}_\ell E$ of E,

$$\mathcal{T}_\ell E = \varprojlim_n E(\bar{K})[\ell^n]$$

is a free $\mathbb{Z}_\ell$-module of rank 2.

Proposition 1.3.6. *The map*

$$\begin{array}{rccc} \rho_{E,\ell} : & \mathrm{Gal}(\bar{K}/K) & \longrightarrow & \mathrm{Aut}_{\mathbb{Z}_\ell}(\mathcal{T}_\ell E) \\ & \sigma & \longmapsto & \sigma : (P_n)_n \mapsto (\sigma(P_n))_n \end{array}$$

is a Galois representation. A choice of a $\mathbb{Z}_\ell$-basis in $\mathcal{T}_\ell E$ induces a continuous Galois representation

$$\rho_{E,\ell} : \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Proof. The group $\mathrm{Gal}(\bar{K}/K)$ acts on $\mathcal{T}_\ell E$ componentwise. Indeed,

$$\sigma((P_n)_n) := (\sigma(P_n))_n \in \mathcal{T}_\ell E$$

since $\varphi_n(\sigma(P_n)) = \ell\sigma(P_n) = \sigma(\ell P_n) = \sigma(P_{n-1})$. □

Let $K = \mathbb{Q}$. The local representations $\rho_{E,\ell}|_{G_p}$ are quite well understood.

Theorem 1.3.7 (Nerón-Ogg-Shafarevich criterion)**.** *Let $\rho_{E,\ell}$ be the ℓ-adic Galois representation attached to E and let p be a prime $p \neq \ell$. Then $\rho_{E,\ell}$ is ramified at p if and only if p is a prime of bad reduction of E.*

See [53, Ch. VII Theorem 7.1]. As a consequence, $\rho_{E,\ell}$ is ramified at finitely many primes.

Theorem 1.3.8. *Let $p \neq \ell$ be a prime of good reduction of E and let $E(\mathbb{F}_p)$ be the group of $\mathbb{F}_p$-points of (a minimal model over $\mathbb{Z}_p$ of) E. Let φ_p denote the Frobenius map $x \to x^p$ in $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$. Then $\rho_{E,\ell}(\varphi_p)$ has characteristic polynomial*

$$X^2 - a_p X + p,$$

where $a_p = p + 1 - \#E(\mathbb{F}_p)$.

See Ch. V of Silverman's book [53]. Appendix C.16 loc. cit., and [54, Ch. IV §10].

Theorem 1.3.9. *Let p be prime $p \neq \ell$. The conductor exponent of $\rho_{E,\ell}|_{G_p}$ is an integer ≤ 8 and is ≤ 2 if $p \neq 2, 3$.*

See Appendix C.16 loc. cit. and [54, Ch. IV §10].

1.3.3 Full two-torsion elliptic curves

In this section we consider Frey-Hellegouarch curves over $\mathbb{Q}$. That is, elliptic curves over $\mathbb{Q}$ with full rational 2-torsion. Notice that those are the curves with trivial mod 2 Galois representation.

Lemma 1.3.10. *Let (A, B, C) be a tern in $\mathbb{Q}^3$ such that $A+B+C = 0$. The Weierstrass equation*

$$E_{(A,B,C)} : Y^2Z = X(X - AZ)(X + BZ)$$

defines an elliptic curve if and only if $ABC \neq 0$.

Proof. The curve $E_{(A,B,C)} : Y^2Z = X(X-AZ)(X+BZ)$ is an elliptic curve if and only if E is non-singular, if and only if $X(X-A)(X+B)$ has no double roots. □

The elliptic curve $E_{(A,B,C)}$, is known as the *Frey Curve* attached to (A, B, C). Let $V = \{(A, B, C) \in \mathbb{Q}^3 : A + B + C = 0\}$. The group $G := \mathbb{Q}^\times \times \mathfrak{S}_3$ acts on V by

$$(\lambda, \sigma)(x_1, x_2, x_3) := (\lambda x_{\sigma(1)}, \lambda x_{\sigma(2)}, \lambda x_{\sigma(3)}).$$

The set of terns satisfying $ABC = 0$ is stable under this action.

Proposition 1.3.11. *Let τ be a transposition in $\mathfrak{S}_3$. The action of G on V induces an action of $G/\langle G^2, (-1, \tau)\rangle \simeq \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ on the set of Frey Curves modulo $\mathbb{Q}$-isomorphism.*

Proof. Notice that

$$\begin{array}{ccc} E_{(A,B,C)} & \longrightarrow & E_{(B,C,A)} \\ (X, Y, Z) & \longmapsto & (X + BZ, Y, Z) \end{array}$$

defines an isomorphism of elliptic curves. Thus the group $\mathfrak{A}_3 = \mathfrak{S}_3^2$ of even permutations acts trivially on the set of isomorphism classes of Frey elliptic curves. Notice that

$$E_{(-1,Id)(A,B,C)} = E_{(B,A,C)}.$$

For every $\sigma \in \mathfrak{S}_3$ let $s(\sigma) \in \{\pm 1\}$ denote the sign of σ, one deduces from previous equation that

$$E_{(1,\sigma)(A,B,C)} \simeq E_{(s(\sigma),Id)(A,B,C)}.$$

Let $g \in \mathbb{Q}^\times$, the map

$$\begin{array}{ccc} E_{(A,B,C)} & \longrightarrow & E_{g^2(A,B,C)} \\ (X,Y,Z) & \longmapsto & (g^2X, g^3Y, Z) \end{array}$$

defines an isomorphism of elliptic curves. Thus, $\langle G^2, (-1,\tau)\rangle$ acts trivially on the set of isomorphism classes of Frey curves. □

Let ℓ be a prime and $g \in \mathbb{Q}^\times \setminus (\mathbb{Q}^\times)^2$. The curves $E_{(A,B,C)}$, $E_{g(A,B,C)}$ are generally non-isomorphic over $\mathbb{Q}$.[5] Nevertheless, $E_1 = E_{(A,B,C)}$, $E_2 = E_{g(A,B,C)}$ are isomorphic over $K = \mathbb{Q}(\sqrt{g})$. Thus $E_1(\bar{\mathbb{Q}})$ and $E_2(\bar{\mathbb{Q}})$ are isomorphic as $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$-modules. It turns out that $E_2(\bar{\mathbb{Q}})$ is a *twist* of $E_1(\bar{\mathbb{Q}})$ as $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules.

Proposition 1.3.12. *Let $P = (x,y) \in E_1(\bar{\mathbb{Q}})$, let*

$$\chi : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q}) = \{\pm 1\}.$$

be the quadratic character attached to $K = \mathbb{Q}(\sqrt{g})$ and consider the isomorphism

$$\begin{array}{rccc} \theta : & E_1 & \longrightarrow & E_2 \\ & (X,Y,Z) & \longmapsto & (gX, g\sqrt{g}Y, Z) \end{array}$$

of elliptic curves over K. Then

$$\theta(\sigma(P)) = [\chi(\sigma)]\sigma(\theta(P)),$$

for every $\sigma \in G_{\mathbb{Q}}$.

[5] The equality $E_{(1,1-2)} = E_{(-1,-1,2)}$ is an exception.

Proof. The inverse morphism $[-1] : E_2 \to E_2$, $P \mapsto -P$, is defined by $[x : y : z] \mapsto [x : -y : z]$. If $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/K)$, i.e. $\sigma(\sqrt{g}) = \sqrt{g}$, then $[\chi(\sigma)] = [1] = Id$ and $\sigma(\theta(P)) = \theta(\sigma(P))$. If $\sigma(\sqrt{g}) = -\sqrt{g}$ and $P = [x : y : z] \in E_1(\bar{\mathbb{Q}})$ then

$$\begin{aligned}[-1]\sigma(\theta(P)) &= [-1]\ [\sigma(gx) : \sigma(g\sqrt{g}y) : \sigma(z)] \\ &= [-1]\ [g\sigma(x) : -g\sqrt{g}\sigma(y) : \sigma(z)] \\ &= \theta(\sigma(P)).\end{aligned}$$

□

Corollary 1.3.13. *Let E_1, E_2 be elliptic curves as above, let χ be the quadratic character attached to $K = \mathbb{Q}(\sqrt{g})$, g square-free and let ℓ be prime. Then $T_\ell E_2$ and $T_\ell E_1 \otimes \chi$ are isomorphic as $\mathbb{Z}_\ell[\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})]$-modules.*

Thus, a tern $[A : B : C]$ in the projective line $A + B + C = 0$ defines a unique Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathbb{Z}})$ up to twist by a quadratic character.

Let $\rho_{E,\ell}$ be the ℓ-adic Galois representation attached to E and let $\rho_{E,\ell} \otimes \chi$ be a twist as described above. If $\rho_{E,\ell}$ has conductor exponent ≤ 1 at $p \mid g$, $p \neq \ell, 2$ then $\rho_{E,\ell} \otimes \chi$ has conductor exponent 2. See for example Proposition 1 in [61]. The cases of conductor exponent ≥ 2 or $p = 2$ are more subtle.

1.4 Prime divisors of $\Phi_n(\ell)$

In this section we give some lower bounds to the number ω of prime divisors of $\ell^n \pm 1$ for an integer $\ell \geq 3$.

Let Φ_n be the nth cyclotomic polynomial. A usual description of Φ_n is given by the formula

$$\Phi_n(X) = \prod_k (X - \zeta_n^k)$$

where $\zeta_n = e^{2\pi i/n}$ is a primitive nth root of unity and k ranges over the units of $\mathbb{Z}/n\mathbb{Z}$. Gauss proved that Φ_n is irreducible in $\mathbb{Z}[X]$, hence $\mathbb{Z}[X]/\Phi_n \simeq \mathbb{Z}[\zeta_n] \subseteq \mathbb{C}$ is a domain. In particular

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X)$$

is the factorization of $X^n - 1$ in irreducible factors over $\mathbb{Z}[X]$.

Let k be a positive integer. The map $\mathbb{Z}[X] \to \mathbb{Z}/k\mathbb{Z}$, $X \mapsto \ell$ factors through $\mathbb{Z}[\zeta_n] \to \mathbb{Z}/k\mathbb{Z}$, $\zeta_n \mapsto \ell$ if, and only if, $k \mid \Phi_n(\ell)$.

Lemma 1.4.1. *Let $p \nmid n$ be a prime and assume that there is a ring homomorphism $\theta : \mathbb{Z}[\zeta_n] \to \mathbb{F}_p$. Then $\theta(\zeta_n)$ has order n in $\mathbb{F}_p^\times$ and $n \mid p - 1$.*

Proof. Let $\alpha = \theta(\zeta_n)$. Then $\alpha^n - 1 = \prod_d \Phi_d(\alpha) = 0$. Notice that $X^n - 1$ is separable over $\mathbb{F}_p$ since $nX^{n-1} \neq 0$ in $\mathbb{F}_p[X]$. Hence α has order n in $\mathbb{F}_p^\times$ and the lemma follows. □

Lemma 1.4.2. *Let p be an odd prime. There is no ring homomorphism $\mathbb{Z}[\zeta_p] \to \mathbb{Z}/p^2\mathbb{Z}$. There is no ring homomorphism $\mathbb{Z}[\zeta_4] \to \mathbb{Z}/4\mathbb{Z}$.*

Proof. It is enough to prove that $\Phi_p(X) = \sum_{i=0}^{p-1} X^i$ has no roots in $\mathbb{Z}/p^2\mathbb{Z}$. The following proof is standard. Assume that there is a root a of Φ_p in $\mathbb{Z}/p^2\mathbb{Z}$. Then $a = 1 \pmod p$, since $\Phi_p = (X-1)^{p-1}$ in $\mathbb{F}_p$. Notice that $\Phi_p(1 + pb) = \sum_{i=0}^{p-1} 1 + ipb = p$ in $\mathbb{Z}/p^2\mathbb{Z}$ for every b. Hence $\Phi_p(a) = p$ for every $a \equiv 1 \pmod p$.

Notice that $\Phi_4(X) = X^2 + 1$ has no roots in $\mathbb{Z}/4\mathbb{Z}$. □

Lemma 1.4.3. *Let $\ell \geq 3$, $n \geq 2$ be integers and let p be the largest prime divisor of n, then $|\Phi_n(\ell)| > p$.*

Proof. The Euler's totient function φ, satisfies that

$$p - 1 \mid \varphi(n)$$

if $p \mid n$. Hence

$$|\Phi_n(\ell)| = \prod_k |\ell - \zeta_n^k| \geq \prod_k 2 \geq 2^{p-1}$$

and case $p \geq 3$ follows.

If $p = 2$ then n is a power of 2, $n = 2^m$, and

$$\Phi_n(\ell) = \ell^{2^{m-1}} + 1 > 2.$$

□

The polynomial Φ_n has no real roots for $n \geq 3$, hence $|\Phi_n(\ell)| = \Phi_n(\ell)$.

Lemma 1.4.4. *Let $\ell \geq 3, n \geq 3$ integers. There is a prime divisor of $\Phi_n(\ell)$ not dividing $2n$.*

Proof. Case $n = 2^m \geq 4$.
One has that $\Phi_{2^m}(X) = X^{2^{m-1}} + 1$ and $\Phi_n(\ell) \geq 10$. If $4 \nmid \Phi_n(\ell)$ then $\mathbb{Z}[\zeta_n] \to \mathbb{Z}/4\mathbb{Z}$, $\zeta_n \mapsto \ell$ defines a ring homomorphism that restricts to $\mathbb{Z}[\zeta_4] \subseteq \mathbb{Z}[\zeta_n]$. This contradicts Lemma 1.4.2. Hence either $\Phi_n(\ell)$ is odd or $\Phi_n(\ell)/2 \geq 5$ is odd.

Case $p \mid n$, p odd.
Notice that $\Phi_n(\ell)$ is odd. Indeed, a ring homomorphism

$$\mathbb{Z}[\zeta_n] \to \mathbb{F}_2$$

induces by restriction a map

$$\mathbb{Z}[\zeta_p] \to \mathbb{F}_2$$

hence $p \mid 2 - 1$.

Let us see that either $\Phi_n(\ell)$ and n are coprime or there is a prime p such that $\Phi_n(\ell)/p, n$ are coprime. Assume that $p < q$ are prime divisors of $\Phi_n(\ell)$ and n. Then there is a ring homomorphism

$$\mathbb{Z}[\zeta_q] \subseteq \mathbb{Z}[\zeta_n] \to \mathbb{F}_p$$

and $q \mid p - 1$ which contradicts $p < q$. Hence the greatest common divisor of $\Phi_n(\ell)$ and n is a possibly trivial power of an odd prime p. If $p \mid n$ then $p^2 \nmid \Phi_n(\ell)$ by Lemma 1.4.2. Hence either $\Phi_\ell(n), 2n$ are coprime or there is an odd prime divisor p of $\Phi_n(\ell)$ such that $\Phi_n(\ell)/p$ and $2n$ are coprime. In the second case $\Phi_n(\ell)/p > 1$ is an odd integer and the lemma follows. □

Theorem 1.4.5. *Let $\ell \geq 3$. Assume that $n_1, \ldots, n_r$ are pairwise different integers ≥ 3. Then*

$$\prod_i \Phi_{n_i}(\ell)$$

has at least r odd prime divisors.

Proof. Let p_i be a prime divisor of $\Phi_{n_i}(\ell)$ coprime to $2n_i$ as in Lemma 1.4.4. Then ℓ has order n_i in $\mathbb{F}_{p_i}^{\times}$. Hence $p_i \neq p_j$. □

For an integer k let $\omega(k)$ denote the number of prime divisors of k and let $\sigma(k)$ denote the number of divisors of k.

Corollary 1.4.6. *Let $\ell \geq 3$, $n \geq 1$ be integers. If $(\ell, n) \neq (3, even)$ then*

$$\omega(\ell^n - 1) \geq \sigma(n).$$

Otherwise

$$\omega(3^{2t} - 1) \geq \sigma(2t) - 1.$$

Proof. Let $i \in \{1, 2\}$ such that $n \equiv i \pmod 2$. Then

$$A := \prod_{\substack{d \mid n \\ d \geq 3}} \Phi_d(\ell) = \frac{\ell^n - 1}{\ell^i - 1}$$

has at least $\sigma(n) - i$ odd prime divisors $S = \{p_d\}_{d|n, d\geq 3}$. Notice that $p_d \nmid \ell^i - 1$ for every $p_d \in S$. Indeed, if an odd prime p divides $\ell^i - 1$ then ℓ has order $\leq i$ in $\mathbb{F}_p^{\times}$, hence $p \notin S$. Thus

$$\omega(\ell^n - 1) \geq \sigma(n) - i + \omega(\ell^i - 1).$$

It is enough to prove that $\omega(\ell^i - 1) \geq i$ if and only if $(\ell, i) \neq (3, 2)$. If $i = 1$ then $\ell - 1 \geq 2$ and $\omega(\ell - 1) \geq 1$. If $i = 2$ then $gcd(\ell - 1, \ell + 1) \leq 2$. Assume $\omega(\ell^2 - 1) < 2$ then $\ell - 1, \ell + 1$ are powers of two. Hence $\ell = 3$. □

Corollary 1.4.7. *Let $\ell \geq 3$, $n \geq 1$ be integers and let n_2 be the largest odd divisor of n. Then*

$$\omega(\ell^n + 1) \geq \sigma(n_2).$$

Proof. Let $n = 2^m n_2$ then $\ell^n + 1 = \prod_{d|n_2} \Phi_{2^{m+1}d}(\ell)$. For every d such that $2^{m+1}d \neq 2$ consider a prime $p_d \mid \Phi_{2^{m+1}d}(\ell)$ as in Theorem 1.4.5. If $m = 0$ let p_1 be an arbitrary prime divisor of $\Phi_2(\ell) = \ell + 1$. Then $\prod_{d|n_2} p_d$ is a squarefree divisor of $\ell^n + 1$. □

1.4.1 Catalan Conjecture

One deduces a case of Catalan's Conjecture.

Theorem 1.4.8 (Partial Catalan's Conjecture)**.** *Let $\ell \geq 3$ be an integer and assume that*

$$2^m - \ell^n \in \{\pm 1\}$$

for some integers $m, n \geq 2$. Then $m = \ell = 3$, $n = 2$.

Proof. Assume that $2^m = \ell^n + 1$, $n \geq 2$ and let n_2 be the largest odd divisor of n. Then ℓ is odd and $\ell^n + 1 \geq 4$. By Corollary 1.4.7 we have that $1 = \omega(\ell^n + 1) \geq \sigma(n_2)$, hence $n_2 = 1$ and $n = 2^r$ for some positive m. Since $2^m = \ell^{2^r} + 1 \equiv 2 \pmod 4$ one has that $m = 1$ and $2 = \ell^{2^m} + 1$.

Assume that $2^m = \ell^n - 1$, $n \geq 2$. If $(\ell, n) = (3, even)$ then $1 = \omega(3^{2t} - 1) \geq \sigma(2t) - 1$. Hence $t = 1$.

If $(\ell, n) \neq (3, even)$, by Corollary 1.4.6 one has that $1 = \omega(\ell^n - 1) \geq \sigma(n)$. Hence $n = 1$. □

This partial result is well known to experts. See [44] for a complete treatment of Catalan's conjecture written before Preda Mihăilescu's proof [39].

Chapter 2

Change of sign at a Steinberg prime

In this chapter we present original work developed in [17] in joint work with Luis Dieulefait. We would like to thank K. Ribet for providing so much valuable feedback. We would like to thank X. Guitart and S. Anni for many stimulating conversations and N. Billerey for helpful comments.

Let f be a cusp Hecke eigenform of weight 2, level N and trivial nebentypus. We attach to f a sequence $\{a_n\}_{n\geq 1}$ of complex numbers consisting of the Fourier coefficients of f at infinity. We say that f is normalized if $a_1 = 1$. In this case $K_f = \mathbb{Q}(\{a_n\}_n) \subset \bar{\mathbb{Q}}$ and it is a number field. Let f, f' be normalized eigenforms of common weight 2, level N and N' respectively and trivial nebentypus. Consider the composite field $L = K_f \cdot K_{f'}$ in $\bar{\mathbb{Q}}$ and let $\mathfrak{l}$ be a prime of L, $\ell\mathbb{Z} = \mathfrak{l}\cap\mathbb{Z}$. We will be interested in pairs of newforms f and f' for which

$$a_n \equiv a'_n \pmod{\mathfrak{l}} \qquad \text{for every } n \text{ coprime to } \ell NN'. \tag{2.0.1}$$

The Fourier coefficients of a newform are completely determined by the a_p coefficients of prime subindex. It is easy to see then that (2.0.1) is equivalent to

$$a_p \equiv a'_p \pmod{\mathfrak{l}} \qquad \text{for every prime } p \nmid \ell NN'. \tag{2.0.2}$$

Let $\lambda = \mathfrak{l} \cap \mathcal{O}_{K_f}$ and $\lambda' = \mathfrak{l} \cap \mathcal{O}_{K'_f}$ and assume that the residual Galois representations $\bar{\rho}_{f,\lambda}$, $\bar{\rho}_{f',\lambda'}$ attached to f and f' are irreducible.

Then f, f' satisfy (2.0.1) if and only if $\bar{\rho}_{f,\lambda}$ and $\bar{\rho}_{f',\lambda'}$ are isomorphic. In general, it is not an easy problem to find for a given newform f another eigenform f' satisfying (2.0.1), neither proving the existence of such an eigenform f'. Ribet's level raising [45] and level lowering [46] theorems are very powerful in this context. In this chapter we will consider a newform f of weight 2 on $\Gamma_0(N)$ together with a prime $\lambda \nmid 2N$ of K_f and will give necessary and sufficient conditions for the existence of another eigenform f' of weight 2 on $\Gamma_0(N)$ and a prime λ' of $K_{f'}$ such that

- $\bar{\rho}_{f,\lambda}$ and $\bar{\rho}_{f',\lambda'}$ are isomorphic and
- $a_p = -a'_p$ for a prime p dividing N once and f' is p-new.

See [45] (Ribet 1990) for a definition of p-new and Theorem 2.3.4 for a precise statement of our result.

2.1 Galois representations attached to a Hecke eigenforms

From now on let us fix an odd prime ℓ and an immersion $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. In particular, for every number field K we have fixed a prime λ over ℓ and a completion $K_\ell \subset \overline{\mathbb{Q}}_\ell$ of K with respect to λ. Let $\overline{\mathbb{F}}_\ell$ denote the residue field of the ring of integers of $\overline{\mathbb{Q}}_\ell$, which is indeed an algebraic closure of $\mathbb{F}_\ell$. Let f be a normalized eigenform on $\Gamma_0(N)$ with q-expansion at infinity $f(z) = q + \sum_{n\geq 2} a_n q^n$. As in the introduction, K_f denotes the number field $\mathbb{Q}(\{a_n\}_n)$ of coefficients of f and by $\mathcal{O}_f$ its ring of integers. Consider the ℓ-adic Galois representation attached to f by Deligne

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow GL_2(K_{f,\ell})$$

where $K_{f,\ell}$ denotes the completion of K_f with respect to (the fixed prime λ above) ℓ and $\mathcal{O}_{f,\ell}$ denotes its ring of integers. Since $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ is compact one can (non-canonically) embed its image in $GL_2(\mathcal{O}_{f,\ell})$,

$$\iota : \mathrm{Im}\, \rho_{f,\ell} \longrightarrow GL_2(\mathcal{O}_{f,\ell}).$$

Recall that $\mathcal{O}_{f,\ell}$ is a local ring whose residue field $\mathcal{O}_{f,\ell}/\mathfrak{m}_{f,\ell}$ is a finite extension of $\mathbb{F}_\ell$ contained in $\overline{\mathbb{F}}_\ell$. Reducing $\iota \circ \rho_{f,\ell}$ mod $\mathfrak{m}_{f,\ell}$, we obtain

the mod ℓ Galois representation

$$\bar{\rho}_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow GL_2(\mathcal{O}_{f,\ell}/\mathfrak{m}_{f,\ell}) \hookrightarrow GL_2(\overline{\mathbb{F}}_\ell)$$

attached to f (independent of ι up to semi-simplification), satisfying

$$\mathrm{tr}\, \bar{\rho}_{f,\ell}(Frob_p) \equiv a_p \qquad \det \bar{\rho}_{f,\ell}(Frob_p) \equiv p \pmod{\mathfrak{m}_{f,\ell}}$$

for every rational prime $p \nmid \ell N$.

2.2 Lowering and raising the levels

We state here Ribet's theorems, they will be the main tools needed in the proof of our theorem. See [46] and [45] (theorem 1 and remarks in section 3) for the proofs.

Theorem 2.2.1 (Ribet's level lowering theorem)**.** *Let f be a newform of weight 2 on $\Gamma_0(N)$, let p be a prime dividing N once. Assume that $\ell \nmid 2p$ and that the mod ℓ Galois representation*

$$\bar{\rho}_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow GL_2(\overline{\mathbb{F}}_\ell)$$

is irreducible and unramified at p. If one or both of the following conditions hold

1. *$\ell \nmid N$,*
2. *$\bar{\rho}_{f,\ell}|_{G_{\mathbb{Q}(\zeta_\ell)}}$ is irreducible,*

then there exists a newform f' of weight 2 on $\Gamma_0(M)$ for some M divisor of N/p such that $\bar{\rho}_{f',\ell}$ is isomorphic to $\bar{\rho}_{f,\ell}$.

Proof. By theorem 1.1 of [46] we may assume that $\bar{\rho}_{f,\ell}|_{G_{\mathbb{Q}(\zeta_\ell)}}$ is irreducible. We first prove the existence of a representation $\rho : \mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q}) \to GL_2(\bar{\mathbb{Q}}_p)$ lifting $\bar{\rho}_{f,\ell}$ satisfying enough properties such that, if modular, it arises from a cusp eigenform of weight 2 on $\Gamma_0(N/p)$. We use some results of [55] §2, §7 and we follow the notation therein. Consider the lifting problem with

(i) Σ equal to the set of primes different from p at which $\rho_{f,\ell}$ is ramified and ℓ,

(ii) ψ trivial,

(iii) type function t equal to the one attached to $\rho_{f,\ell}$,

(iv) for each $q \in \Sigma$ the inertial type τ_q of $\rho_{f,\ell}|_{G_q}$.

By proposition 2.6.1 in [55], t is definite. Since $\{\rho_{f,\ell}|_{G_q}\}_{q\in\Sigma}$ is a local solution to our lifting problem theorem 7.2.1 in [55] says that there is a global solution ρ that is finitely ramified weight two. It is irreducible since $\bar{\rho}$ is irreducible, and odd since its determinant is the cyclotomic character. By theorem 1.1.4 in [55] ρ is modular, so it arises from a newform g of weight two. Comparing $\rho_{f,\ell}|_{G_q}$ and $\rho|_{G_q}$ at every q we have that g has level N/p and trivial nebentypus (since $\psi = 1$). □

Theorem 2.2.2 (Ribet's level raising theorem)**.** *Let f be a normalized eigenform of weight 2 on $\Gamma_0(N)$ such that the mod ℓ Galois representation*

$$\bar{\rho}_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow GL_2(\overline{\mathbb{F}}_\ell)$$

is irreducible. Let $p \nmid \ell N$ be a prime satisfying

$$\mathrm{tr}\, \bar{\rho}_{f,\ell}(Frob_p) \equiv (-1)^j(p+1) \pmod{\ell}$$

for some $j \in \{0,1\}$. Then there exists a normalized eigenform f' p-new of weight 2 on $\Gamma_0(pN)$ such that $\bar{\rho}_{f,\ell}$ is isomorphic to $\bar{\rho}_{f',\ell}$. Moreover, the p^{th} Fourier coefficient a'_p of f' equals $(-1)^j$. If $p+1 \equiv 0 \pmod{\ell}$ then there are at least two such eigenforms f': one for each coefficient $a'_p \in \{\pm 1\}$.

2.3 Steinberg primes and proof

In this chapter we consider newforms f of weight 2 on $\Gamma_0(N)$ and we work with primes p dividing N once. Recall that in this case the local type of (the automorphic form attached to) f at p is a twist of the Steinberg representation.

Definition 2.3.1. *Let f be a normalized cusp Hecke eigenform of weight 2 level N and trivial nebentypus. We say that a prime p is a* Steinberg prime *of f if $p \parallel N$ and f is p-new.*

Remark 2.3.2. *With the hypothesis of definition 2.3.1, Corollary 4.6.20 in [42] says that there is a unique newform g of weight 2 on $\Gamma_0(N')$ for some divisor N' of N, $p \mid N'$, such that f is in the old-space generated by g. Theorem 4.6.17 in [42] implies that $a_p(g) \in \{-1, 1\}$. Since f is normalized and $p \nmid N/N'$ it is easy to see that $a_p(f) = a_p(g)$.*

Here we state a useful lemma related to the local behavior of the mod ℓ Galois representations at a Steinberg prime.

Lemma 2.3.3 (Langlands)**.** *Let f be a cusp Hecke eigenform of weight 2, level N and trivial nebentypus. Let p be a Steinberg prime of f. Then one has that*

$$\bar{\rho}_{f,\ell}|_{D_p} \sim \begin{pmatrix} \bar{\chi} \cdot \bar{\varepsilon}_\ell & * \\ & \bar{\chi} \end{pmatrix}$$

for every prime $\ell \neq p$, where $\bar{\chi} : D_p \to \mathbb{F}_\ell^*$ denotes the unramified character that maps $Frob_p$ to $a_p(f)$ and $\bar{\varepsilon}_\ell$ denotes the mod ℓ cyclotomic character.

Proof. See [35] (Loeffler, Weinstein 2012) proposition 2.8, we follow the notation therein. The newform f is p-primitive since $p \parallel N$. Recall that Hecke correspondence (a modification of local Langlands correspondence) attaches to $\pi_{f,p} \simeq St \otimes \alpha$, for an unramified character α of $\mathbb{Q}_p^*$, a two dimensional Weil-Deligne representation that corresponds to a Galois representation $r : \mathrm{Gal}(\bar{\mathbb{Q}}_p \mid \mathbb{Q}_p) \to GL_2(\bar{\mathbb{Q}}_\ell)$ of the form

$$r \sim \begin{pmatrix} \alpha \cdot \varepsilon_\ell & * \\ & \alpha \end{pmatrix},$$

where we identify α with a character of $\mathrm{Gal}(\bar{\mathbb{Q}}_p \mid \mathbb{Q}_p)$ via local class field theory. It is a theorem of Carayol [7] that $\rho_{f,\ell}|_{D_p}$ and r are isomorphic. □

Theorem 2.3.4 (Main result)**.** *Let f be a newform of weight 2 on $\Gamma_0(N)$ and let p be a prime at which f is Steinberg. Let $\ell \nmid 2p$ be a prime. Assume either*

1. *$\ell \nmid N$ and $\bar{\rho}_{f,\ell}$ is absolutely irreducible, or*
2. *$\bar{\rho}_{f,\ell}|_{G_{\mathbb{Q}(\zeta_\ell)}}$ is absolutely irreducible.*

Then the following are equivalent:

(a) $\bar{\rho}_{f,\ell}$ *is unramified at* p *and*

$$p \equiv -1 \pmod{\ell}.$$

(b) There is a normalized eigenform f' *p-new of weight* 2 *on* $\Gamma_0(N)$ *such that* $\bar{\rho}_{f',\ell}$ *is isomorphic to* $\bar{\rho}_{f,\ell}$ *and*

$$a_p = -a'_p$$

where a_p *(resp.* a'_p*) is the* p^{th} *Fourier coefficient of* f *(resp.* f'*).*

Proof. (b) implies (a)

Let us write $\bar{\rho} = \bar{\rho}_{f,\ell}$ and $\bar{\rho}' = \bar{\rho}_{f',\ell}$ for simplicity. Let $D_p \subseteq \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ be a decomposition group of p. Since $\{a_p, a'_p\} = \{1, -1\}$, we may assume without loss of generality that $\bar{\rho}$, $\bar{\rho}'$ act locally at p as

$$\bar{\rho}|_{D_p} \sim \begin{pmatrix} \bar{\varepsilon}_\ell & * \\ & 1 \end{pmatrix}$$

and

$$\bar{\rho}'|_{D_p} \sim \begin{pmatrix} \bar{\chi} \cdot \bar{\varepsilon}_\ell & * \\ & \bar{\chi} \end{pmatrix}$$

due to Lemma 2.3.3. Since $\bar{\rho}$ and $\bar{\rho}'$ are isomorphic so are their local behaviors. Thus, specializing at a Frobenius map

$$\begin{pmatrix} p & * \\ & 1 \end{pmatrix} \sim \begin{pmatrix} -p & * \\ & -1 \end{pmatrix} \pmod{\ell}.$$

Eigenvalues must coincide and $\ell > 2$ so

$$p \equiv -1 \pmod{\ell}$$

To see that $\bar{\rho}$ is unramified at p notice that

$$\bar{\chi}\bar{\varepsilon}_\ell \not\equiv \bar{\varepsilon}_\ell.$$

Thus, $\bar{\rho}|_{D_p} \simeq \bar{\varepsilon}_\ell \oplus \bar{\chi}\bar{\varepsilon}_\ell$. Indeed, Lemma 2.3.3 and the isomorphism $\bar{\rho} \simeq \bar{\rho}'$ say that $\bar{\rho}|_{D_p}$ has two 1-dimensional subrepresentations. Since

the actions are different, they generate the whole space. Hence $\bar{\rho}$ is unramified at p.

(a) implies (b)
Ribet's lowering level theorem applies to the modular representation $\bar{\rho}_{f,\ell}$ of level N. Thus, there exists a newform g of weight 2 on $\Gamma_0(M)$, for some $M \mid N/p$ such that $\bar{\rho}_{g,\ell} \sim \bar{\rho}_{f,\ell}$. Moreover, we have that

$$\begin{aligned} \mathrm{tr}\bar{\rho}_{f,\ell}(\mathrm{Frob}_p) &\equiv a_p \cdot (p+1) \\ &\equiv 0 \pmod{\ell} \end{aligned}$$

by Lemma 2.3.3. Now we can apply Ribet's raising level theorem to $\bar{\rho}_{g,\ell}$ and there exists an eigenform f' p-new on $\Gamma_0(N)$ such that

$$\bar{\rho}_{f',\ell} \sim \bar{\rho}_{f,\ell}.$$

By §3 page 9 of [45], when both conditions

$$\mathrm{tr}\bar{\rho}_{g,\ell}(Frob_p) \equiv \pm(p+1) \pmod{\ell}$$

are satisfied Ribet's proof allows us to choose the a_p coefficient of f'. We shall choose f' such that $a'_p = -a_p$ and the implication holds. □

Remark 2.3.5. *Let f be a newform satisfying (a). We expect that Theorem 2.3.4 can be strengthened so that f' can be chosen to be a newform, not necessarily unique. This would follow from a stronger version of [45]. See section 5 for an example.*

2.4 An example

In this section we are going to give an example of mod 5 Galois representation to which our theorem applies. We will use many well-known properties of elliptic curves without proof.

Let ℓ be a prime, $n > 0$ an integer and E an elliptic curve over $\mathbb{Q}$. The ℓ^n-th torsion group $E[\ell^n]$ of E has a natural structure of free $\mathbb{Z}/\ell^n\mathbb{Z}$-module of rank 2. The action of the Galois group $G = \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ is compatible with the $\mathbb{Z}/\ell^n\mathbb{Z}$-module structure of $E[\ell^n]$, so that $E[\ell^n]$ has a natural structure of $(\mathbb{Z}/\ell^n\mathbb{Z})[G]$-module. That is, the action induces a group homomorphism

$$\bar{\rho}_{E,\ell^n} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow Aut_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n]) \simeq GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$$

where the isomorphism depends on the choice of a basis in $E[\ell^n]$. The case $n = 1$ is of special interest and is known as the mod ℓ Galois representation attached to E. The Tate module $\mathcal{T}_\ell E = \varprojlim E[\ell^n]$ of E at ℓ is a free $\mathbb{Z}_\ell$-module of rank 2. The morphisms $\{\bar{\rho}_{E,\ell^n}\}$ induce a group morphism

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow Aut(\mathcal{T}_\ell E) \simeq GL_2(\mathbb{Z}_\ell)$$

known as the ℓ-adic Galois representation attached to E. The mod ℓ Galois representation $\bar{\rho}_{E,\ell}$ attached to E can be recovered from $\rho_{E,\ell}$ by taking reduction mod $\ell\mathbb{Z}_\ell$.

Well-known modularity theorems as Wiles, Taylor-Wiles and Breuil-Conrad- Diamond-Taylor state that such a ℓ-adic Galois representation is isomorphic to the Galois representation $\rho_{f_E,\ell}$ attached to some newform f_E of weight 2 on $\Gamma_0(N)$ for N equal to the conductor of E and $K_f = \mathbb{Q}$. Moreover the pth Fourier coefficient of f_E coincides with the c_p coefficient of E (defined below) for every prime p. In this section we will apply Theorem 2.3.4 to the mod 5 Galois representation $\bar{\rho}_{E,5} \simeq \bar{\rho}_{f_E,5}$ attached to the following elliptic curve given by a (global minimal) Weierstrass equation:

$$E : ZY^2 + XYZ + YZ^2 = X^3 + X^2Z - 614XZ^2 - 5501Z^3.$$

Its discriminant is

$$\Delta = 2^5 \cdot 19^5 \cdot 37.$$

For every prime p let $\tilde{E}_p$ denote the curve obtained by reducing mod p a global minimal Weierstrass model of E. As usual, we consider the value

$$c_p = p + 1 - \#\tilde{E}_p$$

for every prime p. One can check that

$$\begin{cases} \tilde{E}_2 \text{ has a node with tangent lines defined over } \mathbb{F}_2, \\ \tilde{E}_{19} \text{ has a node with tangent lines not defined over } \mathbb{F}_{19}, \\ \tilde{E}_{37} \text{ has a node with tangent lines not defined over } \mathbb{F}_{37}, \\ \tilde{E}_p \text{ is an elliptic curve over } \mathbb{F}_p, \text{ otherwise.} \end{cases}$$

Thus E has conductor $N = 2 \cdot 19 \cdot 37 = 1406$, $c_2 = -c_{19} = -c_{37} = 1$ and there is a newform $f = q + \sum_{n\geq 2} a_n q^n$ of weight 2 on $\Gamma_0(1406)$ such that

- $\rho_{E,5}$ and $\rho_{f,5}$ are isomorphic.
- $c_p = a_p$ for every prime p.

Let us see now that $\bar{\rho}_{f,5}$ satisfies the hypothesis of the Theorem 2.3.4 for $p = 19$. Since

$$\begin{aligned} E_3 &= \{[x : y : z] \in \mathbb{P}^2_{\mathbb{F}_3} : zy^2 + xyz + yz^2 = x^3 + x^2z + xz^2 + z^3\} \\ &= \{[0 : 1 : 0], [2 : 0 : 1]\} \end{aligned}$$

then $c_3 = 2$ and the characteristic polynomial of $\bar{\rho}_{f,5}(Frob_3)$ is congruent to

$$P(X) = X^2 - 2X + 3 \pmod 5.$$

Since the discriminant of $P(X)$ is 2 (mod 5) and 2 is not a square in $\mathbb{F}_5$, then $P(X)$ is irreducible over $\mathbb{F}_5$. In particular $\bar{\rho}_{f,5} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_5)$ is irreducible. It is well known that such a representation is irreducible if and only if it is absolutely irreducible, thus $\bar{\rho}_{f,5}$ is absolutely irreducible. Indeed, $\bar{\rho}_{f,5}$ is odd and hence its image contains a matrix E with eigenvalues $\{\pm 1\}$. Say $\bar{\rho}_{f,5}(c) = E$. If $\bar{\rho}_{f,5}$ is not absolutely irreducible $\bar{\rho}_{f,5}$ is conjugate over $\overline{\mathbb{F}}_5$ to a representation of the form

$$\bar{r} = \begin{pmatrix} \theta_1 & * \\ & \theta_2 \end{pmatrix}$$

for some characters θ_1, θ_2. Take $\epsilon := \theta_1(c) \in \{\pm 1\}$. By changing coordinates over $\mathbb{F}_5$ we may assume that

$$\bar{\rho}_{f,5}(c) = \begin{pmatrix} \epsilon & 0 \\ & -\epsilon \end{pmatrix}.$$

By comparing $\bar{r}$ and $\bar{\rho}_{f,5}$ at c it follows that the conjugation matrix is upper triangular and hence that $\bar{\rho}_{f,5}$ is upper triangular over $\mathbb{F}_5$.

On the other hand, it is well known (see [12] proposition 2.12) that for a prime $p \neq \ell$ dividing once the conductor of an elliptic curve E, $\bar{\rho}_{E,\ell}$ is unramified at p if and only if $\ell \mid v_p(\Delta)$. Since $v_{19}(\Delta) = 5$, $\bar{\rho}_{f,5}$ is also unramified at 19. Hence Theorem 2.3.4 applies to $\bar{\rho}_{E,5}$ and there exists another eigenform f' of weight 2 on $\Gamma_0(1406)$ such that $\bar{\rho}_{f',\ell}$ is isomorphic to $\bar{\rho}_{E,5}$. Thus,

$$c_p \equiv a_p \pmod{\mathfrak{m}_{f',\ell}}. \qquad \text{for every } p \nmid 1406 \cdot 5.$$

and the 19th Fourier coefficient a'_{19} of f' satisfies

$$a'_{19} = -c_{19} = 1.$$

In this example we can find an elliptic curve E' of conductor 1406 such that its corresponding newform f' satisfies part (b) of Theorem 2.3.4. In order to find E' we have assumed that f' can be chosen to be a newform, see Remark 2.3.5. Assuming that f' is newform we can determine a'_2 and a'_{37} of f' as follows. If $a'_2 = -c_2$ Theorem 2.3.4 applies with $\ell = 5$ and $p = 2$ so we conclude that $2 \equiv -1 \pmod 5$. Hence, $a'_2 \neq -c_2$. Since $a'_2 \in \{\pm 1\}$ then $a'_2 = c_2 = 1$. Similarly one can prove that $a'_{37} = c_{37} = -1$. There are three newforms (up to conjugation) with this configuration of signs $(a'_2, a'_{19}, a'_{37}) = (1, 1, -1)$ out of sixteen newforms of weight 2 on $\Gamma_0(1406)$. One of those (the only one satisfying $a'_3 \equiv c_3 \pmod{\mathfrak{m}_{f',5}}$) corresponds to the elliptic curve E' given by a global minimal Weierstrass equation

$$E' : Y^2Z + XYZ + YZ^2 = X^3 - X^2Z - 1191XZ^2 + 507615Z^3.$$

One can check that its conductor is $N = 1406$ and that $c'_2 = c'_{19} = -c'_{37} = 1$. We will use Sturm's bound (see theorem 9.18 in [56] Stein's book) in order to prove that E' corresponds to an eigenform f' as in Theorem 2.3.4. Notice that

$$c'_{19} = 19 + 1 - \#\tilde{E}' = 1 = -c_{19}.$$

Hence, Sturm's result does not apply to the pair $(f_E, f_{E'})$. After twisting both modular forms f_E, $f_{E'}$ by the quadratic character ψ of conductor 19 we get two cusp forms f_E^{ψ}, $f_{E'}^{\psi}$ of weight 2 on $\Gamma_0(1406 \cdot 19)$. Sturm's bound for cusp forms of weight 2 on $\Gamma_0(1406 \cdot 19)$ is 7218.38 and one can check computationally that

$$\psi(p)c_p \equiv \psi(p)c'_p \pmod 5 \tag{2.4.1}$$

for every prime $p < 7219$. Hence, Sturm's result applies to $(f_E^{\psi}, f_{E'}^{\psi})$ and (2.4.1) is true for every p. Thus

$$c_p \equiv c'_p \pmod 5$$

for every prime p for which $\psi(p) \neq 0$, i.e for every prime $p \neq 19$.

Remark 2.4.1. *Take again* $\ell = 5$, $p = 19$. *Similarly one can check that at level* 741 *there is an elliptic curve (Cremona's labeling 741b) satisfying Theorem 2.3.4 a). Notice that there exists no elliptic curve of conductor* 741 *corresponding to an* f' *as in Theorem 2.3.4 b). However, it does exist a newform* f *on* $\Gamma_0(741)$ *and weight* 2 *satisfying Theorem 2.3.4 b), it satisfies* $[K_f : \mathbb{Q}] = 4$.

Chapter 3

Raising the level at your favorite prime

In this chapter we present original work developed in [18]. This exposition is a further improvement of the original ArXiv version thanks to some comments of Samuele Anni and an anonymous referee, for which I am very grateful. Also, we would like to thank Sara Arias-de-Reyna, Nicolas Billerey, Roberto Gualdi, Xavier Guitart, Ricardo Menares and Xavier Xarles for helpful conversations and comments.

3.1 Introduction

For a newform h and a prime $\mathfrak{l}$ in the ring of algebraic integers $\bar{\mathbb{Z}}$ consider the semisimple 2 dimensional continuous Galois representation $\bar{\rho}_{h,\mathfrak{l}}$ with coefficients in $\mathbb{F}_{\mathfrak{l}} = \bar{\mathbb{Z}}/\mathfrak{l}$ attached to h and let $\{a_p(h)\}_p \subset \bar{\mathbb{Z}}$ be the sequence of prime index Fourier coefficients of h. Let f and g be newforms of weight 2 and trivial character. We say that f and g are *Galois congruent* if there is some prime $\mathfrak{l}$ in $\bar{\mathbb{Z}}$ such that $\bar{\rho}_{f,\mathfrak{l}}$, $\bar{\rho}_{g,\mathfrak{l}}$ are isomorphic. This is equivalent to

$$a_p(f) \equiv a_p(g) \pmod{\mathfrak{l}}$$

for all but finitely many p. In 1990 Ribet proved the following

Theorem (K. Ribet)**.** *Let f be a newform in $S_2(\Gamma_0(N))$ such that*

the mod $\mathfrak{l}$ *Galois representation*

$$\bar{\rho}_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$$

is absolutely irreducible. Let $p \nmid N$ *be a prime satisfying*

$$a_p(f) \equiv \varepsilon(p+1) \pmod{\mathfrak{l}}$$

for some $\varepsilon \in \{\pm 1\}$. *Then there exists a newform* g *in* $S_2(\Gamma_0(pM))$, *for some divisor* M *of* N *such that* $\bar{\rho}_{f,\mathfrak{l}}$ *is isomorphic to* $\bar{\rho}_{g,\mathfrak{l}}$. *If* $2 \notin \mathfrak{l}$ *then* g *can be chosen with* $a_p(g) = \varepsilon$.

Hence under some conditions one can *raise the level* of f at p. That is, there is a newform g Galois congruent to f with level divisible by p once. When considering level-raisings of f at p we will tacitly assume that p is *not in the level* of f. In this chapter we do level raising at *every* $p > 2$ by admitting congruences at any prime $\mathfrak{l}$. More precisely, we prove the following.

Theorem 3.1.1. *Let* f *be a newform in* $S_2(\Gamma_0(N))$ *and let* p *be a prime not dividing* N. *Assume that*

(*AbsIrr*) $\bar{\rho}_{f,\mathfrak{l}}$ *is absolutely irreducible for every* $\mathfrak{l}$.

(a_2) *If* $p = 2$ *assume that* $a_2(f)^2 \neq 8$.

Then there exists some M *dividing* N *and some newform* g *in* $S_2(\Gamma_0(Mp))$ *such that* f *and* g *are Galois congruent.*

Remark 3.1.2. *Samuele Anni has pointed out that condition* **(a_2)** *can be dropped. This follows from Theorem 2.1 in [10]. Indeed, if* $a_2(f)^2 = 8$ *then* $x^2 - a_2 x + 2$ *has a double root.*

We prove Theorem 3.1.1 and a variant of it in section 3.4. Condition **(*AbsIrr*)** is quite a stringent one but it is satisfied by lots of forms. For example a theorem of B. Mazur implies that Theorem 1 applies to most of the rational elliptic curves. In section 3.5 we exhibit an infinite family of modular forms satisfying **(*AbsIrr*)** with coefficient fields constant equal to $\mathbb{Q}$.

Remark 3.1.3. *It is worth remarking the existence of infinite families with coefficient fields of unbounded degree satisfying all of the condition* **(*AbsIrr*)**, *see [19].*

Lemma 3.3.3 together with Ribet's theorem imply that we can *choose the sign* of $a_p(g)$ when the congruence of f and g is in odd characteristic. An obstruction appears in characteristic 2 since Ribet's methods identify $1, -1$ mod 2. Le Hung and Li [31] have recently provided a solution to this problem for some f arising from elliptic curves using 2-adic modularity theorems of [1] for the ordinary case and quaternion algebras for the supersingular case. In this chapter we treat the ordinary case.

Theorem 3.1.4. *Let f be a newform in $S_2(N)$, let p be a prime not dividing $6N$ and choose a sign $\varepsilon \in \{\pm 1\}$. Assume that f satisfies* ***(AbsIrr)*** *and for every $\mathfrak{l} \ni 2$ assume that*

(DiehReal) *$\bar{\rho}_{f,\mathfrak{l}}$ has dihedral image induced from a real quadratic extension,*

(2Ord) $\bar{\rho}_{f,\mathfrak{l}}|_{G_2} \simeq \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$.

Then there exists some M dividing N and some newform g in $S_2(Mp)$ such that f and g are Galois congruent and $a_p(g) = \varepsilon$.

We deal with this obstruction in section 3.4.2 following techniques in [31].

Let $E/\mathbb{Q}$ be an elliptic curve. Modularity theorems attach to E a newform $f(E)$ such that $\bar{\rho}_{f,\mathfrak{l}} \simeq E[\ell] \otimes_{\mathbb{F}_\ell} \mathbb{F}_\mathfrak{l}$ modulo semisimplification, for every $\mathfrak{l}$. We obtain an application to elliptic curves.

Theorem 3.1.5. *Let $E/\mathbb{Q}$ be an elliptic curve such that*

- *E has no rational q-isogeny for every q prime,*
- *$\mathbb{Q}(E[2])$ has degree 6 over $\mathbb{Q}$.*

Let p be a prime of good reduction. Then there exists some divisor M of the conductor of E and some newform g in $S_2(Mp)$ such that $f(E)$ and g are Galois congruent. Let $\varepsilon \in \{\pm 1\}$. Assume further that

- *$p \geq 5$,*
- *E has good or multiplicative reduction at 2 and*
- *E has positive discriminant*

then g can be chosen with $a_p(g) = \varepsilon$.

Notation

Let $\bar{\mathbb{Q}}$ denote the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Let $\bar{\mathbb{Z}}$ be the ring of algebraic integers contained in $\bar{\mathbb{Q}}$. We use p, q, ℓ to denote rational primes and $\mathfrak{l}$, $\mathfrak{l}'$ to denote primes of $\bar{\mathbb{Z}}$. We use *prime* of $\bar{\mathbb{Z}}$ to refer to maximal ideals of $\bar{\mathbb{Z}}$, i.e. non-zero prime ideals. We denote by $\mathbb{F}_{\mathfrak{l}}$ the residue field of $\mathfrak{l}$ and ℓ its characteristic. We consider modular forms as power series with complex coefficients and for a newform f we define by $\mathbb{Q}_f$ its field of coefficients, that is the number field $\mathbb{Q}_f = \mathbb{Q}(\{a_p\}_p)$. We denote by $G_{\mathbb{Q}}$ the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})$ and by G_p a decomposition group of p contained in $G_{\mathbb{Q}}$.

3.2 Newforms

Let $\Gamma_0(N)$ be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ corresponding to upper triangular matrices mod N. The space $S_2(N) := S_2(\Gamma_0(N))$ of weight 2 level N trivial Nebentypus cusp forms is a finite dimensional vector space over $\mathbb{C}$. For every M dividing N, $S_2(M)$ contributes in $S_2(N)$ under the so-called degeneracy maps $S_2(M) \hookrightarrow S_2(N)$. Let $S_2(N)^{old}$ be the subspace of $S_2(N)$ spanned by the images of the degeneracy maps for every M properly dividing N. Let $S_2(N)^{new}$ be the orthogonal space of $S_2(N)^{old}$ with respect to the Peterson inner product. A theorem of Atkin-Lehner says that $S_2(N)^{new}$ admits a basis of Hecke eigenforms called newforms; this basis is unique.

3.2.1 Galois representation

Let f be a newform of level N and let $\mathfrak{l}$ be a prime of residue characteristic ℓ. A construction of Shimura (see [12] section 1.7) attaches to f an abelian variety A_f over $\mathbb{Q}$ of dimension $n = [\mathbb{Q}_f : \mathbb{Q}]$. That abelian variety has good reduction at primes not dividing N. Let $\mathbb{Q}_{f,\mathfrak{l}}$ denote the completion of $\mathbb{Q}_f$ with respect to $\mathfrak{l}$. Working with the Tate module $\mathcal{V}_\ell(A_f) = \varprojlim_n A_f[\ell^n] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ one can attach to A_f a continuous Galois representation

$$\rho_{f,\mathfrak{l}} : G_{\mathbb{Q}} \longrightarrow \mathrm{GL}_2(\mathbb{Q}_{f,\mathfrak{l}})$$

such that $det\rho_{f,\mathfrak{l}}$ is the ℓ-adic cyclotomic character and $tr\rho_{f,\mathfrak{l}}(Frob_p) = a_p(f)$ for every $p \nmid N\ell$. Indeed, $\mathcal{V}_\ell(A_f)$ and $\rho_{f,\mathfrak{l}}$ are unramified at

$p \nmid N\ell$ by Neron-Ogg-Shafarevich criterion. Then $\bar{\rho}_{f,\mathfrak{l}}$ is obtained as the semisimple reduction of $\rho_{f,\mathfrak{l}}$ mod $\mathfrak{l}$ tensor $\mathbb{F}_{\mathfrak{l}}$.

Next definition is central in this chapter.

Definition 3.2.1. *Let f, g be newforms of weight two, level N, N' respectively and trivial character.*

- *We say that f and g are* Galois congruent *if there is some prime $\mathfrak{l}$ in $\bar{\mathbb{Z}}$ such that*
$$\bar{\rho}_{f,\mathfrak{l}} \simeq \bar{\rho}_{g,\mathfrak{l}}.$$
- *We say that g* is a level-raising of f at p *if f and g are Galois congruent and $p \parallel N'$ but $p \nmid N$.*
- *We say that g* is a strong level-raising of f at p over $\mathfrak{l}$ *if g is a level raising of f at p with $N' = Np$.*

Remark 3.2.2. *From Brauer-Nesbitt theorem ([11] theorem 30.16) we have that a semisimple Galois representation $\bar{\rho} : \mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q}) \to GL_2(\bar{\mathbb{F}}_\ell)$ is uniquely determined by its characteristic polynomial function. Hence $\bar{\rho}$ is determined by tr and det. Since all Galois representations we consider have cyclotomic determinant Galois congruence is equivalent to congruence on traces of unramified Frobenius (cf. Chebotarev density theorem, [52] Corollary 2).*

Remark 3.2.3. *Let R be a ring at which 2 is invertible and M a free R-module of rank 2. For an endomorphism f of M we have that $tr(f^2) = tr(f)^2 - 2det(f)$ and hence det is determined by tr. This is [12] Proposition 2.6 b) for $d = 2$ and gives necessary conditions on existence of Galois congruences for general weights and levels (cf. [50]).*

Remark 3.2.4. *With our definition Le Hung and Li [31] do strong level raising at a set of primes with some extra requirements always in characteristic 2.*

Let ω_ℓ denote the mod ℓ cyclotomic character and for $\alpha \in \bar{\mathbb{Z}}$ let λ_α be the unique unramified character $\lambda_\alpha : G_p \to \mathbb{F}_{\mathfrak{l}}^\times$ sending the arithmetic Frobenius $Frob_p$ to α mod $\mathfrak{l}$. We collect in the following theorem work of Deligne, Serre, Fontaine, Edixhoven, Carayol and Langlands. It gives some necessary conditions for level-raising existence.

Theorem 3.2.5. *Let g be a newform in $S_2(Mp)$ with $p \nmid 2M$ and fix a prime $\mathfrak{l}$. Then*

$$\bar{\rho}_{g,\mathfrak{l}}|_{G_p} \simeq \begin{pmatrix} \omega_\ell & * \\ & 1 \end{pmatrix} \otimes \lambda_{a_p(g)}.$$

Let f be a newform $S_2(N)$, $p \nmid 2N$ and fix a prime $\mathfrak{l}$ containing p. Then either $\bar{\rho}_{f,\mathfrak{l}}|_{G_p}$ is irreducible or

$$\bar{\rho}_{f,\mathfrak{l}}|_{G_p} \simeq \begin{pmatrix} \omega_p \lambda_{a_p(f)^{-1}} & * \\ & \lambda_{a_p(f)} \end{pmatrix}$$

with $*$ 'peu ramifié'.

Proof. Case $p \in \mathfrak{l}$ is Theorem 6.7 in [5] for $k = 2$. Because $a_p(g) \in \{\pm 1\}$, we have that g is ordinary at p. Case $p \notin \mathfrak{l}$ follows from Carayol's theorem in [7].

The statement for f is Corollary 4.3.2.1 in [6]. □

Following corollaries were inspired by Proposition 6 in [4].

Corollary 3.2.6. *Let $f \in S_2(N)$, $g \in S_2(Mp)$ be Galois congruent newforms over $\mathfrak{l}$, $p \nmid 2NM$. Then*

$$a_p(f) \equiv a_p(g)(p+1) \pmod{\mathfrak{l}}.$$

Proof. Case $p \notin \mathfrak{l}$. We have that $tr\bar{\rho}_{g,\mathfrak{l}}(Frob_p) = a_p(g)(p+1)$. On the other hand $\bar{\rho}_{f,\mathfrak{l}}$ is unramified at p and has trace $a_p(f)$ at $Frob_p$.
Case $p \in \mathfrak{l}$. The isomorphism $\bar{\rho}_{f,\mathfrak{l}}|_{G_p} \simeq \bar{\rho}_{g,\mathfrak{l}}|_{G_p}$ implies that $\bar{\rho}_{f,\mathfrak{l}}|_{G_p}$ reduces and we have equality of characters

$$\{\omega_p \lambda_{a_p(g)}, \lambda_{a_p(g)}\} = \{\omega_p \lambda_{a_p(f)^{-1}}, \lambda_{a_p(f)}\}$$

The mod p cyclotomic character is ramified since $p \neq 2$. In particular $a_p(g) \equiv a_p(f) \pmod{\mathfrak{l}}$. □

As a consequence we obtain a result on congruent modular forms with level-raising.

Corollary 3.2.7. *Let $f \in S_2(N)$, $g \in S_2(Mp)$ be newforms, $p \nmid 2NM$. If f and g are* congruent, *that is*

$$a_n(f) \equiv a_n(g) \pmod{\mathfrak{l}} \qquad \text{for every } n,$$

then

$$\ell = p \qquad \text{and} \qquad a_p(f) \equiv a_p(g) = \pm 1 \pmod{\mathfrak{l}}.$$

Proof. Congruence implies Galois congruence. We have that

$$a_p(g) \equiv a_p(f) \equiv a_p(g)(p+1) \pmod{\mathfrak{l}}.$$

The corollary follows since $a_p(g) \in \{\pm 1\}$. □

3.2.2 Ribet's level raising

Ribet's theorem says that the necessary condition of Corollary 3.2.6 for level-raising turns out to be enough modulo some irreducibility condition.

Theorem 3.2.8 (Ribet's level raising theorem)**.** *Let f be a newform in $S_2(N)$ such that the mod $\mathfrak{l}$ Galois representation*

$$\bar{\rho}_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{F}_{\mathfrak{l}})$$

is absolutely irreducible. Let $p \nmid N$ be a prime satisfying

$$a_p(f) \equiv \varepsilon(p+1) \pmod{\mathfrak{l}}$$

for some $\varepsilon \in \{\pm 1\}$. Then there exists a newform g in $S_2(pM)$, for some divisor M of N such that $\bar{\rho}_{f,\mathfrak{l}}$ is isomorphic to $\bar{\rho}_{g,\mathfrak{l}}$. If $2 \notin \mathfrak{l}$ then g can be chosen with $a_p(g) = \varepsilon$.

Remarks 3.2.9.

- *Ribet's original approach [47] deals with modular Galois representations $\bar{\rho}$ so that in particular there is some newform f such that $\bar{\rho} \simeq \bar{\rho}_{f,\mathfrak{l}}$. His approach deals with traces of Frobenii; this forces him to deal with unramified primes only, hence the hypothesis $p \neq \ell$. As Ribet explains loc. cit. the theorem can be stated in terms of Hecke operators and hence in terms of Fourier coefficients even if $p = \ell$, when the level of f is prime to p.*

- *Every normalized Hecke eigenform f' has attached a unique newform f so that the $\mathfrak{l}$-adic Galois representations attached to f' are the ones attached to f. Furthermore, the level of f divides the level of f'. Hence p-new in Ribet's article means new of level pM for some $M \mid N$.*

We introduce a definition in order to deal with the irreducibility condition.

Definition 3.2.10. *Let $f \in S_2(N)$ be a newform, let $\mathfrak{l}$ be a prime of $\overline{\mathbb{Z}}$ and let $\bar{\rho}_{f,\mathfrak{l}} : \mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_{\mathfrak{l}})$ denote the semisimple mod $\mathfrak{l}$ Galois representation attached to f by Shimura. We say that f satisfies condition* ***(AbsIrr)*** *if $\bar{\rho}_{f,\mathfrak{l}}$ is absolutely irreducible for every prime $\mathfrak{l}$.*

In section 3.6 we provide explicit examples with $\mathbb{Q}_f = \mathbb{Q}$. See [19] Theorem 6.2 for a construction of families $\{f_n\}$ for which the set of degrees $\{\dim_{\mathbb{Q}} \mathbb{Q}_{f_n}\}_n$ is unbounded.

Remark 3.2.11. *N. Billerey and R. Menares have pointed out that Theorem 3.2.8 has been extended to cases where the irreducibility condition is not satisfied. In particular one can commonly do level-raising through reducible mod $\mathfrak{l}$ Galois representations. Nevertheless, we will only consider level-raisings obtained through absolutely irreducible mod $\mathfrak{l}$ Galois representations, see section 3.7.*

3.3 Bounds and arithmetics of Fourier coefficients

In light of Ribet's theorem and the following well-known properties of Fourier coefficients we study some arithmetic properties of $p + 1 \pm a_p$.

Theorem 3.3.1. *Let f be a newform in $S_2(N)$ and let a_p be the p^{th} Fourier coefficient of f, p prime. Then*

(i) $a_p \in \overline{\mathbb{Z}}$,

(ii) a_p *is totally real. That is, its minimal polynomial splits over* $\mathbb{R}$,

(iii) (Hasse-Weil Theorem) $|\sigma(a_p)| \leq 2\sqrt{p}$ *for every embedding* $\sigma : \mathbb{Q}(a_p) \longrightarrow \mathbb{R}$.

We say that $a_p \in \overline{\mathbb{Q}}$ is a p^{th} *Fourier coefficient* if a_p satisfies conditions $(i) - (iii)$.

3.3.1 Arithmetic lemmas

Let K be a number field with ring of integers $\mathcal{O}$. Let S be the set of complex embeddings $\sigma : K \to \mathbb{C}$ of K. For every $\alpha \in \mathcal{O}$ we consider the norm

$$N_K(\alpha) = \prod_{\sigma \in S} \sigma(\alpha)$$

and the characteristic polynomial

$$P_\alpha(X) = \prod_{\sigma \in S} (X - \sigma(\alpha)).$$

One has that $P_\alpha(0) = (-1)^{|S|} N_K(\alpha)$. The following well-known lemma is basic algebraic number theory.

Lemma 3.3.2. *Let K be a number field and α an algebraic integer of K. Then $P_\alpha(X) \in \mathbb{Z}[X]$ and $N_K(\alpha) \in \mathbb{Z}$. A rational prime ℓ divides $N_K(\alpha)$ if and only if there is some prime $\mathfrak{l}$ in $\bar{\mathbb{Z}}$ of residue characteristic ℓ such that $\alpha \equiv 0 \pmod{\mathfrak{l}}$. In particular α is a unit of $\mathcal{O}$ if and only if $N_K(\alpha) = \pm 1$.*

Proof. Let $n = |S| = \dim_{\mathbb{Q}} K$. Consider the embedding $\iota : K \hookrightarrow End_{\mathbb{Q}}(K)$, where $\iota(\alpha)$ is the multiplication-by-α morphism. A choice of integral basis of K induces an embedding $\iota : K \hookrightarrow M_{n\times n}(\mathbb{Q})$ with $\iota(\mathcal{O}) \subset M_{n\times n}(\mathbb{Z})$. Then $P_\alpha(X)$ is the characteristic polynomial of $\iota(\alpha)$ by Cayley-Hamilton theorem. For a nonzero $\alpha \in \mathcal{O}$ one has that $|N_K(\alpha)| = |\mathcal{O}/\alpha\mathcal{O}| = \prod_i |\mathcal{O}/\mathfrak{p}_i^{e_i}|$ where $\alpha\mathcal{O} = \prod_i \mathfrak{p}_i^{e_i}$ is the factorization in prime ideals of the ideal generated by α. Thus ℓ divides $N_K(\alpha)$ if and only if some prime $\mathfrak{p}$ of $\mathcal{O}$ containing ℓ divides $\alpha\mathcal{O}$. Moreover, the map $MaxSpec(\bar{\mathbb{Z}}) \to MaxSpec(\mathcal{O})$ given by $\mathfrak{l} \mapsto \mathfrak{l} \cap \mathcal{O}$ is surjective and the lemma follows. □

Lemma 3.3.3. *Let a_p be a p^{th} Fourier coefficient.*

(a) $(p+1+a_p)(p+1-a_p)$ is unit in $\bar{\mathbb{Z}}$ if and only if $p = 2$ and $a_2^2 = 8$.

(b) If $p > 3$ then $p + 1 \pm a_p$, is not unit in $\bar{\mathbb{Z}}$.

Proof. Let $K = \mathbb{Q}(a_p)$ and $S = \{\sigma : \mathbb{Q}(a_p) \hookrightarrow \mathbb{R}\}$ be the set of embeddings. Its cardinality equals n the degree of $\mathbb{Q}(a_p) \mid \mathbb{Q}$.

(a) We have

$$\begin{aligned}\sigma((p+1+a_p)(p+1-a_p)) &= (p+1)^2 - \sigma(a_p)^2 \\ &\geq (p+1)^2 - 4p \\ &= (p-1)^2 \\ &\geq 1.\end{aligned}$$

Hence $N_K((p+1+a_p)(p+1-a_p)) \geq (p-1)^{2n} \geq 1$. Equalities hold if and only if $p = 2$ and $9 - a_2^2 = 1$.

(b) Since $\sigma(p+1 \pm a_p) \geq p+1-2\sqrt{p} = (\sqrt{p}-1)^2$ then

$$N_K(p+1 \pm a_p) \geq (\sqrt{p}-1)^{2n} > 1$$

provided that $p > 3$.

□

Lemma 3.3.4 (Avoiding p)**.** *Fix a positive odd integer n. There exists an integer C_n such that if a_p is a p^{th} coefficient of degree n with $p > C_n$ then there is a prime $\mathfrak{l}$ not over p such that*

$$\mathfrak{l} \mid (a_p + p + 1)(a_p - p - 1).$$

Proof. Let $K = \mathbb{Q}(a_p)$ and assume that $(p+1+a_p)(p+1-a_p)$ factors as product of primes over p in the ring of integers of K. Then $N_K(p+1-a_p)$, $N_K(p+1+a_p)$ are powers of p in the closed interval $I_n = [(\sqrt{p}-1)^{2n}, (\sqrt{p}+1)^{2n}]$. We can take p great enough so that p^n is the unique power of p in I_n. Thus

$$\begin{aligned}N_K(p+1-a_p) = N_K(p+1+a_p) &= p^n \\ N_K(-p-1-a_p) = (-1)^n N_K(p+1+a_p) &= -p^n\end{aligned}$$

In particular $0 \equiv P_{a_p}(p+1) - P_{a_p}(-p-1) = 2p^n \pmod{p+1}$. □

We can describe the bound C_n: conditions $p^{n+1}, p^{n-1} \notin I_n$ are equivalent to

$$p > \left(\frac{p}{p - 2\sqrt{p} + 1}\right)^n =: \alpha(p, n),$$
$$p > \left(\frac{p + 2\sqrt{p} + 1}{p}\right)^n =: \beta(p, n)$$

Notice that $\beta < \alpha$ and that p satisfies $p > \alpha(p, n)$ if and only if $x^n > x^{n-1} + 1$ where $x^{2n} = p$. Since n is odd we can take θ the greatest real root of $X^n - X^{n-1} - 1$ and $C_n := \theta^{2n}$. One can check that C_n grows asymptotically as $f(n) = e^{2W(n)}$, where W is the Lambert W function. Recall that

$$\left(\frac{n}{\log n}\right)^2 \leq f(n) \leq n^2 \qquad \text{if } n \geq 3.$$

Lemma 3.3.5. *The best bound for $n = 1$ is $C_1 = 2$.*

Proof. Notice that $(p+1)^2 - a_p^2 = 8$ if $p = 2$, $a_p = \pm 1$. Following the notation above we have that $\theta = 2$ for $n = 1$ and $C_1 = 4$ works. Thus it is enough to check that $(4 - a_3)(4 + a_3)$ is not $\pm$ a power of 3. Both factors are positive by Hasse's bound. Thus $4 + a_3 = 3^a$, $4 - a_3 = 3^b$ and $3^a + 3^b = 8$. □

3.4 Proofs

3.4.1 Proof of the main result and a variant

Proof of Theorem 3.1.1. Let $f \in S_2(N)$ new and $p \nmid N$. We need to check that Ribet's theorem applies for some $\mathfrak{l}$. By Theorem 3.3.1 and Lemma 3.3.3, $(p + 1 + a_p)(p + 1 - a_p)$ is not invertible in $\bar{\mathbb{Z}}$. Hence it is contained in a maximal ideal $\mathfrak{l}$. That is, either $a_p \equiv p + 1 \pmod{\mathfrak{l}}$ or $a_p \equiv -p - 1 \pmod{\mathfrak{l}}$. □

Following variant allows us to do level-raising at p over characteristic $\ell \neq p$. This together with Corollary 3.2.7 ensures that the predicted Galois congruence is not a congruence of *all* Fourier coefficients, at least when the level-raising is at $p \neq 2$.

Theorem 3.4.1. *Let f be a newform in $S_2(N)$ such that $n := \dim_{\mathbb{Q}} K_f$ is odd. Assume that*

(*AbsIrr*) *$\bar{\rho}_{f,\mathfrak{l}}$ is absolutely irreducible for every $\mathfrak{l}$.*

There exists a constant $C > 0$ such that for every prime $p > C$ f has a level-raising g at p over a prime $\mathfrak{l}$ of residue characteristic different from p. C depends only on n.

Proof. Let $f \in S_2(N)$ new. Due to **(*AbsIrr*)** it is enough to find a maximal ideal $\mathfrak{l}$ not over p. This is done in Lemma 3.3.4. □

3.4.2 Choice of sign mod 2

In this section we adapt some ideas of [31] to our case. The strategy is to solve a finitely ramified deformation problem. This kind of deformation problem consists on specifying the ramification behavior at all but one chosen prime q. If such a deformation problem has solution and some modularity theorem applies this provides newforms with specified weight, character and prime-to-q part level. If one chooses an auxiliary prime q, a twist argument kills the ramification at q so that one recovers a newform with the specified weight, character and level.

Fix a prime ideal $\mathfrak{l} \ni 2$ of $\bar{\mathbb{Z}}$. Let ρ_2 be a Galois representation $G_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{F}_{\mathfrak{l}})$ with *dihedral image* D and let $E = \bar{\mathbb{Q}}^D$ be the number field fixed by $\ker \rho_2$. The order of an element in $\mathrm{SL}_2(\mathbb{F}_{\mathfrak{l}})$ is either 2 or odd. This forces D to have order $2r$, $2 \nmid r$. In particular $E \mid \mathbb{Q}$ has a unique quadratic subextension $K \mid \mathbb{Q}$ and ρ_2 is induced from a character $\chi : \mathrm{Gal}(\bar{\mathbb{Q}} \mid K) \to \mathbb{F}_{\mathfrak{l}}^{\times}$ of order r.

We say that q is an *auxiliary prime* for ρ_2 if

- $q \equiv 3 \pmod 4$ and
- ρ_2 is unramified at q and $\rho_2(Frob_q)$ is non-trivial of odd order.

Proposition 3.4.2. *Let g be a newform in $S_2(Mq^{\alpha})$, $q \nmid M$, such that $\bar{\rho}_{g,\mathfrak{l}}$ is unramified at an auxiliary prime q. Then either g or $g \otimes \left(\frac{\cdot}{q}\right)$ has level M.*

Proof. $\bar{\rho}_{g,\mathfrak{l}}(Frob_q)$ has different eigenvalues by the order condition, thus $\rho_{g,\mathfrak{l}}|_{I_q}$ factors through a quadratic character η of I_q (Lemma 3.4 in [31]). By the structure of tame inertia at $q \neq 2$ there is a unique open

subgroup in I_q of index 2 and $\eta : I_q \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_q^{ur}(\sqrt{q}) \mid \mathbb{Q}_q^{ur}) \simeq \{\pm 1\}$. If η is trivial then $\alpha = 0$ and we are done. Otherwise, η extends locally to $G_q \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}_q(\sqrt{-q}) \mid \mathbb{Q}_q)$ and globally to the Legendre symbol

$$\left(\frac{\cdot}{q}\right) : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{-q}) \mid \mathbb{Q}) \simeq \{\pm 1\}.$$

Legendre symbol over q is only ramified at q and the proposition follows. □

Auxiliary primes are inert at $\mathbb{Q}(i)$ and split at K by a parity argument. In particular, ρ_2 has auxiliary primes only if $K \neq \mathbb{Q}(i)$.

Lemma 3.4.3. *Let $\rho_2 : G_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{F}_\mathfrak{l})$ be a Galois representation as above. Assume that ρ_2 is not ramified at p and that $K \neq \mathbb{Q}(i)$. Then the set of auxiliary primes for ρ_2 splitting at $\mathbb{Q}(\sqrt{p})$ has positive density in the set of all primes.*

Proof. As in Lemma 3.2 of [31] E and $\mathbb{Q}(i, \sqrt{p})$ are linearly disjoint since E is unramified at p and $K \neq \mathbb{Q}(i)$. Chebotarev density theorem implies the lemma. □

Theorem 3.4.4. *Let f be a newform in $S_2(N)$, p be a prime not dividing $6N$ and $\varepsilon \in \{\pm 1\}$ a sign. Assume that $a_p \equiv 1 + p \bmod \mathfrak{l}$ for some prime $\mathfrak{l}$ containing 2. Assume that*

1. *$\bar{\rho}_{f,\mathfrak{l}}$ has dihedral image induced from a real quadratic extension, and*
2. ***(2Ord)*** $\bar{\rho}_{f,\mathfrak{l}}|_{G_2} \simeq \begin{pmatrix} 1 & * \\ & 1 \end{pmatrix}$

then there exists some M dividing N and some newform g in $S_2(Mp)$ such that f and g are Galois congruent and $a_p(g) = \varepsilon$.

Proof. Let q be an auxiliary prime for $\bar{\rho}_{f,\mathfrak{l}}|_{G_2}$ splitting at $\mathbb{Q}(\sqrt{p})$. By Theorem 4.2 of [31] there is some newform g in $S_2(Npq^\alpha)$ with $a_p(g) = \varepsilon$. Let g' be the newform in $S_2(Np)$ obtained by Proposition 3.4.2. Then $a_p(g') = a_p(g)$ since $\left(\frac{p}{q}\right) = 1$. □

Proof ot Theorem 3.1.4. By Lemma 3.3.3 there are some maximal ideals $\mathfrak{l}^+$, $\mathfrak{l}^-$ such that $a_p(f) \equiv p + 1 \pmod{\mathfrak{l}^+}$ and $a_p(f) \equiv -p - 1 \pmod{\mathfrak{l}^-}$. If $2 \notin \mathfrak{l}^+, \mathfrak{l}^-$ then Ribet's theorem applies and we are done. Otherwise apply previous theorem. □

3.5 Case $n = 1$. Elliptic curves and $\mathbb{Q}$-isogenies

Let $E/\mathbb{Q}$ be an elliptic curve and let $E_p/\mathbb{F}_p$ be the mod p reduction of (the minimal Weierstrass model over $\mathbb{Q}_p$ of) E for a prime p. Consider the integer $c_p = p + 1 - \#E_p(\mathbb{F}_p)$. Then there is a unique newform f of weight 2 such that $a_p(f) = c_p$ for every prime p. This is a consequence of modularity of elliptic curves over $\mathbb{Q}$. In particular, $\bar{\rho}_{f,\mathfrak{l}}$ and $E[\ell] \otimes \mathbb{F}_\mathfrak{l}$ are isomorphic up to semisimplification for every prime $\mathfrak{l}$. In this section we characterize elliptic curves whose corresponding newform f satisfies $\textbf{(}\boldsymbol{AbsIrr}\textbf{)}$.

Let $E/\mathbb{Q}$ be an elliptic curve, ℓ an odd prime and $c \in \mathrm{Gal}(\mathbb{C} \mid \mathbb{R}) \subset \mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})$ be the complex conjugation. Then c acts on $E[\ell]$ with characteristic polynomial $X^2 - 1$. This follows from the existence of the Weil pairing. In particular $E[\ell]$ is irreducible if and only if $E[\ell] \otimes \mathbb{F}_\mathfrak{l}$ is irreducible, i.e if and only if $E[\ell]$ is absolutely irreducible. We say that E satisfies $\textbf{(}\boldsymbol{Irr}\textbf{)}$ if $E[\ell]$ is irreducible for every ℓ. From a particular study of the case $\ell = 2$ one obtains the

Lemma 3.5.1. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E satisfies $\textbf{(}\boldsymbol{AbsIrr}\textbf{)}$ if and only if E satisfies $\textbf{(}\boldsymbol{Irr}\textbf{)}$ and $\mathbb{Q}(E[2])$ has degree 6 over $\mathbb{Q}$.*

Proof. Let us explain the above discussion. Let ℓ be an odd prime and assume that $V := E[\ell] \otimes \mathbb{F}_\mathfrak{l}$ is reducible. Then there is a line L, i.e. a $\mathbb{F}_\mathfrak{l}$-submodule of V of rank 1, stable under the action of $G_\mathbb{Q}$. The complex conjugation c acts on V with minimal polynomial $X^2 - 1$. Thus, c acts on L as εId for some $\varepsilon \in \{\pm 1\}$. Let $v \in E[\ell]$ such that $cv = \varepsilon v$, then $v \in L$ and $L = v\mathbb{F}_\mathfrak{l}$. Thus $v\mathbb{F}_\ell$ is stable under the action of $G_\mathbb{Q}$, i.e. $E[\ell]$ is reducible.

□

3.5.1 Isogenies

In practice one can deal with $\textbf{(}\boldsymbol{Irr}\textbf{)}$ by studying the graphs of isogeny. The LMFDB project has computed in [36] a huge amount of elliptic curves and isogenies. We recall some well known results on this topic.

Let E, E' be elliptic curves defined over $\mathbb{Q}$. An *isogeny* is a non-constant morphism $E \longrightarrow E'$ of abelian varieties over $\mathbb{Q}$. The map

$$\begin{array}{ccccc} \{E \to E' \text{ isogeny}\}/\cong & \longrightarrow & \{\text{finite } \mathbb{Z}[\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})]\text{-submodules of } E\} \\ \varphi & \longmapsto & \ker \varphi \end{array}$$

defines a bijection. Here, E is fixed and E' ranges over all elliptic curves over $\mathbb{Q}$. Also one says that $(E \xrightarrow{\varphi} E') \cong (E \xrightarrow{\psi} E'')$ if there is an isomorphism $E' \xrightarrow{\theta} E''$ of elliptic curves such that $\psi = \theta \circ \varphi$. Hence, the torsion group $E[n]$ corresponds to the multiplication-by-n map $E \xrightarrow{[n]} E$ under the bijection.

The set of elliptic curves over $\mathbb{Q}$ (up to $\mathbb{Q}$-isomorphism) has a natural graph structure with edges consisting in isogenies. Let E be an elliptic curve over $\mathbb{Q}$. The graph of the isogeny class of E is the maximal connected subgraph containing E. We say that E has trivial graph of isogenies if the graph of the isogeny class of E consists in the vertex E.

Lemma 3.5.2. *Let $E/\mathbb{Q}$ be an elliptic curve. The following are equivalent*

1. *E satisfies* $\boldsymbol{(Irr)}$.
2. *E is has trivial graph of isogenies.*
3. *Every finite $\mathbb{Z}[\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})]$-submodule of E is of the form $E[n]$ for some n.*

Proof. Let $G_{\mathbb{Q}}$ denote the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}} \mid \mathbb{Q})$. We will prove that (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1). For the first implication let $E \xrightarrow{\varphi} E'$ be an isogeny. Then there exists a maximal n such that φ factors as

$$E \xrightarrow{[n]} E \xrightarrow{\psi} E'$$

for some isogeny $\psi : E \to E'$. It can be checked that n is the biggest integer satisfying $E[n] \subset \ker \varphi$. Let $r = \#\ker \psi$. If $p \mid r$ then $E[p] \cap \ker \psi$ is a nontrivial subrepresentation of $E[p]$. If E satisfies $\boldsymbol{(Irr)}$ then $r = 1$ and ψ is an isomorphism.
For the implication (2) $\Rightarrow$ (3) let H be a finite $\mathbb{Z}[G_{\mathbb{Q}}]$-submodule of E. It corresponds to some isogeny $E \xrightarrow{\varphi} E'$ with kernel equal to H. By hypothesis E and E' are isomorphic say $E' \xrightarrow{h} E$. Thus $h \circ \varphi$ is an endomorphism of E defined over $\mathbb{Q}$. Hence $h \circ \varphi = [n]$ for some n, see Theorem 2.2 in [54]. Thus, $E[n] = \ker h \circ \varphi = \ker \varphi = H$. The last implication is trivial. □

If the graph of isogenies is unknown one can still do something. In 1978 Barry Mazur proved the

Theorem 3.5.3 (B. Mazur)**.** *Let $E/\mathbb{Q}$ be an elliptic curve and let ℓ be a prime such that $E[\ell]$ is reducible. Then*

$$\ell \in \mathcal{T} := \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

See [38]. Hence, there is a complete list of possible irreducible submodules of $E[\ell]$. We will use Mazur's theorem later in order to exhibit a family of elliptic curves satisfying **(*Irr*)**.

3.5.2 Twists

Condition **(*AbsIrr*)** is invariant under $\bar{\mathbb{Q}}$-isomorphism. This follows from the fact that Galois representations attached to $\bar{\mathbb{Q}}$-isomorphic rational elliptic curves differ by a finite character. The useful invariant in this context is the j-invariant. More precisely, the map

$$\begin{array}{rccc} j: & Ell := \{E/\mathbb{Q} \text{ elliptic curve }\}/\cong_{\bar{\mathbb{Q}}} & \longrightarrow & \mathbb{Q} \\ & E & \longmapsto & j(E) \end{array}$$

is a bijection, hence **(*AbsIrr*)** is codified in the j-invariant.

Definition 3.5.4. *Let $a/b \in \mathbb{Q}$, with a, b coprime integers. The* Weil height *of a/b is*

$$h(a/b) := \max\{|a|, |b|\}.$$

Let S be a subset of Ell. We say that S has Weil density *d if*

$$\lim_{n\to\infty} \frac{\#\{E \in S : h(j(E)) \leq n\}}{\#\{x \in \mathbb{Q} : h(x) \leq n\}} = d.$$

Proposition 3.5.5. *Let S be the set elliptic curves satisfying* **(*AbsIrr*)** *modulo isomorphism. Then S has Weil density* 1*.*

Proof. The j-invariant morphism extends to an isomorphism $X(1)_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ of rational algebraic curves. Here $X(1)_{\mathbb{Q}}$ denotes a rational model of the trivial-level modular curve. Hence Ell is the set $Y(1)(\mathbb{Q}) \subseteq X(1)(\mathbb{Q})$ of rational non-cuspidal points of $X(1)$. Let $p \geq 2$ be prime and let $X_0(p)_{\mathbb{Q}}$ a model over $\mathbb{Q}$ of the modular curve of level $\Gamma_0(p)$.

We have the forgetful map $X_0(p) \to X(1)$ which is a morphism of algebraic curves of degree $p+1$. Elliptic curves not satisfying **(*Irr*)** correspond to non-cuspidal points in the image of $f_p : X_0(p)(\mathbb{Q}) \to X(1)(\mathbb{Q})$, for $p \leq 163$ by Mazur. Either $X_0(p)$ has genus 0, in which case $p \in \{2,3,5,7,13\}$, or $X_0(N)$ has positive genus, in which case $p \in \{11,17,19,37,43,67,163\}$ and $X_0(p)(\mathbb{Q})$ is finite. Image of f_p has 0 Weil density in $X(1)$ for every $p \leq 163$, this follows from Theorem $B.2.5$ in [26] for the genus 0 case. In particular elliptic curves satisfying **(*Irr*)** have density 1. One can deal similarly with the condition $\dim_{\mathbb{Q}} \mathbb{Q}(E[2]) = 6$. □

3.6 Examples

3.6.1 A family of elliptic curves

In this section we give a family of elliptic curves over $\mathbb{Q}$ satisfying **(*AbsIrr*)**. First we find a family of elliptic curves with irreducible 2-torsion as $\bar{\mathbb{F}}_2[G_{\mathbb{Q}}]$-module. This is done by exhibiting a family of rational cubic polynomials with symmetric Galois group. Second we take a subfamily with irreducible ℓ-torsion as $\mathbb{F}_\ell[G_{\mathbb{Q}}]$-module, for every $\ell \in \mathcal{T}$. See Theorem 3.5.3 for the definition of $\mathcal{T}$.

Lemma 3.6.1. *Let $n \neq \pm 1$ be an integer such that $3n$ is not square. The polynomial $P_n(X) = X^3 - 3(n+1)X + 2(n+1)$ has Galois group isomorphic to S_3.*

Proof. Let us see that P_n is irreducible over $\mathbb{Q}$ when $n \neq 0, \pm 1$. Consider a factorization $P_n(X) = (X-a)(X^2+bX+c)$ over the integers. By equating coefficients we have that

$$\begin{cases} a & = b \\ 2a^2 + 3ac - 2c & = 0 \\ -ac & = 2(n+1) \end{cases}$$

The conic $0 = 18(2X^2 + 3XY - 2Y) = (6X + 9Y + 4)(6X - 4) + 16$ has finitely many integer points, namely

$$(a,b) \in \{(0,0), (-2,1), (1,-2), (2,-2)\}.$$

In particular P_n is irreducible if and only if $n \notin \{-1, 0, 1\}$. In this case either P_n has Galois group of order three or P_n has Galois group isomorphic to S_3, the latter corresponds to the nonsquare discriminant case. The discriminant of P_n is $\Delta_n = 3n \cdot 36(n+1)^2$ and the lemma follows. □

Lemma 3.6.2. *Consider the elliptic curve defined over $\mathbb{F}_{1427}$ given by the equation*

$$\bar{E} : Y^2 = X^3 + 3 \cdot 11X - 2 \cdot 11.$$

Then $\bar{E}[\ell]$ is irreducible over $\mathbb{F}_\ell$ for every $\ell \in \mathcal{T}$.

Proof. It can be checked that $\#\bar{E}(\mathbb{F}_{1427}) = 1424$. Let φ denote the Frobenius over 1427, then φ satisfies

$$\varphi^2 - 4\varphi + 1427 = 0$$

as an endomorphism of $\bar{E}$. The polynomial $X^2 - 4X + 1427$ is irreducible over $\mathbb{F}_\ell$ for every $\ell \in \mathcal{T}$ and hence $\bar{E}[\ell]$ is irreducible. □

Theorem 3.6.3. *Let n be an integer such that*

$$k \equiv -11 \pmod{1427}.$$

Then the elliptic curve given by the equation

$$E_k : Y^2 = X^3 - 3kX + 2k$$

satisfies ***(AbsIrr)***. *In particular it is Galois congruent to infinitely many newforms.*

Proof. Since -12 is not a square in $\mathbb{F}_{1427}$ Lemma 3.6.1 applies and since $E_k[\ell]$ is unramified over 1427 for every $\ell \in \mathcal{T}$ the theorem follows. □

Remark 3.6.4. *Notice that Theorem 3.4.1 together with Lemma 3.3.5 say that every level-raising of E_k at $p > 2$ can be done far from p. This together with Corollary 3.2.7 implies that odd level-raisings of E_k can be chosen not congruent.*

3.6.2 Control of M

Let f be a newform of level N and let $\mathfrak{l}$ be a prime. If $\bar{N} = N(\bar{\rho}_{f,\mathfrak{l}})$ denotes the prime-to-ℓ conductor of $\bar{\rho}_{f,\mathfrak{l}}$ then $\bar{N} \mid N$. With this in mind we manage in next theorem to take $M = N$.

Theorem 3.6.5. *Let $E/\mathbb{Q}$ be an elliptic curve such that*

(i) E has trivial graph of isogenies,

(ii) $\mathbb{Q}(E[2])$ has degree 6 over $\mathbb{Q}$,

(iii) E is semistable with good reduction at 2,

(iv) $\Delta(E)$ is square-free.

Let N denote the conductor of E and let $p \nmid N$ be a prime. Then there exists some newform $g \in S_2(Np)$ Galois congruent to $f(E)$.

Proof. Let $\mathfrak{l}$ be a prime and g a newform in $S_2(Mp)$ such that g is a level raising of E over $\mathfrak{l}$. Let us prove that $M = N$. Since $\Delta(E)$ is square-free then $E[\ell]$ is ramified at every prime $p \mid N$, $p \neq \ell$, and the prime-to-ℓ conductor N_ℓ of E is the prime-to-ℓ conductor of $E[\ell]$ (cf. Proposition 2.12 in [12]). In particular

$$M \in \{N, N/\ell\}.$$

Assume that $M \neq N$, then $N = M\ell$ and $\ell \neq 2$ since E has good reduction at 2. Theorem 3.2.5 (or Tate's p-adic uniformization) says that $E[\ell]|_{G_\ell}$ is reducible. In particular

$$E[\ell]|_{G_\ell} \simeq \bar{\rho}_{f,\mathfrak{l}}|_{G_\ell} \simeq \begin{pmatrix} \omega_\ell \lambda_{a_\ell(f)^{-1}} & * \\ & \lambda_{a_\ell(f)} \end{pmatrix}$$

with $*$ 'peu ramifié'. This together with Proposition 8.2 of [20] and Proposition 2.12 of [12] leads to a contradiction. □

Remarks 3.6.6.

- *Condition (iii) is equivalent to N being odd and square-free.*
- *The rational elliptic curve of conductor 43 satisfies conditions $(i) - (iv)$.*

3.7 An application: safe chains

When considering safe chains as in [16] (Steinberg) level-raising at an appropriate (small) prime is a useful tool. In particular, this combined with a standard modular congruence gives an alternative way of introducing a "MGD" prime to the level. Having a MGD prime in the level is one of the key ingredients in a safe chain. Therefore, one could expect to use generalizations of Theorem 3.1.1 to build safe chains in more general settings. In the process of doing so one can rely on tools as in [19] to ensure that the condition **(*AbsIrr*)** holds when required. Also, most modularity lifting theorems require an absolute irreducibility condition; in particular for applications to nonsolvable base change this condition is necessary to all modularity lifting theorems available, this justifies **(*AbsIrr*)** condition, see 3.2.11.

Chapter 4

Fermat equation with coefficients

Let p be a rational prime and consider the degree p Fermat equation

$$x^p + y^p + z^p = 0. \tag{4.0.1}$$

The group $\mathbb{Q}^\times$ acts on the set of rational solutions of 4.0.1 by

$$\lambda(x, y, z) = (\lambda x, \lambda y, \lambda z), \qquad \lambda \in \mathbb{Q}^\times.$$

That allows us to consider solutions in the rational projective plane

$$\mathbb{P}_2(\mathbb{Q}) = (\mathbb{Q}^3 \setminus \mathbf{0})/\mathbb{Q}^\times,$$

That is, equation 4.0.1 defines a projective plane curve F_p in $\mathbb{P}_2$.

By the *genus-degree* formula F_p has genus

$$g_p = (p-1)(p-2)/2.$$

Faltings' theorem [21] states that the set $F_p(\mathbb{Q})$ of $\mathbb{Q}$-rational points of F_p is finite if $g_p \geq 2$. Genus 0 and genus 1 curves, corresponding to $p = 2$ and $p = 3$ respectively, might have infinitely many rational points. Since the main theorem in this chapter is to prove a finiteness property we shall avoid the case $p \leq 3$.

Fermat's last Theorem predicted that

$$F := \bigcup_{p \geq 5} F_p(\mathbb{Q}) = \{[1 : -1 : 0], [1 : 0 : -1], [0 : 1 : -1]\}.$$

In this chapter we are interested in the finiteness of F and we shall generalize it to Fermat equations with coefficients. Let a, b, c non-zero integers and let $F_p^{a,b,c}$ denote the projective curve given by

$$ax^p + by^p + cz^p = 0.$$

The Asymptotic Fermat Conjecture with coefficients a, b, c predicts that

Conjecture 4.0.1. *The set*

$$AF_{a,b,c} := \bigcup_{p \geq 5} F_p^{a,b,c}(\mathbb{Q})$$

is finite.

It is straightforward to see that the set of *trivial points* in $AF_{a,b,c}$, i.e. points $[x : y : z]$ satisfying $xyz = 0$, is finite.

The very first non-trivial evidence of conjecture 4.0.1 was stablished by Andrew Wiles when proving Taniyama-Shimura conjecture for the semistable case and hence proving case $a = b = c = 1$.

Theorem 4.0.2 (Wiles, [63])**.**

$$AF_{1,1,1} = \{[1 : 0 : -1], [1 : -1 : 0], [0 : 1 : -1]\}.$$

Remark 4.0.3. *Case $p = 3$ of Fermat last Theorem was proved by Leonhard Euler.*

Jean-Pierre Serre, Barry Mazur and Gerhard Frey had previously stablished some cases of the conjecture, conditionally on Serre's conjecture or Taniyama-Shimura conjecture; both proved now.

Theorem 4.0.4 (Serre,[50])**.** *Let n a non-negative integer and let q be a prime in*

$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}.$$

Then

$$AF_{1,1,q^n} \subseteq F_5^{1,1,q^n}(\mathbb{Q}) \cup F_7^{1,1,q^n}(\mathbb{Q}) \cup F_q^{1,1q^n}(\mathbb{Q}) \cup \{\textit{trivial points}\}.$$

Theorem 4.0.5 (Frey-Mazur, [23]). *Let q an odd prime which is neither a Mersenne prime nor a Fermat prime, let n be a positive integer and m a non-negative integer. Then*

$$AF_{1,q^n,2^m} \qquad \textit{is finite.}$$

Kenneth Ribet, for the case $2 \leq m < p$, and Henri Darmon, Loïc Merel, for the case $m = 1$ studied equation $X^p + Y^p + 2^m Z^p = 0$. In particular they proved that

Theorem 4.0.6 (Ribet [47], Darmon-Merel, [13]).

$$AF_{1,1,2^m} = \{[1 : -1 : 0]\} \cup \{[2^r : 2^r : -1] \mid m = rp + 1 \textit{ for } p \geq 5\}.$$

For a non-zero integer N let $\mathrm{rad}(N)$ denote the greatest square-free divisor of N. Let $\mathbf{P}$ denote the set of prime numbers. We can and will identify the image of $\mathrm{rad} : \mathbb{Z} \setminus \{0\} \to \mathbb{N}$ with the set of finite subsets of $\mathbf{P}$. In particular the *radical* of ± 1 corresponds to the empty set under that identification. Similarly $\mathrm{rad}'(N)$ will denote the greatest odd square-free divisor of N.

Alain Kraus has given effective bounds related to the Asymptotic Fermat conjecture and proved the following.

Theorem 4.0.7 (Kraus, [27]). *Let (a, b, c) be non-zero pairwise co-prime integers such that $\mathrm{rad}(abc) = 2q$ for an odd prime q which is neither a Mersenne prime nor a Fermat prime. Then there is an explicit constant $G = G(a, b, c)$ such that*

$$AF_{a,b,c} = \{\textit{trivial points}\} \cup \bigcup_{5 \leq p < G} F_p^{a,b,c}(\mathbb{Q}).$$

Remark 4.0.8. *Case $(a, b, c) = (1, 1, 2^\alpha q^\beta)$ is not explicitly stated in Kraus' paper. Nonetheless the same method applies to case $(1, 2^\alpha, q^\beta)$.*

Related to this conjecture Nuno Freitas, Emmanuel Halberstadt and Alain Kraus, have recently developed the so-called *symplectic method* to solve Fermat equations for a positive density of exponents p, see [22] or [24]. Our approach follows similar strategies as in [27] and relies strongly on modularity; see [9] chapter 15 for an exposition of the modular method written by Samir Siksek and Theorem 15.5.3 therein for an improvement of Serre's Theorem, 4.0.4.

In this chapter we exhibit non-trivial local obstructions[1] to some S-unit equations and we deduce results as the following. Let (a, b, c) a primitive tern, i.e. $gcd(a, b, c) = 1$, of non-zero integers.

Theorem 4.0.9. *Assume that* $\mathrm{rad}(abc)$ *is a product of primes all in* $1 + 12\mathbb{Z}$ *then* $AF_{a,b,2^r c}$ *is finite for every* $r \geq 0$, $r \neq 1$.

Theorem 4.0.10. *Assume that* $\mathrm{rad}(abc)$ *is a product of primes all in* $1 + 3\mathbb{Z}$ *then* $AF_{a,b,16c}$ *is finite.*

We also consider some particular cases with $\mathrm{rad}(abc) = q\ell$, for different odd primes q, ℓ. For example

Theorem 4.0.11. *Let* q, $\ell \geq 5$ *be primes such that* $q \equiv -\ell \equiv 5 \pmod{24}$. *If* $\mathrm{rad}(abc) = q\ell$ *then,* $AF_{a,b,c}$ *is finite.*

See section 4.5 for the complete list of cases we consider.

Remark 4.0.12. *We use Kraus method to deduce explicit bounds* $G(a, b, c)$ *on* p, *see 4.6.*

4.1 Fermat-type curves

Let $a, b, c \in \mathbb{Z}$, p prime, $abc \neq 0$. By a Fermat-type curve we mean a projective plane curve of the form

$$F_p^{a,b,c} : ax^p + by^p + cz^p = 0.$$

Fermat-Type curves share some geometric properties with the classical ones $x^p + y^p + z^p = 0$.

Notice that $F_p^{a,b,c}$ is non-singular if and only if $abc \neq 0$.

Theorem 4.1.1 (Faltings, [21])**.** *Let* $C/\mathbb{Q}$ *be a projective curve of genus* ≥ 2. *Then* $C(\mathbb{Q})$ *is finite.*

By the genus-degree formula one has that $F_p^{abc}/\mathbb{Q}$ has genus

$$(p - 1)(p - 2)/2.$$

[1] We shall use the terminology *non-trivial local obstructions* to distinguish from the ones introduced in Proposition 4.1.2.

This is a consequence of Hurwitz theorem, [53, II, 5.9].[2]

Thus $F_p^{a,b,c}(\mathbb{Q})$ is finite for $p \geq 5$. The sets $F_2^{a,b,c}(\mathbb{Q})$, $F_3^{a,b,c}(\mathbb{Q})$ might be infinite[3]. Let us fix a, b, c and consider the set $AF_{a,b,c}$ defined in 4.0.1.

Proposition 4.1.2. *Assume that there is a prime ℓ such that $v_\ell(a)$, $v_\ell(b)$, $v_\ell(c)$ are pairwise different. Then $AF_{a,b,c}$ is finite.*

Proof. Let us see that

$$F_p^{a,b,c}(\mathbb{Q}) = \emptyset$$

for every $p > k := \max_{q \text{ prime}} v_q(abc)$. Indeed, let $[x : y : z] \in AF_{a,b,c}$ and $(A, B, C) = (ax^p, by^p, cz^p)$. Then $A + B + C = 0$ and $v_\ell(A) \leq v_\ell(B) \leq v_\ell(C) \leq \infty$ for some permutation of A, B, C. Thus $v_\ell(B) = v_\ell(A)$ since $v_\ell(B) = v_\ell(A + C) \geq v_\ell(A)$. Thus $v_\ell(b) = v_\ell(c)$ since $v_\ell(b) \equiv v_\ell(B) = v_\ell(C) \equiv v_\ell(c) \pmod{p}$.

Hence

$$AF_{a,b,c} = \bigcup_{p \leq k} F_p^{a,b,c}(\mathbb{Q})$$

is finite by Faltings. □

We say that a tern a, b, c has a *trivial local obstruction* if there is a prime q such that $v_q(a)$, $v_q(b)$, $v_q(c)$ are pairwise different. Thus, we shall focus on terns with no trivial obstruction. We make the following hypothesis.

(*F*) : The tern (a, b, c) has no trival local obstruction and $gcd(a, b, c) = 1$.

Notice that a, b, c satisfies **(*F*)** if a, b, c are pairwise coprime.

Lemma 4.1.3. *Let a, b, c be a tern satisfying* **(*F*)** *and let p be a prime such that*

$$p > \max_{q \text{ prime}} \max(v_q(a), v_q(b), v_q(c)).$$

Then there are pairwise coprime integers α, β, γ such that $\mathrm{rad}(\alpha\beta\gamma) = \mathrm{rad}(abc)$ *and*

$$F_p^{a,b,c} \simeq F_p^{\alpha,\beta,\gamma}$$

[2] Consider the degree p morphism $\phi : F_p^{a,b,c} \to \mathbb{P}_1$, $[x : y : z] \mapsto [x : y]$. It is ramified at p points with constant ramification index p.

[3] The set $F_2^{a,b,c}(\mathbb{Q})$ is infinite if and only if it is not empty. If $\mathcal{O} \in F_3^{a,b,c}(\mathbb{Q})$ then $(F_3^{a,b,c}, \mathcal{O})$ is an elliptic curve over $\mathbb{Q}$ and $F_3^{a,b,c}(\mathbb{Q})$ is a finitely generated group.

as algebraic curves over $\mathbb{Q}$.

Proof. Let a, b, c be non-zero integers satisfying **(F)** and let

$$\begin{aligned} T_a &= gcd(b, c), \\ T_b &= gcd(a, c), \\ T_c &= gcd(a, b). \end{aligned}$$

Then there are integers a', b', c' such that $a', b', c', T_a, T_b, T_c$ are pairwise coprime and

$$\begin{array}{lllll} a = a' & T_b & T_c, \\ b = b' & T_a & T_c, \\ c = c' & T_a & T_b. \end{array}$$

The Lemma follows by an induction on the number of prime divisors of $T_aT_bT_c$. If $T_aT_bT_c = 1$ we are done. So assume that $q^e \parallel T_a$ with $1 \leq e < p$. Then the map $F_p^{a_1,b_1,c_1} \to F_p^{a,b,c}$, $[x : y : z] \mapsto [qx : y : z]$ is an isomorphism, where $q^e(a_1, b_1, c_1) = (q^p a, b, c)$. Hence

$$\begin{array}{rcl} T_{a_1} & = & T_a/q^e, \\ T_{b_1} & = & T_b, \\ T_{c_1} & = & T_c. \end{array}$$

and $\mathrm{rad}(a_1b_1c_1) = \mathrm{rad}(abc)$.

□

Remark 4.1.4. *With the notation above one has that* $v_q(\alpha\beta\gamma) = v_q(abc)$ *if* $q \nmid T_aT_bT_c$ *and* $v_q(\alpha\beta\gamma) = p - v_q(abc)/2 = p - v_q(T_aT_bT_c)$ *otherwise.*

4.2 S-unit equations

Let S be a finite set of primes. We identify S with its product in $\mathbb{Z}$. Let a, b, c be non-zero integers and consider the projective line $L : aX + bY + cZ = 0$ attached to it. The set

$$L(\mathbb{Q}) = \{[x : y : z] \in \mathbb{P}^2(\mathbb{Q}) : L(x, y, z) = 0\}$$

of rational points of L is infinite.

Definition 4.2.1. *Let $P \in L(\mathbb{Q})$ and let $(x, y, z) \in \mathbb{Z}^3$ be a primitive representative of P, that is $gcd(x, y, z) = 1$. We say that P is an S-point of L if $xyz \neq 0$ and $\mathrm{rad}(xyz) \mid S$. We say that P is a proper S-point if $\mathrm{rad}(xyz) = S$.*

Theorem 4.2.2 (Siegel-Mahler)**.** *Let a, b, c non-zero integers and let S be a finite set of prime numbers. The set of S-points in the line*

$$aX + bY + cZ = 0$$

is finite.

Proof (Lang, [29]). S-points of the line correspond to points of the affine curve $C : aX + bY + c = 0$ with values in

$$\Gamma = \mathbb{Z}[1/N]^\times < \mathbb{Q}^\times, \qquad N = \prod_{p \in S} p.$$

The set S together with -1 generate the abelian group Γ, hence Γ/Γ^5 is finite. If C has infinitely many points with coefficients in Γ, then infinitely many points $\{(x_i, y_i)\}_{i \geq 1}$ coincide mod Γ^5. Thus the curve $ax_1X^5 + by_1Y^5 + c = 0$ has infinitely many rational points and it has genus 6 since $ax_1by_1c \neq 0$. This contradicts Faltings theorem. □

We shall restrict our attention to the projective line

$$L_0 : X + Y + Z = 0.$$

Frey-Kraus-Mazur method on the Asymptotic Fermat Conjecture with coefficients (a, b, c) considers the set of primes $S = \mathrm{rad}(2abc)$ and seeks for S-unit points of L_0. The 2-adic valuation of S-unit points will play an important role. We say that a point $P \in L_0(\mathbb{Q})$ has *height* $r = h_2(P)$ if $v_2(xyz) = r$, for a primitive representative $(x, y, z) \in \mathbb{Z}^3$ of P.[4]

One has that

- $h_2(P) \geq 1$ for every $P \in L_0(\mathbb{Q})$.
- $h_2(P) = \infty$ if and only if $P \in \{[1 : -1 : 0], [1 : 0 : -1], [0 : 1 : -1]\}$.

[4] We follow the usual convention that $v_2(0) = \infty$.

In particular L_0 has no S-unit points if $2 \notin S$.

Example 4.2.3. *For $S = 2$ the S-unit points of L_0 are $[2 : -1 : -1]$ up to permutation of coordinates.*

Proposition 4.2.4. *Let q be an odd prime and let $S = 2q$. Then the set of proper S-points of $X + Y + Z = 0$ is*

- $\{[9 : -8 : -1], [3 : -2 : -1], [3 : -4 : 1]\}$, *if $q = 3$,*
- $\{[q : -2^n : -1]\}$ *with height a power of 2, if q is a Fermat prime ≥ 5,*
- $\{[q : -2^n : +1]\}$ *with prime height, if q is a Mersenne prime ≥ 7,*
- $\emptyset$, *otherwise,*

up to permutation of coordinates.

Proof. Let (x, y, z) be a primitive representative of a proper S-point. Then x, y, z are non-zero pairwise coprime integers We may assume without loss of generality that $x = q^m, y = -2^n, z = \pm 1$, $m, n \geq 1$. By Theorem 1.4.8 one has that either $q = n = 3$ and $m = 2$ or $m = 1$. We deduce that case $q = 3$ has 3 points. Case $m = 1$, $q \geq 5$ implies that either $q = 2^n + 1$ is a Fermat prime and n is a power of 2 or $q = 2^n - 1$ is a Mersenne prime and n is prime. Notice that 3 is the only prime being Fermat and Mersenne. □

The method we use to prove new cases of Conjecture 4.0.1 relies on finding pairs (S, H) such that

- S is a set of primes containing 2,
- H is a set of non-negative integers to be defined and
- there is no proper S-unit point of height $h_2 \in H$ in $X+Y+Z = 0$.

In the following subsections we exhibit infinite families of such pairs.

4.2.1 $S = 2q\ell$

Let q, ℓ be odd primes. In this subsection we deal with equations of the form

$$\begin{array}{rcrcl} 2^r q^s & = & \ell^t & \pm & 1 \\ 2^r & = & q^s \ell^t & \pm & 1 \\ 2^r & = & q^s & \pm & \ell^t \end{array}$$

The first equation is quite restrictive.

Proposition 4.2.5. *Let ℓ, q be odd primes and assume that*

$$2^r q^s = \ell^{2t} - 1$$

for some positive integers r, s, t. The solutions are

$$\begin{aligned} 2^4 \cdot 5 &= 3^4 - 1 \\ 2^3 \cdot 3 &= 5^2 - 1, \\ 2^4 \cdot 3 &= 7^2 - 1, \\ 2^5 \cdot 3 &= 17^2 - 1. \end{aligned}$$

Proof. Notice that $3 \mid \ell q$ since either $\ell \mid 3$ or $3 \mid \ell^{2t} - 1 = 2^r q^s$.

Let r, s, t, q, ℓ be a solution. If $\ell = 3$ then $\sigma(2t) \leq 3$. Hence $t \in \{1, 2\}$ with solutions $3^2 - 1 = 2^3$, $3^4 - 1 = 2^4 \cdot 5$. The case $3^2 - 1 = 2^3$ is not allowed.

If $\ell \neq 3$ then $q = 3$, $t = 1$. The integers $\ell + 1$, $\ell - 1$ are consecutive even numbers and $gcd(\ell + 1, \ell - 1) = 2$. Case $\ell \pm 1 = 2^{r-1} \cdot 3^s$, $\ell \mp 1 = 2$ is not possible since $\ell \geq 5$. So assume

$$\begin{aligned} \ell + \varepsilon &= 2 \cdot 3^s \\ \ell - \varepsilon &= 2^{r-1} \end{aligned}$$

for some unit ε. Then $3^s - 2^{r-2} = \varepsilon$ with solutions $3^2 - 2^3 = 1$, $3 - 2 = 1$, $3 - 2^2 = -1$. Hence $\ell \in \{17, 5, 7\}$. □

Proposition 4.2.6. *Let ℓ, q be odd primes and assume that*

$$2^r q^s = \ell^t - 1$$

for some positive integers r, s, $t \geq 3$ odd. Then t is prime, $\Phi_1(\ell) = \ell - 1 = 2^r$ and $\Phi_t(\ell) = q^s$. Hence ℓ is a Fermat prime.

Proof. The integer t is prime since $2 \leq \sigma(t) \leq \omega(\ell^t - 1) = 2$. Thus

$$2^r q^s = (\ell - 1)\Phi_t(\ell).$$

Notice that $\Phi_t(\ell)$ is odd and has a prime divisor coprime to $2t$, then $q \mid \Phi_t(\ell)$ and $q \neq t$. Notice that the greatest common divisor of $\ell - 1$ and $\Phi_t(\ell)$ divides t. Hence $\ell - 1$ and $\Phi_t(\ell)$ are coprime. □

Proposition 4.2.7. *Let ℓ, q be odd primes and assume that*

$$2^r q^s = \ell^{2t} + 1$$

for some positive integers r, s, t. Then $r = 1$ and $2t = 2^m$ for some $m \geq 1$ and $2^{m+1} \mid q - 1$.

Proof. Let $2t = 2^m t_2$, t_2 odd. Then

$$X^{2t} + 1 = \prod_{d \mid t_2} \Phi_{2^{m+1}d}$$

and by Theorem 1.4.5 $\ell^{2t} + 1$ has $\sigma(t_2)$ odd prime divisors, at least. Thus $t_2 = 1$. In particular ℓ has order 2^{m+1} in $\mathbb{F}_q^\times$. Notice that $\ell^{2^m} + 1 \equiv 2 \pmod 4$ thus $r = 1$. □

Let $n \geq 2$ be an integer. The equation $2X^n - 1 = Z^2$ was studied by Carl Störmer in [58, Section 3]. He proved that either n is a power of two or $X = Z = 1$ is the only solution in $\mathbb{Z}$. See also [44, A11.1].

Theorem 4.2.8. *Assume that there are odd primes ℓ, q such that*

$$2^r q^s = \ell^{2t} + 1$$

for integers $r, s, t \geq 1$. Then $r = 1$ and either

- $s = 1$ *and* $q = \dfrac{\ell^{2t} + 1}{2}$, *or*
- $(q, \ell) = (13, 239)$, *or*
- $s = 2, t = 1$.

Proof. We have already seen that r is necessarily 1. Case $s = 1$ has many solutions. Assume $s \geq 2$. Then s, $2t$ are powers of two due to Störmer's result and Proposition 4.2.7. The curve $2x^4 = y^2 + 1$ has two positive integer solutions $(1, 1)$ and $(13, 239)$ due to [33] or [57]. The curve $2x^2 = y^4 + 1$ is a genus one curve with Jacobian variety isomorphic to the elliptic curve $E : y^2 = x^3 - x$. The Mordell - Weil group $E(\mathbb{Q})$ of E consists in its two-torsion. See for example elliptic curves over $\mathbb{Q}$ in [36] with Cremona Label 32a2. Professor Marc Masdeu helped us with some computations and concluded that $2x^2 = y^4 + 1$ has a unique positive rational point, $(1, 1)$.

Thus equation $2q^{2^n} = \ell^{2^m}$ has only solution $(13, 239)$ for $mn \geq 2$. □

Proposition 4.2.9. *Let ℓ, q be odd primes and assume that*

$$2^r q^s = \ell^t + 1$$

for some positive integers r, s and $t \geq 3$ odd. Then t is prime, $\ell + 1 = 2^r$ and $\Phi_{2t}(\ell) = q^s$. Hence ℓ is a Mersenne prime.

Proof. The integer t is prime since $2 \leq \sigma(t) \leq \omega(\ell^t + 1) = 2$. Thus

$$2^r q^s = (\ell + 1)\Phi_{2t}(\ell).$$

One proves as in 4.2.6 that $\Phi_{2t}(\ell)$ and $\ell + 1$ are coprime. Notice that $\Phi_{2t}(\ell)$ is odd. □

Remark 4.2.10. *Let q, ℓ be odd primes and assume that ℓ is neither a Fermat prime nor a Mersenne prime. One deduces from previous statements an algorithm to determine whether there are solutions to the equation $2^r q^s = \ell^t + \varepsilon$. Indeed, case $t = 1$ or $s = 1$ is easy to deal with. Assume that $s, t \geq 2$. Cases $\varepsilon = -1$ and $(\varepsilon, t) = (1, odd)$ imply ℓ Mersenne or Fermat. Assume $\varepsilon = 1$, t even. One deduces from Theorem 4.2.8 that either $(q, \ell) = (13, 239)$ or $s = t = 2$ and $r = 1$. One needs at most 5 arithmetic operations to check whether $2q^2 = \ell^2 + 1$. Some computations suggest that the set of primes (q, ℓ) satisfying equation $2q^2 = \ell^2 + 1$ has zero density.*

Remark 4.2.11. *Let $p_1 < \cdots < p_n$ be prime numbers and let N an integer. One can determine whether $\mathrm{rad}(N) = p_1 \cdots p_n$ in $\log_{p_1} N$ integer divisions.*

There are indeed solutions to equation $2^r q^s = \ell^t \pm 1$.

Examples 4.2.12.

- $2 \cdot 11^2 = 3^5 - 1$.
- $2 \cdot 5^2 = 7^2 + 1$.
- $2 \cdot 29^2 = 41^2 + 1$.
- $2 \cdot 13^4 = 239^2 + 1$.
- $\Phi_5(3) = 11^2$ *and* $2\,\Phi_5(3) = 3^5 - 1$.
- $\Phi_7(5)$ *is prime and* $2^2 \cdot \Phi_7(5) = 5^7 - 1$.
- $\Phi_{34}(7)$ *is prime and* $2^3 \cdot \Phi_{34}(7) = 7^{17} + 1$.

The solutions to equation $\ell^{2^m} - 2q^{2^n} = -1$, $m, n \geq 1$ are easily related with the units in $A = \mathbb{Z}[\sqrt{2}]$. We have iterated the powers of the fundamental unit $1 + \sqrt{2}$ of A to find examples.

We finish this subsection with a general statement about S-unit equations for $|S| = 3$.

Lemma 4.2.13. *Let q, $\ell \geq 5$ be primes. Assume one of the following:*

1. $q \equiv 3 \pmod 8$, $\ell \equiv 5 \pmod 8$ *and* $q \equiv -\ell \pmod 3$.
2. $q \equiv 11 \pmod{24}$, $\ell \equiv 5 \pmod{24}$ *and* $\left(\frac{q}{\ell}\right) = -1$.
3. $q \equiv \pm 3 \pmod 8$, $\ell \equiv -1 \pmod{24}$, $\ell \not\equiv -1 \pmod q$.

Let S be $2q\ell$. The S-unit equation

$$X + Y + Z$$

has no proper points of height ≥ 3.

Proof. This a mod 24 exercise. See section 4.8. □

4.2.2 Large $|S|$

Lemma 4.2.14 ($h_2 = 4$)**.** *Let S be a finite set of primes in $1 + 3\mathbb{Z}$. Then L_0 has no proper $2S$-unit point of height 4.*

Proof. Let (A, B, C) be a proper $2S$-unit point of height 4 and let $\varepsilon_A, \varepsilon_B, \varepsilon_C$ the sign of A, B, C, respectively. Hence $\mathrm{rad}(ABC) = 2S$ and

$$0 = A + B + C \equiv \varepsilon_A + \varepsilon_Y + \varepsilon_C \pmod 3.$$

Hence $(\varepsilon_A, \varepsilon_B, \varepsilon_C) = \pm(1, 1, 1)$ and $A+B+C$ is either strictly positive or strictly negative. □

Lemma 4.2.15 ($h_2 = 4$)**.** *Let n be a positive integer not dividing 14, 16 nor 18 and let S be a finite set of primes in $\pm 1 + n\mathbb{Z}$. Then L_0 has no proper $2S$-unit point of height 4.*

Proof. Let (A, B, C) be a proper point of height 4. Say $A = 2^4 A'$, then $\mathrm{rad}(A'BC) = S$ and $A', B, C \equiv \pm 1 \pmod n$. Thus

$$0 = A + B + C \equiv \pm 16 \pm 1 \pm 1 \pmod n.$$

Hence $n \mid 14, 16$ or 18. □

Lemma 4.2.16 ($h_2 \geq 2$)**.** *Let p an odd prime. Let S be a finite set of primes in $1+4p\mathbb{Z}$. Then L_0 has no proper $2S$-unit point of height ≥ 2.*

Proof. Let (A, B, C) a proper point. Say

$$\begin{array}{rcll} A & = & \varepsilon_A & A' \quad 2^r \\ B & = & \varepsilon_B & B' \\ C & = & \varepsilon_C & C' \end{array}$$

for $r \geq 2$ and $\varepsilon_x = \operatorname{sign} x$. Then $A' \equiv B' \equiv C' \equiv 1 \pmod{4p}$ and

$$0 = A + B + C \equiv 2^r \varepsilon_A + \varepsilon_B + \varepsilon_C \pmod{4p}.$$

Thus $\varepsilon_B \equiv -\varepsilon_C \pmod 4$ and $2^r \varepsilon_A + \varepsilon_B + \varepsilon_C \equiv 0 \pmod p$. Then $\varepsilon_B = -\varepsilon_C$ and $p \mid 2^r$. □

4.3 Frey-Kraus-Mazur method

Let a, b, c be non-zero pairwise coprime integers and let

$$p > \max\left(4, \max_{q \text{ prime}} v_q(abc)\right) \tag{4.3.1}$$

be a prime. Assume that $F_p^{a,b,c}(\mathbb{Q})$ has a non-trivial point P and let (x, y, z) be a primitive tern of non-zero integers such that $[x : y : z] = P$. That is, $xyz \neq 0$, $gcd(x, y, z) = 1$ and

$$ax^p + by^p + cz^p = 0.$$

Notice that $(A, B, C) = (ax^p, by^p, cz^p)$ are pairwise coprime integers.[5]

4.3.1 The Frey curve

Following the notation above consider the elliptic curve

$$E = E_{A,B,C} : Y^2 = X(X - A)(X + B)$$

over $\mathbb{Q}$. The definition of $E_{A,B,C}$ is sensible to the order of (A, B, C). More precisely, the curve $E_{A,B,C}$ is a twist of $E_{B,A,C}$ by the quadratic twist of $\mathbb{Q}(i)/\mathbb{Q}$ while even permutations of (A, B, C) define $\mathbb{Q}$-isomorphic elliptic curves. Hence $E_{A,B,C}$, $E_{B,A,C}$ have common prime-to-2 conductor. Let us reorder (A, B, C) so that E has minimal conductor exponent over $\mathbb{Q}_2$.[6]

Proposition 4.3.1. *E has conductor $2^r \operatorname{rad}'(abcxyz)$ where*

$$r = \begin{cases} 1 & \text{if } xyz \text{ is even or } v_2(abc) \geq 5, \\ 0 & \text{if } xyz \text{ is odd and } v_2(abc) = 4, \\ 3 & \text{if } xyz \text{ is odd and } v_2(abc) \in \{2, 3\}, \\ 5 & \text{if } xyz \text{ is odd and } v_2(abc) = 1. \end{cases}$$

Proof. The elliptic curve E has semi-stable reduction at every odd prime since A, B, C are pairwise coprime. Let ℓ be an odd prime, then E has bad reduction over $\mathbb{Q}_\ell$ if and only if $\ell \mid ABC$. Thus, E

[5] Indeed, if $q \mid x, y$ then $q^p \mid c$ and $p \leq v_q(c) \leq v_q(abc)$.

[6] For example one can take B even and $A \equiv -1 \pmod 4$.

has prime-to-2 conductor $\mathrm{rad}'(ABC) = \mathrm{rad}'(xyzabc)$ by Neron-Ogg-Shafarevich. The conductor exponent E over $\mathbb{Q}_2$ has been computed in [14, Lemma 2]. If xyz is even then $v_2(ABC) \geq pv_2(xyz) \geq p > 4$ by hypothesis, thus $r = 1$. □

Notice that $v_2(abc) = 0$ implies xyz even.

Lemma 4.3.2. *The Galois representation*

$$\bar{\rho}_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

is irreducible.

Proof. Recall that $p \geq 5$ by assumption 4.3.1. The irreducibility condition is proved in Serre's paper [50, Proposition 6] for the semistable case, i.e. $r \leq 1$. Serre's proof relies on Mazur's theorem [38, Theorem 2].

Let us prove irreducibility for $r \in \{3, 5\}$. Consider the local Galois representation

$$\rho_{E,p}|_{G_2} : \mathrm{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2) \to Aut(\mathcal{T}_p(E))$$

and the residual representation

$$\bar{\rho}_{E,p}|_{G_2} : \mathrm{Gal}(\bar{\mathbb{Q}}_2/\mathbb{Q}_2) \to Aut(E[p]).$$

The conductor of $\rho_{E,p}|_{G_2}$ is larger than or equal to the conductor of $\bar{\rho}_{E,p}|_{G_2}$. Henri Carayol computed in [8] the cases where the inequality is strict. See the discussion in page 789 and Proposition 2 therein. Since $\rho_{E,p}|_{G_2}$ has unramified determinant and $r \geq 3$ one deduces that $\rho_{E,p}|_{G_2}, \bar{\rho}_{E,p}|_{G_2}$ have common conductor 2^r. Assume that $\bar{\rho}_{E,p}$ is reducible then

$$\bar{\rho}_{E,p}|_{G_2} \simeq \begin{pmatrix} \chi_1 & * \\ & \chi_2 \end{pmatrix}$$

with $\chi_1\chi_2$ being the (unramified) mod p cyclotomic character. Thus χ_1, χ_2 have common conductor. The Swan conductor is invariant under semisimplification. Thus, the Swan conductor of $\bar{\rho}_{E,p}|_{G_2}$ coincides with the Swan conductor of $\chi_1 \oplus \chi_2$. That is, either χ_1, χ_2 are unramified and $\bar{\rho}_{E,p}|_{G_2}$ has conductor ≤ 1 or χ_1, χ_2 are ramified with common Swan conductor m. In the last case one has that $\bar{\rho}_{E,p}|_{G_2}$ has even conductor exponent $r = \dim_{\mathbb{F}_p} E[p] - \dim_{\mathbb{F}_p} E[p]^{I_2} + 2m = 2 + 2m$. □

4.3.2 Lowering the level

We shall lower the level of E via $E[p]$. The standard reference here is Ribet's level lowering theorem, [46]. Let us recall some notation therein. Let $\bar{\rho} := E[p]$ be the mod p irreducible representation attached to E. Then $\bar{\rho}$ is modular of level $N = 2^r \operatorname{rad}'(abcxyz)$ by Wiles [63], see also [14]. Let ℓ be a prime divisor of N, $\ell \parallel N$. The representation $\bar{\rho}$ is finite at ℓ if some geometric condition is satisfied.[7] For the case of modular elliptic curves that condition has a pleasant equivalence.

Lemma 4.3.3. *Let p be a prime, let E' be an elliptic curve over $\mathbb{Q}$ of conductor N' and let $\ell \parallel N'$ be a prime. Then $E'[p]$ is finite at ℓ if and only if $p \mid v_\ell(j_{E'})$. If $p \neq \ell$ then $E'[p]$ is finite at ℓ if and only if $E'[p]$ is unramified at ℓ.*

Proof. The lemma is a consequence of Tate's uniformization for multiplicative reduction elliptic curves over $\mathbb{Q}_\ell$. See [12, 2.12] and [20, 8.2]. □

Let s be the conductor exponent of $E[p]$ at 2, $s \leq r$. If $r \in \{0, 3, 5\}$ then $s = r$. If $r = 1$ then s is ruled by Tate's uniformization. That is, $s = 0$ if and only if $v_2(abc) = 4$.

Theorem 4.3.4. *Following the notation above, let*

$$\bar{\rho} : \operatorname{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{F}_p)$$

be the Galois representation attached to the p-torsion of $E = E_{A,B,C}$. There is a newform $f \in S_2(2^s \operatorname{rad}'(abc))$ whose mod p Galois representation is isomorphic to $\bar{\rho}$.

Proof. Let ℓ be an odd prime divisor of $\operatorname{rad}'(abcxyz)$. Then $E[p]$ is finite at ℓ if and only if $\ell \nmid abc$. Indeed,

$$j_E = \frac{2^8(C^2 - AB)^3}{A^2B^2C^2}$$

and $v_\ell(j_E) = -2v_\ell(abc) - 2pv_\ell(xyz)$. Thus $p \mid v_\ell(j_E)$ if and only if

$$p \mid v_\ell(abc).$$

[7] More precisely, $\bar{\rho}$ is finite at ℓ if there is a finite flat $\mathbb{F}_p$-vector space scheme H over $\mathbb{Z}_\ell$ such that $H(\bar{\mathbb{Q}}_\ell)$ is isomorphic to $\bar{\rho}|_{G_\ell}$ as $\mathbb{F}_p[G_\ell]$-modules.

Recall that $p > v_\ell(abc)$ by assumption 4.3.1. Thus $E[p]$ is finite at an odd prime ℓ if and only if $\ell \nmid abc$.

Ribet's level lowering Theorem states that $\bar{\rho}$ is modular of level $2^s \operatorname{rad}'(abc)$. I.e., there is a newform in $S_2(M)$, for some $M \mid 2^s \operatorname{rad}'(abc)$, and a prime $\mathfrak{p} \ni p$ such that $\bar{\rho}_{f,\mathfrak{p}}$ and $\bar{\rho}$ are isomorphic. See 4.7 for a proof of the equality $M = 2^s \operatorname{rad}'(abc)$. □

The final step is to connect f with S-unit equations. Kraus method allows us to impose the following conditions.

- $[\mathbb{Q}_f : \mathbb{Q}] = 1$ so that f corresponds to an elliptic curve $E'/\mathbb{Q}$.
- E' has full rational 2-torsion.

Theorem 4.3.5. *There is a constant $H = H(\operatorname{rad}(abc), s)$ such that if $p > H$ then the newform described in Theorem 4.3.4 corresponds to an elliptic curve over $\mathbb{Q}$ with full rational 2-torsion (up to isogeny).*

Proof. See Théorème 3 and Théorème 4 in [27]. □

Notice that H depends on $[x : y : z]$ since r and s may vary from point to point. Nevertheless, one can still give a uniform bound depending only on a, b, c by taking $\max_s(H(\operatorname{rad}(abc), s))$.

Proposition 4.3.6. *Let N be a square-free odd integer and let $r \in \{0, 1, 3, 5\}$. The existence of a Frey Curve of conductor $2^r N$ is equivalent to the existence of a proper $2N$-unit point of height*

$$\begin{array}{cc} \geq 5 & \text{if } r = 1, \\ 4 & \text{if } r = 0, \\ 2 \text{ or } 3 & \text{if } r = 3, \\ 1 & \text{if } r = 5. \end{array}$$

Proof. The existence of a Frey curve attached to a $2N$-unit follows as in Proposition 4.3.1. For the other implication let

$$E : Y^2 = X(X - A)(X + B)$$

be a Frey curve of conductor $2^r N$, $A, B \in \mathbb{Z}$. There is a Frey curve

$$E' : Y^2 = X(X - a)(X + b)$$

twist of E such that a, b are coprime, $a \equiv -1 \mod 4$ and b is even. Mainly, the tern $(a, b, -a-b) \in \mathbb{Z}^3$ is a primitive representative of $[A : B : -A - B]$ up to permutation of coordinates. Let us see that (a, b, c) is a proper $2N$ point with the corresponding constrains on the height. The curve E' has conductor $2^{r'} rad'(ab(a+b))$ where

$$r' = \begin{cases} 0 & \text{if } v_2(b) = 4, \\ 1 & \text{if } v_2(b) \geq 5, \\ 3 & \text{if } v_2(b) = 2, 3, \\ 5 & \text{if } v_2(b) = 1 \end{cases}$$

as described in [14]. Thus, it is enough to prove that $r' = r$ and $N = rad'(ab(a+b))$. Let $g \in \mathbb{Z}$ square-free such that E is a twist of E' by the quadratic character attached to $\mathbb{Q}(\sqrt{g})$. Equivalently,

$$E \simeq E'' : Y^2 = X(X - ag)(X + bg).$$

This model of E'' is minimal over $\mathbb{Z}_p$ for every odd prime p. Thus E has additive reduction over every odd prime divisor of g. Since N is square-free one deduces that $g \in \{\pm 1, \pm 2\}$ and $N = rad'(ab(a+b))$. The conductor of E' over $\mathbb{Q}_2$ needs special consideration. If $r' \in \{0, 1, 3\}$ then E has conductor $r = 4$ if $g = -1$ and $r = 6$ if $g = \pm 2$. If $r' = 5$ then E has conductor $r = 5$ if $g = -1$ and $r = 6$ if $g = \pm 2$. The standard reference here is Tate's algorithm [60]. See also [3, Theorem 3.1] for a general statement on twists of newforms. See [61, Proposition 1] for the case where $\mathbb{Q}(\sqrt{g})$ is more deeply ramified than $\rho_{E',\ell}$, that is $g \in \{-1, \pm 2\}$ and $r' \leq 1$. Since $r \neq 4, 6$ by hypothesis one deduces that $r' = r$. □

4.4 Kraus Theorem

Theorem 4.4.1 (2-good)**.** *Assume that b is odd and $v_2(c) = 4$. Let $S = \mathrm{rad}(abc)$ and assume that there are no proper S-unit points of L_0 of height 4. Then there is a constant $G(a, b, c)$ such that*

$$AF_{a,b,c} \subseteq \bigcup_{5 \leq p \leq G(a,b,c)} F_p^{a,b,c} \cup \{\textit{trivial points}\}$$

Theorem 4.4.2 (2-node)**.** *Assume one of the following*

1. *bc is odd,*

2. *b is odd and $v_2(c) \geq 5$, or*

3. *$v_2(b) = v_2(c) \geq 1$.*

Let $S = \mathrm{rad}(2abc)$ and assume that there are no proper S-unit points of height ≥ 5. Then there is a constant $G(a,b,c)$ such that

$$AF_{a,b,c} \subseteq \bigcup_{5 \leq p \leq G(a,b,c)} F_p^{a,b,c} \cup \{\textit{trivial points}\}$$

Theorem 4.4.3. *Assume that b is odd and $v_2(c) \in \{2,3\}$. Assume that there are no proper S-unit points of height 2, 3 or ≥ 5 for $S = \mathrm{rad}(abc)$. Then there is a constant $G(a,b,c)$ such that*

$$AF_{a,b,c} \subseteq \bigcup_{5 \leq p \leq G(a,b,c)} F_p^{a,b,c} \cup \{\textit{trivial points}\}.$$

Theorem 4.4.4. *Assume that b odd, $v_2(c) = 1$ and let $S = \mathrm{rad}(abc)$. Assume that there are no proper S-unit points of height 1 or ≥ 5. Then there is a constant $G(a,b,c)$ such that*

$$AF_{a,b,c} \subseteq \bigcup_{5 \leq p \leq G(a,b,c)} F_p^{a,b,c} \cup \{\textit{trivial points}\}.$$

See 4.6 for a description of $G(a,b,c)$.

Proof. Assume that there is a prime $p > G(a,b,c)$ such that $F_p^{a,b,c}(\mathbb{Q})$ has non-trivial points. Let α, β, γ be pairwise coprime integers such that $F_p^{a,b,c} \simeq F_p^{\alpha,\beta,\gamma}$ and $\mathrm{rad}(abc) = \mathrm{rad}(\alpha\beta\gamma)$ and let (x,y,z) be a primitive representative of a non trivial point P in $F_p^{\alpha,\beta,\gamma}(\mathbb{Q})$. Let $(A,B,C) = (\alpha x^p, \beta y^p, \gamma z^p)$ and reorder (A,B,C) so that $E = E_{A,B,C}$ has minimal conductor. If b, c are both even then the choice of $G(a,b,c)$ ensures that $v_2(\alpha) \geq 5$, see remark 4.1.4. Otherwise, $v_2(\alpha\beta\gamma) = v_2(abc)$. The level lowering trick combined with the fact that p is large, see 4.3.5, implies that there is an elliptic curve E' over $\mathbb{Q}$ with full rational 2-torsion such that $E[p] = E'[p]$. Moreover E' has conductor

$2^s \operatorname{rad}'(abc)$ where

$$s = \begin{cases} 0 & \text{if } b \text{ is odd and } v_2(c) = 4, \\ 1 & \text{if } b, c \text{ have same parity}, \\ 1 & \text{if } b \text{ is odd, } v_2(c) \in \{1, 2, 3\} \text{ and } xyz \text{ is even}, \\ 3 & \text{if } b \text{ is odd, } v_2(c) \in \{2, 3\} \text{ and } xyz \text{ is odd}, \\ 5 & \text{if } b \text{ is odd, } v_2(c) = 1 \text{ and } xyz \text{ is odd}. \end{cases}$$

Thus $E' = E_{R,S,T}$ is a Frey curve, with $\operatorname{rad}(RST) = \operatorname{rad}(2abc)$. That is, there is a proper $\operatorname{rad}(2abc)$-unit point of height

$$\begin{cases} 1 & \text{if } s = 5, \\ 2 \text{ or } 3 & \text{if } s = 3, \\ 4 & \text{if } s = 0, \\ \geq 5 & \text{if } s = 1, \end{cases}$$

by Proposition 4.3.6. □

4.5 Statements

In this section we translate Lemmas 4.2.13, 4.2.14,4.2.15 and 4.2.16 to new cases of Asymptotic Fermat Conjecture with coefficients. Let (a, b, c) be a tern of non-zero integers satisfying $\boldsymbol{(F)}$, a odd.

Theorem 4.5.1. *Let S be a set of primes all in $1 + 3\mathbb{Z}$. and assume that $\operatorname{rad}(abc) = S$. Then the Fermat equation*

$$ax^p + by^p + 16cz^p = 0$$

has no solutions other than $xyz = 0$ for p larger than $G(a, b, 16c)$.

Proof. There are no proper $2S$-unit points of height 4 by Lemma 4.2.14. The theorem follows due to 4.4.1. □

Theorem 4.5.2. *Let n a positive integer not dividing $14, 16, 18$ and let S be a finite set of primes all in $(1 + n\mathbb{Z}) \cup (-1 + n\mathbb{Z})$. Assume $\operatorname{rad}(abc) = S$. Then the Fermat equation*

$$ax^p + by^p + 16cz^p = 0$$

has no solutions other than $xyz = 0$ for p larger than $G(a, b, 16c)$.

Proof. There are no proper $2S$-unit points of height 4 by Lemma 4.2.15. The theorem follows due to 4.4.1. □

Theorem 4.5.3. *Let q be an odd prime and let S be a finite set of primes all in $1+4q\mathbb{Z}$. Assume that either $\mathrm{rad}(abc) = S$ or $\mathrm{rad}(abc) = 2S$ and $v_2(bc) \geq 2$. Then the Fermat equation*

$$ax^p + by^p + cz^p = 0$$

has no solutions other than $xyz = 0$ for p larger than $G(a, b, c)$.

Proof. Case $\mathrm{rad}(abc) = S$ follows from Theorem 4.4.2 and Lemma 4.2.16. If $v_2(bc) \geq 2$ then either b and c are even or b is odd and $m = v_2(c) \geq 2$. The first case follows by Theorem 4.4.2 and Lemma 4.2.16. The second case follows by Theorem 4.4.2 for $n \geq 4$ and by Theorem 4.4.3 for $2 \leq n \leq 3$. □

Theorem 4.5.4. *Let $q, \ell \geq 5$ be primes. Assume one of the following:*

1. $q \equiv 3 \pmod 8$, $\ell \equiv 5 \pmod 8$ *and* $q \equiv -\ell \pmod 3$.
2. $q \equiv 11 \pmod{24}$, $\ell \equiv 5 \pmod{24}$ *and* $\left(\frac{q}{\ell}\right) = -1$.
3. $q \equiv \pm 3 \pmod 8$, $\ell \equiv -1 \pmod{24}$, $\ell \not\equiv -1 \pmod q$.

Assume that $\mathrm{rad}(abc) = \ell q$.
Let $n = 0$ or ≥ 4 then the Fermat equation

$$ax^p + by^p + 2^n cz^p = 0,$$

has no solutions other than $xyz = 0$ for p larger than $G(a, b, 2^n c)$.
Let $r \geq 1$ then the Fermat equation

$$ax^p + 2^r by^p + 2^r cz^p = 0,$$

has no solutions other than $xyz = 0$ for p larger than $G(a, 2^r b, 2^r c)$.

Proof. If either $n = 0$ or $n \geq 5$ or $r \geq 1$ then this is Theorem 4.4.2 with Lemma 4.2.13. If $n = 4$ then this is Theorem 4.4.1 with Lemma 4.2.13. □

4.6 Bounds

Let us recall the explicit bound $G(a,b,c)$ as in Kraus' paper. In the following presentation we relax the bound so that statements are shorter. For example, $G(a,b,c)$ is taken so that a,b,c are pth-power-free for every $p > G(a,b,c)$.

Let us describe the bound $G(a,b,c)$. Let N be a positive integer and let

$$\begin{aligned}\mu(N) &= [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \cdot \prod_{\ell \mid N \text{ prime}} \left(1 + \frac{1}{\ell}\right),\\ g(N) &= \dim_{\mathbb{C}} S_2^{new}(N),\\ F(N) &= \left(\sqrt{\frac{\mu(N)}{6}} + 1\right)^{2g(N)}.\end{aligned}$$

where $S_2^{new}(N)$ denotes the space of weight 2 newforms of level N. Let a,b,c non-zero integers satisfying $\boldsymbol{(F)}$, $0 = v_2(a) \leq v_2(b) \leq v_2(c)$. Let

$$N = \begin{cases} \mathrm{rad}'(abc) & \text{if } b \text{ is odd and } v_2(c) = 4,\\ 2^3\ \mathrm{rad}'(abc) & \text{if } b \text{ is odd and } v_2(c) = 2,3,\\ 2^5\ \mathrm{rad}'(abc) & \text{if } b \text{ is odd and } v_2(c) = 1,\\ 2\ \mathrm{rad}'(abc) & \text{otherwise.}\end{cases}$$

If b is odd then G is defined by

$$G(a,b,c) := \max(F(N), \max_{q \text{ prime}} v_q(a), \max_{q \text{ prime}} v_q(b), \max_{q \text{ prime}} v_q(c)).$$

If b is even, that is $v_2(b) = v_2(c) \geq 1$ then G is defined by

$$G(a,b,c) := \max(F(N), \max_{q \text{ prime}} v_q(a), \max_{q \text{ prime}} v_q(b), \max_{q \text{ prime}} v_q(c), v_2(c)+4).$$

Example 4.6.1. *Let $S \neq \emptyset$ be a finite set of primes in $1 + 12\mathbb{Z}$ and let a,b,c be non-zero, square-free, pairwise coprime integers such that*

$\mathrm{rad}(abc) = S$. *Then*

$$N = 2\,\mathrm{rad}(abc) = 2S,$$
$$g(N) = \frac{\varphi(S)}{12} + (-1)^{\omega(2S)},$$
$$\mu(N) = 3\prod_{\ell \in S}(\ell + 1).$$

Here φ *denotes the Euler's totient function and* $\omega(2S)$ *the number of prime divisors of* $2S$. *The dimension* $g(N)$ *of* $S_2^{new}(N)$ *has been computed in [37].*

Appendix. Some computations on Frey curves

4.7 The conductor of $E[p]$

The j-invariant of a Frey curve is given by the formula

$$j_E = \frac{2^8(C^2 - AB)^3}{A^2B^2C^2}.$$

Thus one has for the case $(A, B, C) = (ax^p, by^p, cz^p)$ being pairwise coprime that $C^2 - AB$ and ABC are coprime. Let ℓ be a prime divisor of ABC. Then

$$v_\ell(j_E) = 8v_\ell(2) - 2v_\ell(ABC) \equiv 8v_\ell(2) - 2v_\ell(abc) \pmod{p}.$$

Thus $p \mid v_\ell(j_E)$ if and only if

- ℓ is odd and $p \mid v_\ell(abc)$, or
- $\ell = 2$ and $v_2(abc) \equiv 4 \pmod{p}$.

Proposition 4.7.1. *Let $E = E_{A,B,C}$ be the Frey curve as in Theorem 4.3.4. Let f be a newform in $S_2(M)$ for some divisor M of $2^s \operatorname{rad}'(abc)$ and let $\mathfrak{p}$ be a prime ideal such that*

$$E[p] \simeq \bar{\rho}_{f,\mathfrak{p}}$$

as $\mathbb{F}_p[G_\mathbb{Q}]$-modules. Then $M = 2^s \operatorname{rad}'(abc)$.

Proof. Let R the largest divisor of $2^s \operatorname{rad}'(abc)$ coprime to $2p$. Hence R is square-free. By Tate's uniformization $E[p]$ is ramified at every prime divisor ℓ of R and so is $\bar{\rho}_{f,\mathfrak{p}}$. Thus, $R \mid M$.

Let $\ell = 2$. If $s \in \{3, 5\}$ then Carayol [8] predicts that the lifting $\rho_{f,\mathfrak{p}}$ of $\bar{\rho}_{f,\mathfrak{p}}$ has conductor exponent s. Thus $2^s \mid M$. If $s = 0$ then M is odd and so is R. If $s = 1$ then $E[p]$ is ramified at 2 and so is $\bar{\rho}_{f,\mathfrak{p}}$. Hence $2 \mid M$.

One could just avoid case $p \mid M$ since we will consider big primes p with respect to $\operatorname{rad}(abc)$. Still, if $p \mid \operatorname{rad}'(abc)$ then $E[p]$ is not finite at p. That is, $E[p]|_{G_p}$ is reducible and not *peu ramifié* by [20, Proposition 8.2]. If $p \nmid M$ then $\bar{\rho}_{f,\mathfrak{p}}|_{G_p}$ is either irreducible or reducible and *peu ramifié*. Thus $E[p]|_{G_p} \not\simeq \bar{\rho}_{f,\mathfrak{p}}|_{G_p}$. This completes the proof. □

4.8 Mod 24 exercises

Proof of Lemma 4.2.13: Let (A, B, C) be a primitive S-unit point of height ≥ 3. Assume $A = 2^r$, $r \geq 3$. Then $B + C \equiv 0 \pmod 8$ and $B + C \not\equiv 0 \pmod 3$. Equivalently, one has

$$BC \equiv -1 \pmod 8$$

since $C^{-1} \equiv C \pmod 8$. Also $BC \equiv 1 \pmod 3$ since $B, C \in \{\pm 1\}$ mod 3. Thus

$$\pm q^s \ell^t = BC \equiv 7 \pmod{24}.$$

1. By hypothesis $\{q, \ell\} \in \{\{5, -5\}, \{11, -11\}\}$ mod 24. Notice that

   $$q^s \ell^t \equiv \pm q^{s+t} \not\equiv \pm 7 \pmod{24},$$

   hence A is not a power of two.

   Assume that

   $$2^r q^s = \ell^t + \varepsilon \equiv (\pm 3)^t + \varepsilon \pmod 8$$

   for some $\varepsilon \in \{\pm 1\}$. Then $\varepsilon = -1$ and t is even. Proposition 4.2.5 implies

   $$(q, \ell) \in \{(3, 5), (5, 3), (3, 7), (3, 17)\}.$$

   Condition $q \equiv -\ell \pmod{24}$ leads to a contradiction. Similarly, $2^r \ell^t = q^r + \varepsilon$ has no solution.

2. Assume that $(2^r, -q^s\ell^t, \varepsilon)$ is an S-point for some unit ε. Then $-\varepsilon q^s\ell^t \equiv 7 \pmod{24}$. Thus s, t are odd and $\varepsilon = -1$. That is

$$2^r = q^s\ell^t + 1 \equiv -1 \pmod 3,$$

hence r is odd, $r = 2f+1$. Thus, 2 is a square in $\mathbb{F}_q$, i.e. $q \equiv \pm 1 \pmod 8$. Indeed

$$\left(\frac{1}{q}\right) = \left(\frac{2}{q}\right)^r = \left(\frac{2}{q}\right).$$

Assume that

$$2^r + (-1)^a q^s + (-1)^b \ell^t = 0.$$

Then

$$(-1)^{a+b} q^s \ell^t \equiv 7 \pmod{24}.$$

Hence a, b have same parity and s, t are odd. Thus

$$2^r = q^s + \ell^t \equiv 1 \pmod 3$$

and r is even. Thus q is a square in $\mathbb{F}_\ell$.

Assume that $(2^r q^s, -\ell^t, \varepsilon)$ is an S-point. Then $\ell^t \equiv \varepsilon \pmod 8$. Proposition 4.2.5 applies to case $\varepsilon = 1$, t even. Case $\varepsilon = -1$, t odd implies $3 \mid \ell^t + 1 = 2^r q^s$.

Assume that $(2^r\ell^t, -q^s, \varepsilon)$ is an S-point. Then $\varepsilon = 1$ and s is even. By Proposition 4.2.5 $q \in \{3, 5, 7, 17\}$, hence

$$q \not\equiv 11 \pmod{24}.$$

3. By hypothesis

$$(q, \ell) \equiv (\pm 11, -1) \pmod{24}.$$

Thus $q^s\ell^t \not\equiv \pm 7 \pmod{24}$ and A is not a power of two.

Assume that

$$2^r q^s = \ell^t + 1.$$

Then t is either 1 or an odd prime by Lemma 4.2.9. Case $t = 1$ implies $\ell \equiv -1 \pmod q$. Case t odd prime implies ℓ Mersenne hence

$$\ell \equiv 0, 1 \pmod 3.$$

Assume that

$$2^r q^s = \ell^t - 1.$$

Hence t is even and Proposition 4.2.5 implies $\ell \in \{3, 5, 7, 17\}$, then

$$\ell \not\equiv 23 \pmod{24}.$$

□

Resum en català

Considerem el cos $\mathbb{Q}$ dels nombres racionals i una clausura algebraica $\bar{\mathbb{Q}}$ de $\mathbb{Q}$. El grup $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ de Galois absolut és profinit amb la topologia de Krull. Donat un grup profinit P, demostrar o refutar l'existència d'un epimorfisme continu $G_{\mathbb{Q}} \to P$ és en general un problema difícil. Diem que P és realitzable sobre $\mathbb{Q}$ o Galois sobre $\mathbb{Q}$ si existeix tal morfisme. Equivalentment, el problema consisteix en demostrar o refutar l'existència d'una extensió $L/\mathbb{Q}$ de Galois amb grup de Galois isomorf a P. Aquest és el conegut problema invers de Galois per a P. Una conjectura ben clàssica prediu que tot grup finit és grup de Galois sobre $\mathbb{Q}$. Cal fer notar que el cas de P infinit és fals en general. Per exemple, el grup profinit $\mathbb{Z}_p \times \mathbb{Z}_p$ no és Galois sobre $\mathbb{Q}$ com a conseqüència del Teorema de Kronecker-Weber.

Considerem $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ l'anell d'enters profinits, és a dir la completació profinita de l'anell $\mathbb{Z}$ dels enters. La teoria de varietats abelianes o fins i tot grups algebraics proporciona morfismes continus $G_{\mathbb{Q}} \to \mathrm{GL}_n(\hat{\mathbb{Z}})$. Com a conseqüència, molts grups lineals són realitzables sobre $\mathbb{Q}$. Vegem tres exemples.

1. El grup $\mathrm{GL}_1(\hat{\mathbb{Z}}) = \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$ és grup de Galois sobre $\mathbb{Q}$. En efecte, hom pot prendre l'extensió ciclotòmica infinita $L = \mathbb{Q}(\mu_n)_{n\geq 1}/\mathbb{Q}$ on μ_n denota el grup d'arrels n-èsimes de la unitat a $\bar{\mathbb{Q}}^\times$. Per tant,
$$\mathrm{Gal}(L/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^\times.$$
Aquesta és la representació de Galois associada al grup algebraic multiplicatiu $\mathbb{G}_m$.

2. L'extensió $\mathbb{Q}(E(\bar{\mathbb{Q}})[n])_{n\geq 1}/\mathbb{Q}$ és una generalització natural del cas ciclotòmic. Aquí $E(\bar{\mathbb{Q}})[n]$ denota el grup de punts de n-

torsió d'una corba el·líptica E definida sobre $\mathbb{Q}$. L'acció lineal de $G_{\mathbb{Q}}$ sobre $E(\bar{\mathbb{Q}})[n]$ indueix el morfisme

$$\rho_E : G_{\mathbb{Q}} \to \prod_p \mathrm{Aut}_{\mathbb{Z}_p} \mathcal{T}_p E \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

on $\mathcal{T}_p E$ denota el mòdul de Tate p-àdic associat a E.

Teorema (Serre [48]). *Seguint amb la notació anterior es té que ρ_E mai és exhaustiva. A més,*

(a) o bé E té multiplicació complexa,

(b) o bé la imatge de ρ_E té índex finit a $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

3. Sigui f un forma nova pels operadors de Hecke de pes 2, nivell N i caràcter trivial, considerem el cos K de nombres generat pels coefficients de Fourier de f i $\mathcal{O}$ l'anell d'enters de K. L'existència d'una varietat abeliana A_f sobre $\mathbb{Q}$ associada a f és deguda a Shimura. El grup de punts de torsió d'A_f indueix un morfisme

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathcal{O}}) = \prod_{\mathfrak{p}} \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}})$$

on $\hat{\mathcal{O}}$ denota la completació profinita de $\mathcal{O}$. Vegeu [34] per a una descripció de la imatge de ρ_f.

Aquests exemples estan fortament relacionats. Per exemple, el primer $G_{\mathbb{Q}} \twoheadrightarrow \hat{\mathbb{Z}}^\times$ s'obté com a determinant dels altres. A més, es té el teorema altament no trivial

Teorema (Modularitat). *Cada corba el·líptica sobre $\mathbb{Q}$ és (en la classe d'isogènia d') una varietat abeliana A_f per alguna forma nova f de Hecke de pes 2.*

Com a conseqüència, ρ_E s'obté com a representació de Galois ρ_f per a alguna forma nova f mòdul isogènia.

El propòsit d'aquesta tesi és estudiar aquestes representacions de Galois associades a formes noves.

Considerem $\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_2(\hat{\mathcal{O}})$ el morfisme associat a una forma f nova i considerem $\mathfrak{p}$ un ideal maximal de $\mathcal{O}$. El morfisme projecció $\hat{\mathcal{O}} \to \mathcal{O}_{\mathfrak{p}} \to \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ indueix un morfisme de grups topològics

$$\bar{\rho}_{\mathfrak{p}} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}).$$

Aquesta és l'anomenada representació de Galois mòdul $\mathfrak{p}$ associada a f.

Dues formes modulars f, g diferents defineixen representations ρ_f, ρ_g no isomorfes. Tanmateix, poden compartir alguna representació residual. Per ser més precisos, siguin f,g formes noves i siguin $\mathfrak{p}$, $\mathfrak{p}'$ ideals maximals de $\mathcal{O}_f$ i $\mathcal{O}_g$ respectivament, diem que $\bar{\rho}_{f,\mathfrak{p}}$ and $\bar{\rho}_{g,\mathfrak{p}'}$ són isomorfes si existeix un ideal maximal $\mathfrak{q}$ en el cos compost $K_f K_g$ sobre $\mathfrak{p}, \mathfrak{p}'$ tal que $\bar{\rho}_{f,\mathfrak{p}}$, $\bar{\rho}_{g,\mathfrak{p}'}$ són isomorfes com a representacions mòdul $\mathfrak{q}$. En aquest cas diem que f, g són congruents mòdul $\mathfrak{q}$. La següent pregunta sorgeix de forma natural.

Què pot dir-se d'una forma g nova congruent a una forma nova fixada f?

Els treballs de Hida, Kisin, Mazur, Ribet, Serre, Taylor o Wiles donen múltiples respostes a aquesta pregunta. Els Teoremes de pujada [45] i baixada [46] de nivell de Ribet són exemples prototípics en aquest context ja que descriuen canvis de nivell a través de congruències. Cal fer notar que el Teorema de Modularitat de Modularitat demostrat per Breuil, Conrad, Diamond, Taylor i Wiles és una conseqüència de tot aquest treball i té aplicacions en problemes diofantins com ara l'Últim Teorema de Fermat.

El contingut del nostre treball es divideix en 2 parts: als Capítols 2 i 3 donem noves respostes a la pregunta acabada d'exposar i al capítol 4 resolem nous casos d'equacions diofantines de tipus Fermat. Els capítols 2 i 3 han estat acceptats per publicació a reconegudes revistes, vegeu [17], [18]. Vegem el contingut per capítols.

- El Capítol 1 és de resultats preliminars on recordem la teoria de Galois de $\bar{\mathbb{Q}}/\mathbb{Q}$, representacions de Galois, formes modulars i corbes el·líptiques. El cas especial de corbes de Frey és tractat amb detall. L'última secció és dedicada a l'estudi de polinomis ciclotòmics necessari al Capítol 4 per resoldre algunes equacions en S-unitats.

- Al Capítol 2 descrivim el fenomen de canvi de signe en un primer de Steinberg. Les formes noves amb primer Steinberg p, és a dir, tals que p divideix un cop el nivell, admeten un de dos possibles comportaments locals a p, depenent del signe $a_p \in \{\pm 1\}$. En aquest capítol descrivim el cas on dos formes noves amb primer de Steinberg comú p poden tenir p-èsims coeficients a_p diferents. A més, si f és una forma nova amb primer de Steinberg p, donem condicions necessaries i suficients sobre $\bar{\rho}_{f,\mathfrak{p}}$ per assegurar l'existència d'una forma nova g congruent a f amb signe diferent al primer de Steinberg p. L'estratègia que seguim és la següent: suprimim p del nivell de f mitjançant un teorema de baixada de nivell. Llavors, afegim p al nivell mitjançant un teorema de pujada de nivell que ens permet triar el signe a_p. Demostrem que el teorema de baixada de nivell és aplicable a f si i només si existeix una tal g. Ens restringim al cas irreductible amb característica residual senar.

- Al Capítol 3 fem pujada de nivell sobre qualsevol primer. Sigui f una forma nova tal que la seva representació $\bar{\rho}_{f,\mathfrak{p}}$ de Galois mòdul $\mathfrak{p}$ és irreductible per a cada $\mathfrak{p}$ i sigui p un primer no divisor del nivell N de f. En aquest capítol demostrem que $a_p^2 - (p+1)^2$ no és una unitat a $\mathcal{O}_f$. Combinem aquest fet amb un teorema de pujada de nivell de Ribet assegurar l'existència d'una forma nova g congruent a f amb p al nivell. També demostrem algunes variants d'aquest enunciat on hom pot triar el signe a_p de g.

- Al Capítol 4 resolem nous casos de la Conjectura Asimptòtica de Fermat amb coeficients (AFC). Aquesta conjectura es relaciona amb les representacions de Galois gràcies a treballs de Frey i Mazur. Nosaltres seguirem l'aproximació efectiva de Kraus per tal de donar cotes explícites. Exhibim obstruccions locals a equacions en S-unitats per tal de resoldre $ax^p + by^p = cz^p$ asimptòticament en p amb abc contenint un nombre arbritari de factors primers. Cal fer notar que tots els casos de famílies infinites d'AFC resolts previs al nostre treball consideren el cas $\mathrm{rad}(abc) \mid 2p$.

Bibliography

[1] P. B. Allen: *Modularity of nearly ordinary 2-adic residually dihedral Galois representations.* Compos. Math. **150** (2014), no. 8, 1235–1346.

[2] S. Anni, V. Patel: *Congruence graphs and Hecke algebras*, in preparation (2018).

[3] A. O. L. Atkin, W. C. W. Li: *Twists of newforms and pseudo-eigenvalues of W-operators.* Invent. Math. **48** (1978), no. 3, 221–243.

[4] N. Billerey, I. Chen, L. Dieulefait, N. Freitas: *A multi-Frey approach to Fermat equations of signature (r,r,p).* arXiv:1703.06530, March 2017.

[5] C. Breuil: *Sur quelques représentations modulaires et p-adiques de* $\mathrm{GL}_2(\mathbb{Q}_p)$. *II.* J. Inst. Math. Jussieu **2** (2003), no. 1, 23–58.

[6] C. Breuil, A. Mézard: *Multiplicités modulaires et représentations de* $\mathrm{GL}_2(\mathbb{Z}_p)$ *et de* $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ *en* $\ell = p$. With an appendix by Guy Henniart. Duke Math. J. **115** (2002), no. 2, 205–310.

[7] H. Carayol: *Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert.* Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468.

[8] H. Carayol: *Sur les représentations galoisiennes modulo l attachées aux formes modulaires.* Duke Math. J. **59** (1989), no. 3, 785–801.

[9] H. Cohen: *Number theory. Vol. II. Analytic and modern tools.* Graduate Texts in Mathematics, **240**. Springer, New York, 2007.

[10] R. F. Coleman, B. Edixhoven: *On the semi-simplicity of the Up-operator on modular forms.* Math. Ann. **310** (1998), no. 1, 119–127.

[11] C. W. Curtis, I. Reiner: *Representation theory of finite groups and associative algebras.* Wiley Interscience, New York, 1962.

[12] H. Darmon, F. Diamond, R. Taylor: *Fermat's last theorem. Elliptic curves, modular forms and Fermat's last theorem.* Hong Kong, 1993, 2–140, Int. Press, Cambridge, MA, (1997).

[13] H. Darmon, L. Merel: *Winding quotients and some variants of Fermat's last theorem.* J. Reine Angew. Math. **490** (1997), 81–100.

[14] F. Diamond, K. Kramer: *Modularity of a family of elliptic curves.* Math. Res. Lett. **2** (1995), no. 3, 299–304.

[15] F. Diamond, J. Shurman: *A first course in modular forms.* Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005.

[16] L. Dieulefait: *Automorphy of* $Symm^5(\mathrm{GL}(2))$ *and base change.* J. Math. Pures Appl. (9) **104** (2015), no. 4, 619–656.

[17] L. Dieulefait E. Soto : *On congruences between normalized eigenforms with different sign at a Steinberg prime.* Rev. Mat. Iberoam. **34** (2018), no. 1, 413–421.

[18] L. Dieulefait E. Soto: *Raising the level at your favorite prime.* Atti Accad. Naz. Lincei Rend. Lincei Mat. Appl. (to appear).

[19] L. Dieulefait, G. Wiese: *On modular forms and the inverse Galois problem.* Trans. Amer. Math. Soc. **363** (2011), no. 9, 4569–4584.

[20] B. Edixhoven: *The weight in Serre's conjectures on modular forms.* Invent. Math. **109** (1992), no. 3, 563–594.

[21] G. Faltings: *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. **73** (1983), no. 3, 349–366.

[22] N. Freitas, A. Kraus: *An application of the symplectic argument to some Fermat-type equations.* C. R. Math. Acad. Sci. Paris **354** (2016), no. 8, 751–755.

[23] G. Frey: *Links between elliptic curves and solutions of $A-B=C$.* J. Indian Math. Soc. (N.S.) **51** (1987), 117–145 (1988).

[24] E. Halberstadt, A. Kraus: *Courbes de Fermat: résultats et problèmes.* J. Reine Angew. Math. **548** (2002), 167–234.

[25] R. Hartshorne: *Algebraic geometry.* Graduate Texts in Mathematics, No. **52**. Springer-Verlag, New York-Heidelberg, 1977.

[26] M. Hindry, J. H. Silverman: *Diophantine geometry. An introduction.* Graduate Texts in Mathematics, **201**. Springer-Verlag, New York, (2000).

[27] A. Kraus: *Majorations effectives pour l'équation de Fermat généralisée.* Canad. J. Math. **49** (1997), no. 6, 1139–1161.

[28] S. Lang: *Algebra.* Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[29] S. Lang: *Integral points on curves.* Inst. Hautes Études Sci. Publ. Math. No. 6 1960 27–43.

[30] R. P. Langlands: *Modular forms and ℓ-adic representations.* In *Modular functions of one variable, II* Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, 361–500 Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[31] B. V. Le Hung, C. Li: *Level raising mod 2 and arbitrary 2-Selmer ranks.* arXiv:1501.01344, April 2016.

[32] R. Livne: *On the conductors of mod l Galois representations coming from modular forms.* J. Number Theory **31** (1989), no. 2, 133–141.

[33] W. Ljunggren: *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$. Avh. Norske Vid. Akad. Oslo. I. 1942, (1942). no. 5–27.

[34] D. Loeffler: *Images of adelic Galois representations for modular forms.* Glasg. Math. J. **59** (2017), no. 1, 11–25.

[35] D. Loeffler, J. Weinstein: *On the computation of local components of a newform.* Math. Comp. **81**, no. 278, 1179–1200 (2012).

[36] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, http://www.lmfdb.org, 2013, [Online; accessed 9 October 2017].

[37] G. Martin: *Dimensions of the spaces of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$. J. Number Theory **112** (2005), no. 2, 298–331.

[38] B. Mazur: *Rational isogenies of prime degree.* Invent. Math. **44** (1978), no. 2, 129–162.

[39] P. Mihăilescu: *Primary cyclotomic units and a proof of Catalan's conjecture.* J. Reine Angew. Math. **572** (2004), 167–195.

[40] J. S. Milne: *Fields and Galois Theory.* Lecture notes.

[41] J. S. Milne: *Modular Functions and Modular Forms.* Lecture notes.

[42] T. Miyake: *Modular forms.* Springer-Verlag, Berlin, 2006.

[43] I. Papadopoulos: *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3.* J. Number Theory **44** (1993), no. 2, 119–152.

[44] P. Ribenboim: *Catalan's conjecture. Are 8 and 9 the only consecutive powers?* Academic Press, Inc., Boston, MA, 1994.

[45] K. A. Ribet: *Raising the levels of modular representations.* Séminaire de Théorie des Nombres, Paris 1987–88, 259–271, Progr. Math. **81**, Birkhäuser Boston, Boston, MA, (1990).

[46] K. A. Ribet: *On modular representations of* $\mathrm{Gal}(\bar{Q}/Q)$ *arising from modular forms.* Invent. Math. **100** (1990), no. 2, 431–476.

[47] K. A. Ribet: *On the equation* $a^p + 2^\alpha b^p + c^p = 0$. Acta Arith. **79** (1997), no. 1, 7–16.

[48] J.-P. Serre: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15** (1972), no. 4, 259–331.

[49] J.-P. Serre: *Local fields.* Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[50] J.-P. Serre: *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Duke Math. J. **54** (1987), no. 1, 179–230.

[51] J.-P. Serre: *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.

[52] J.-P. Serre: *Abelian* l*-adic representations and elliptic curves.* Research Notes in Mathematics, **7**. A K Peters, Ltd., Wellesley, MA, (1998).

[53] J. H. Silverman: *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, **106**. Springer, Dordrecht, 2009.

[54] J. H. Silverman: *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, **151**. Springer-Verlag, New York, 1994.

[55] A. Snowden: *On two dimensional weight two odd representations of totally real fields.* arXiv:0905.4266, May 2009.

[56] W. Stein: *Modular forms, a computational approach.* Graduate Studies in Mathematics, **79**. American Mathematical Society, Providence, RI, 2007.

[57] R. Steiner, N. Tzanakis: *Simplifying the solution of Ljunggren's equation* $X^2 + 1 = 2Y^4$. J. Number Theory **37** (1991), no. 2, 123–132.

[58] C. Störmer: *Solution complète en nombres entiers de l'équation* $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$. Bull. Soc. Math. France **27** (1899), 160–170.

[59] T. Szamuely: *Galois groups and fundamental groups.* Cambridge Studies in Advanced Mathematics, *117*. Cambridge University Press, Cambridge, 2009.

[60] J. Tate: *Algorithm for determining the type of a singular fiber in an elliptic pencil.* Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 33–52. Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.

[61] D. Ulmer: *Conductors of ℓ-adic representations.* Proc. Amer. Math. Soc. **144** (2016), no. 6, 2291–2299.

[62] L. C. Washington: *Introduction to cyclotomic fields.* Second edition. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1997.

[63] A. Wiles: *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) **141** (1995), no. 3, 443–551.