UNIVERSIDAD DE BUENOS AIRES
Facultad de Ciencias Exactas y Naturales
Departamento de Matemática

Construcciones de puntos de Heegner

Tesis presentada para optar al título de Doctor de la Universidad de Buenos Aires
en el área Ciencias Matemáticas

Daniel Kohen

Director de tesis: Dr. Ariel Martín Pacetti.
Consejero de estudios: Dr. Ariel Martín Pacetti.

Buenos Aires, 2017
Fecha de defensa:

Construcciones de puntos de Heegner

Dada una curva elíptica racional E y un cuerpo cuadrático imaginario K que satisface la llamada hipótesis de Heegner, podemos construir puntos definidos sobre extensiones abelianas de K conocidos como puntos de Heegner. Estos puntos, que se pueden calcular explícitamente, son cruciales para entender la aritmética de la curva elíptica.

Cuando el signo de la ecuación funcional de E/K es -1 se espera poder construir puntos, aún cuando la hipótesis de Heegner no se satisfaga, de acuerdo a una conjetura propuesta por Darmon. El objetivo principal de la tesis es mostrar cómo obtener estos puntos de forma tanto teórica como computacional en todos los casos en donde uno espera que exista una construcción en un álgebra de cuaterniones no ramificada.

Los casos estudiados en esta tesis, que yacen fuera de la teoría clásica, son cuando la curva tiene primos no estables que son o bien inertes o ramificados en el cuerpo K. En el primer caso, la clave consiste en reemplazar a las curvas modulares clásicas por las llamadas Curvas de Cartan *non-split*. En el segundo caso, la técnica utilizada consiste en asociar a la curva elíptica un objeto geométrico más complicado pero en el cual la existencia de puntos de Heegner está garantizada y luego recuperar los puntos en la curva original.

Palabras claves: Teoría de números, Curvas elípticas, puntos de Heegner, Conjetura BSD, Curvas de Cartan, Sistemas de Heegner, Variedades abelianas de tipo GL_2.

Heegner point constructions

Given a rational elliptic curve E and an imaginary quadratic field K that satisfies the so called Heegner hypothesis, we can construct points on E defined over abelian extensions of K called Heegner points. These points, that can be explicitly computed, are crucial in order to understand the arithmetic of the elliptic curve.

Whenever the sign of the functional equation of E/K is -1 we expect to find analogues of Heegner points, even if the Heegner hypothesis is not satisfied, according to a conjecture of Darmon. The main goal of this thesis is to show how to obtain these points in both a computational and theoretical way in all cases where we expect a construction to take place in an unramified quaternion algebra.

The cases studied in this thesis, which are beyond the scope of the classical theory, are when the curve has unstable primes that are either inert or ramified in the field K. In the first case, the key consists in replacing the classical modular curve with the so called Cartan non-split curves. In the second case, the main technique consists in associating a more complicated geometric object to the elliptic curve, in which the existence of Heegner points is guaranteed, and then recover the points in the original curve.

Keywords: Number theory , Elliptic curves, Heegner points, BSD conjecture, Cartan curves, Heegner systems, Abelian varieties of GL_2-type.

Contents

Introducción

Uno de los problemas centrales de la teoría de números consiste en entender el grupo de puntos racionales de una curva elíptica $E/\mathbb{Q}$. Este es un grupo abeliano finitamente generado, y por lo tanto tiene una parte de torsión y una parte libre. La torsión es muy sencilla de calcular mientras que el rango de la parte libre es mucho más misterioso.

Podemos construir un objeto analítico -la función L de E- que se obtiene de contar la cantidad de puntos de la curva elíptica módulo p para cada primo y pegar esta información en una suerte de función generatriz. Esta función analítica admite una extensión a todo el plano complejo por el famoso teorema de Wiles [Wil95] y las generalizaciones de Wiles-Taylor [TW95] y Breuil-Conrad-Diamond-Taylor [BCDT01], que afirman que toda curva elíptica racional es *modular*, es decir, existe una forma modular cuya función L coincide con la de E.

La conjetura de Birch and Swinnerton-Dyer (BSD) dice que el orden de anulación de la L serie de E en $s = 1$ -*el rango analítico*- coincide con el rango de la curva elíptica E. Además, da una receta precisa que relaciona el primer coeficiente no nulo de la expansión de Taylor en $s = 1$ con ciertos objetos aritméticos relacionados a la curva E. La conjetura está lejos de ser probada y una de las pocas instancias en donde se sabe que vale es cuando el rango analítico de E es menor o igual a 1. En este caso, el concepto de los puntos de Heegner juega un rol fundamental.

Sea N el conductor de E, un número que mide los lugares en donde la curva tiene mala reducción. Por el teorema de Wiles existe una función racional, llamada la parametrización modular,

$$\Phi_N : X_0(N) \to E,$$

donde $X_0(N)$ es el cociente del semiplano complejo superior por las unidades de un orden de Eichler de nivel N. La curva modular $X_0(N)$ tiene una intepretación de moduli; sus puntos sobre un cuerpo F están parametrizados por pares que consisten de una curva elíptica junto con un subgrupo cíclico de orden N, ambos definidos sobre F.

Dado un cuerpo cuadrático imaginario K, decimos que (E, K) satisface la *hipótesis de Heegner* si todo primo que divide a N se parte en K. Bajo tal hipótesis, la curva $X_0(N)$ tiene muchos puntos algebraicos que corresponden a curvas elípticas con multiplicación compleja por órdenes en K. Sus imágenes bajo Φ_N son llamadas puntos de Heegner [Gro84], que son puntos en E definidos sobre extensiones abelianas de K. Gross y Zagier [GZ86] probaron que la traza de estos puntos a K no son de torsión precisamente cuando $L^{'}(E/K, 1) \neq 0$. Luego, Kolyvagin [Kol90] probó que cuando los puntos de Heegner no son de torsión entonces el rango de E/K es precisamente 1. Un aspecto clave en sus resultados es considerar puntos de Heegner para diferentes órdenes (pero para el mismo cuerpo K) y probar que estos puntos satisfacen ciertas compatibilidades con la norma. Esta colección de puntos de Heegner en la curva elíptica E es lo que se conoce como un sistema de Heegner.

Combinando los resultados de Gross-Zagier y Kolyvagin (eligiendo un cuerpo K adecuado) uno puede probar que el rango analítico de $E/\mathbb{Q}$ coincide con el rango de E siempre que el rango analítico de E sea menor o igual a 1.

Un problema interesante, dada una curva elíptica $E/\mathbb{Q}$ y un cuerpo cuadrático imaginario K, es entender los puntos de E definidos sobre K y también sobre sus extensiones abelianas. En [Dar04] se prueba que se puede relajar la hipótesis de Heegner y considerar puntos de Heegner cuando N es libre de cuadrados, todos los primos que dividen a N son no ramificados en K, y el signo de la ecuación funcional de E/K es -1 (este signo es 1 si el orden de anulación de $L(E/K)$ en $s = 1$ es par y -1 si es impar). Podemos factorizar $N = N^+N^-$ donde N^+ es divisible precisamente por los primos que se parten en K y N^- es divisible por los primos inertes. El hecho de que $\text{sign}(E, K) = -1$ implica que la cantidad de primos que dividen a N^- es par. En esta situación podemos reemplazar a la curva modular clásica por una curva de Shimura $X(N^+, N^-)$, que es el cociente del semiplano superior complejo por las unidades de un orden de Eichler de nivel N^+ en el álgebra de cuaterniones sobre $\mathbb{Q}$ de discriminante N^-. Así como $X_0(N)$, la curva de Shimura $X(N^+, N^-)$ tiene una interpretación de moduli y contiene muchos puntos especiales que corresponden a variedades abelianas con multiplicación compleja. El teorema de modularidad de Wiles, combinado con resultados de Jacquet-Langlands [JL70] nos proveen de una parametrización modular racional

$$\Phi_{N^+,N^-} : X(N^+, N^-) \to E.$$

Las imágenes de los puntos especiales bajo Φ_{N^+,N^-} se denominan puntos de Heegner en E. La fórmula de Gross-Zagier fue generalizada a este contexto por Zhang [Zha01] y la teoría de Kolyvagin funciona de manera completamente análoga. Una observación crucial es que a pesar de que podemos calcular explícitamente puntos

de Heegner que provienen de $X_0(N)$, esto se vuelve más complicado para estas curvas de Shimura. El mayor obstáculo es que la parametrización modular es difícil de calcular debido a la ausencia de cúspides (y por lo tanto la ausencia de expansiones de Fourier). Cabe destacar que sin mucha dificultad se pueden considerar los casos donde N es libre de cuadrados y no necesariamente coprimo con el discriminante de K.

La siguiente conjetura, propuesta por Darmon, es la principal motivación de esta tesis.

[Dar04, Conjetura 3.16]: Si $\text{sign}(E, K) = -1$, entonces existe un sistema de Heegner no trivial asociado a (E, K).

Ya explicamos cómo hacer esto para el caso en que N es libre de cuadrados. Cuando esto no sucede, la situación es más delicada y fue estudiada en toda generalidad por Yuan-Zhang-Zhang [YZZ13], donde en vez de trabajar con órdenes de Eichler clásicos, trabajan con grupos aritméticos más generales. El propósito de esta tesis es dar construcciones explícitas de puntos de Heegner para estos casos. Por explícito nos referimos a que podamos calcular numéricamente los puntos teóricos en las distintas extensiones abelianas de K; esto nos restringe a trabajar con álgebras de cuaterniones no ramificadas (ya que en los otros casos la parametrización modular es difícil de calcular).

Sea $\chi : K^\times \backslash K_{\mathbb{A}}^\times \to \mathbb{C}^\times$ un carácter de Hecke anticiclotómico de orden finito, y sea η el carácter que corresponde a la extensión cuadrática $K/\mathbb{Q}$. Para poder construir un punto de Heegner asociado a χ en un álgebra de matrices, para cada número primo p se debe satisfacer la siguiente condición:

$$\epsilon(\pi_p, \chi_p) = \chi_p(-1)\eta_p(-1),$$

donde π es la representación automorfa asociada a E, y $\epsilon(\pi_p, \chi_p)$ es el *root number* local de $L(s, \pi, \chi)$ (ver [YZZ13, Section 1.3.2]). Si imponemos la condición $\text{mcd}(\text{cond}(\chi), N\,\text{cond}(\eta)) = 1$, en los primos que dividen al conductor de $E/\mathbb{Q}$ la ecuación queda

$$\varepsilon_p(E/K) = \eta_p(-1),$$

donde $\varepsilon_p(E/K)$ es el *root number* local en p del cambio de base de E a K (es igual a $\varepsilon_p(E)\varepsilon_p(E \otimes \eta)$). Este *root number* se calcula en términos de la información local de la curva elíptica E de la siguiente manera ([Pac13]).

- Si p es no ramificado en K, entonces $\eta_p(-1) = 1$ y

$$\varepsilon_p(E/K) = \left(\frac{\text{disc}(K)}{p}\right)^{v_p(N)},$$

donde $v_p(N)$ denota la valuación de N en p y $\left(\frac{-}{p}\right)$ denota al símbolo de Legendre.

- Si $p > 3$ es ramificado en K entonces $\eta_p(-1) = \left(\frac{-1}{p}\right)$ y

$$\varepsilon_p(E/K) = \left(\frac{-1}{p}\right) \cdot \begin{cases} \varepsilon_p(E) & \text{si } v_p(N) = 1, \\ \varepsilon_p(E_p) & \text{si } v_p(N_{E_p}) = 1, \\ 1 & \text{si } E \text{ es S.P.}, \\ -1 & \text{si } E \text{ es S.C.}, \end{cases}$$

donde E_p denota al *twist* cuadrático de E por el carácter módulo p $\varkappa_p$; E es $S.P.$ si la representación automorfa de E en p es una serie principal y E es $S.C.$ si la la representación automorfa es supercuspidal.

Esto se puede entender de manera mucho más simple mediante el tipo de reducción de la curva $E/\mathbb{Q}_p$. Cuando $v_p(N) = 1$ el tipo de reducción es multiplicativa (i.e. la curva reducida tiene un nodo) mientras que en el resto de los casos la reducción es aditiva (i.e. la curva reducida tiene una cúspide). Si $v_p(N_{E_p}) = 1$ la curva tiene reducción potencialmente multiplicativa, mientras que los casos restantes tienen reducción potencialmente buena. La diferencia entre la serie principal y el caso supercuspidal es que en el primer caso la curva adquiere reducción buena sobre una extensión abeliana de $\mathbb{Q}_p$.

En la tabla Tabla 1 resumimos las ecuaciones de arriba para $p > 3$, donde el signo corresponde al producto $\varepsilon_p(E/K)\eta_p(-1)$.

	p es inerte	p se parte	p ramifica
Reducción multiplicativa	-1	1	$\varepsilon_p(E)$
Reducción multiplicativa $\otimes\varkappa_p$	1	1	$\varepsilon_p(E_p)$
Serie principal	1	1	1
Supercuspidal	1	1	-1

Table 1: Signos

Nuestro objetivo es dar una construcción explícita en todos los casos en donde los signos de la Tabla 1 son iguales a 1.

La principal contribución de esta tesis son los casos en gris claro y gris oscuro. Las celdas blancas corresponden a la construcción clásica de puntos de Heegner

explicada previamente. El caso de la celda negra está fuera del alcance de las técnicas desarrolladas en este trabajo.

El primer capítulo de esta tesis trata sobre las celdas en gris claro y está basado en los resultados publicados en [KP16], de manera conjunta con mi director. La idea principal es reemplazar las curvas modulares clásicas $X_0(N)$ con las llamadas curvas de Cartan *non-split*. Esto tiene dos ventajas: la primera es que podemos definir el análogo de puntos de Heegner y la segunda es que los sistemas de autovalores de las formas nuevas clásicas aparecen en la cohomología de las curvas de Cartan *non-split*.

En las Secciones 1.1 y 1.2 definimos los subgrupos de Cartan *non-split* y las curvas modulares subyacentes y estudiamos sus propiedades básicas. En la Sección 1.3 damos una interpretación de moduli para tales curvas, lo que nos permite entender tanto los operadores de Hecke como los puntos de Heegner. También, estudiamos a los operadores de Hecke como operadores de doble coclase en la Sección 1.4.

El siguiente paso es probar que los sistemas de autovalores de curvas elípticas aparecen como sistemas de autovalores para los grupos de Cartan *non-split*. Esto será explicado en la Sección 1.5, más precisamente en el Teorema 1.5.1. En esta Sección probamos el Teorema 1.5.3 que es uno de los teoremas cruciales del capítulo. Este teorema nos permite escribir a la q-expansión de una autofunción del grupo de Cartan como una combinación lineal de *twists* de formas nuevas clásicas, que pueden ser explícitamente determinadas. La determinación de las mismas está hecha en la Subsección 1.6.1, donde además estudiamos las representaciones locales asociadas a la curva E. En la Sección 1.6 explicamos cómo calcular efectivamente la q-expansión de las autofunciones para los grupos de Cartan. Luego, estudiamos las propiedades teóricas que satisfacen estas q-expansiones en las Secciones 1.7 y 1.8. Más concretamente, damos la definición correcta de forma modular *racional* (Definición 1.7.3). Esta definición requiere una normalización (distinta de la clásica "$a_1 = 1$") que se obtiene usando el Teorema 90 de Hilbert (Teorema 1.8.7). Las formas racionales tienen su q-expansión con coeficientes en una extensión ciclótomica, de acuerdo al Teorema 1.8.6.

El siguiente paso, realizado en la Sección 1.9, es estudiar la parametrización modular de la curva de Cartan *non-split* a la curva elíptica E usando la construcción de Eichler-Shimura. La principal dificultad que encontramos es que las cúspides de la curva están definidas sobre una extensión ciclotómica y por ende la parametrización modular que uno definiría naturalmente no está definida sobre $\mathbb{Q}$. Para solucionar este problema hay que tomar un promedio sobre las distintas cúspides conjugadas.

En la Sección 1.10 estudiamos los puntos de Heegner en las curvas de Cartan *non-split*. Primero definimos la hipótesis de Cartan-Heegner que nos permite tratar

con las celdas en gris claro de la Tabla 1. Definimos a los puntos de Heegner mediante la intepretación de moduli y mostramos cómo obtenerlos de forma computacional. Finalmente, estudiando la acción de los operadores de Hecke y Atkin-Lehner, obtenemos la noción de sistemas de Heegner, que son una familia de puntos en la curva elíptica que satisfacen ciertas "compatibilidades de norma". Usando la interpretación de moduli vemos que la situación es muy similar al caso clásico, dando lugar al análogo obvio del teorema de Kolyvagin (Teorema 1.11.4). Por último, invocamos a la generalización de la fórmula de Gross-Zagier hecha por Zhang (Teorema 1.11.5) que prueba que la traza a K de los puntos de Heegner construidos no es de torsión precisamente cuando $L'(E/K, 1) \neq 0$.

Concluimos el capítulo dando un ejemplo concreto de los puntos de Heegner construidos utilizando estas ideas.

El segundo capítulo de la tesis se concentra en las celdas pintadas de gris oscuro en la Tabla 1 (más precisamente en el caso que estas celdas tienen signo igual a 1) y está basado en el artículo [KP], que también es un trabajo en conjunto con mi director.

Por razones técnicas asumamos en este caso que si 2 ramifica entonces a lo sumo 2^1 divide a N y si 3 ramifica en K entonces a lo sumo 3^2 divide a N. Además, necesitamos que E no posea multiplicación compleja.

La idea principal de este capítulo es que en este contexto podemos encontrar un *twist* adecuado de la forma modular f_E asociada a E tal que el nivel de la forma nueva correspondiente en los primos inestables de E que ramifican en K sea a lo sumo uno, situándonos en un escenario donde podemos hacer una construcción de Heegner clásica. El principal obstáculo en este plan es que al "twistear" por este carácter cambia el objeto geométrico que estamos considerando y necesitamos trabajar con una variedad abeliana $A/\mathbb{Q}$ del tipo GL_2 que tiene dimension $d = 1, 2$ o 4 sobre $\mathbb{Q}$. Esta variedad abeliana resulta isógena a E^d sobre una extensión abeliana controlada $M/\mathbb{Q}$. Luego, tenemos que entender cómo pasar de puntos en A a puntos en E que satisfagan propiedades análogas a las estudiadas anteriormente y mostrar que los podemos calcular de manera concreta.

En la Sección 2.1 analizamos la existencia de estos *twists* distinguidos en términos del tipo local de la representación automorfa asociada a E, como explicamos en la Subsección 1.6.1. "Twistear" por estos caracteres nos provee de una forma nueva g (posiblemente con Nebentypus) de un nivel más chico que tiene asociada una variedad abeliana A_g. En la Proposición 2.1.1 probamos que existe una isogenía entre A_g y E^d definida sobre M, y explicamos el comportamiento de una tal isogenía bajo la acción del grupo de Galois $\mathrm{Gal}(M/\mathbb{Q})$.

En la Sección 2.2 estudiamos los puntos de Heegner que viven en curvas que están "entre" $X_0(N)$ y $X_1(N)$ que parametrizan a la variedad abeliana A_g. Los puntos de Heegner son precisamente las preimágenes de puntos de Heegner clásicos en $X_0(N)$. Luego, damos una interpretación de moduli para estos puntos y estudiamos su cuerpo de definición en la Proposición 2.2.1. Este cuerpo es la composición del correspondiente cuerpo de clases con la extensión abeliana $M/\mathbb{Q}$.

El siguiente ingrediente fundamental es la forma más general de la fórmula de Zhang dada en la Sección 2.3. Estudiando la relación entre los puntos de Heegner y la isogenía entre A_g y E^d terminamos probando el Teorema 2.3.2, que nos dice que la traza hasta K de los puntos de Heegner no es de torsión justamente cuando la derivada de la L-serie no se anula en su centro de simetría, en perfecta armonía con tanto el caso clásico de puntos de Heegner como con la situación estudiada en el Capítulo 1.

Para poder probar el análogo al teorema de Kolyvagin necesitamos ser un poco más cuidadosos; esto está realizado en la Sección 2.4. Las relaciones de compatibilidad se traducen textualmente a la variedad abeliana A_g pero tenemos que tener en cuenta que a pesar de que tenemos a un cuerpo de números K_g actuando en A_g esto no da una accíon natural en E^d. La solución es restringir las compatibilidades a un conjunto de primos como en la Proposición 2.4.2, y con esta elección chequear que el teorema de Kolyvagin sigue valiendo (Teorema 2.4.3).

Más adelante, en la Sección 2.5 estudiamos el problema de calcular explícitamente un factor 1-dimensional de A_g que sea isógeno a E. Primero, estudiamos la teoría de los "building blocks" de Ribet [Rib77] y las cuentas explícitas de Gonzalez-Lario [GL01]. Luego realizamos la determinación explícita de cierto *splitting map* que trivializa un 2-cociclo dado por unas sumas de Jacobi. Este *splitting map* nos permite obtener un factor 1-dimensional de A_g y luego poder calcular un ismorfismo con E definido sobre M. Terminamos el capítulo con una sección de ejemplos, mostrando los puntos de Heegner construidos con esta técnica.

La construcción de este capítulo es interesante por si misma, y puede ser usada para moverse de una situación delicada a una no tan mala (reduciendo el conductor de la curva pero pagando el costo de introducir un carácter en algunos casos). A pesar de que nos concentramos en álgebras de matrices, los métodos de este capítulo pueden ser usados en una amplia variedad de contextos, por ejemplo en curvas de Shimura más generales. En particular esta construcción también funciona cuando E_p tiene reducción multiplicativa en el primo p y $\varepsilon_p(E_p) = -1$. Además, cabe destacar que esta construcción es fundamentalmente distinta al método estudiado en [YZZ13].

En los artículos [KP16] y [KP] primero estudiamos el problema un primo a la vez, y después vimos como obtener el caso general a partir de eso. Sin embargo, en esta

tesis los resultados están enunciados y probados en su total generalidad, mejorando considerablemente la exposición, notación y organización interna. A pesar de que esto requiere una capa extra de abstracción creemos que esta manera de presentar los resultados es más clara y conceptual y va a resultar más fructífera para la referencia en futuras aplicaciones.

Introduction

One of the main problems in number theory consists in understanding the group of rational points of an elliptic curve $E/\mathbb{Q}$. This is a finitely generated abelian group, and therefore it has a torsion part and a free part. The torsion part is fully understood and easy to compute, while the rank of the free part is very mysterious.

From the elliptic curve E one can construct an analytic object -*the L-function of E*- obtained by counting the points of the elliptic curves modulo every prime and gluing this information together into a generating function. Such analytic function admits an analytic continuation to the whole complex plane due to the famous theorem of Wiles [Wil95] and its subsequent generalizations by Wiles-Taylor [TW95] and Breuil-Conrad-Diamond-Taylor [BCDT01], that assert that every rational elliptic curve is *modular*, that is, there exists a modular form whose associated L-function coincides with the L-function of E.

The conjecture of Birch and Swinnerton-Dyer (BSD) states that the order of vanishing of the L-function at $s = 1$ -*the analytic rank*- coincides with the rank of the elliptic curve E. Moreover, there is a precise recipe that relates the first non-zero term of the Taylor expansion at $s = 1$ with certain arithmetic objects associated to E. This conjecture is far from being proved, and one of the only instances where it is known to hold is when the analytic rank of E is less or equal than one. In that case, the concept of Heegner points plays a key role.

Let N be the conductor of E, a number that measures the places of bad reduction of the elliptic curve. By Wiles' theorem there is a rational map, called the modular parametrization,

$$\Phi_N : X_0(N) \to E,$$

where $X_0(N)$ is a quotient of the upper-half plane by the units in an Eichler order of level N. The modular curve $X_0(N)$ has a nice moduli interpretation, parametrizing pairs consisting of an elliptic curve and a cyclic subgroup of order N.

Given an imaginary quadratic field K we say that (E, K) satisfies the *Heegner hypothesis* if every prime dividing N splits in K. Under such hypothesis, the curve $X_0(N)$ contains many algebraic points corresponding to elliptic curves with complex

multiplication by orders in K. Their images under Φ_N are called Heegner points [Gro84], which are points on E defined over abelian extensions of K. Gross and Zagier [GZ86] proved that the traces to K of Heegner points are non-torsion precisely when $L^{'}(E/K, 1) \neq 0$. Soon after, Kolyvagin [Kol90] proved that when the Heegner points are non-torsion the rank of E/K is exactly 1. A key aspect of his results is to consider different Heegner points for varying orders (but for a fixed field K) and show that these points satisfy certain norm compatibility properties. This collection of Heegner points on the elliptic curve E is known as a Heegner system.

Combining the results from Gross-Zagier and Kolyvagin (choosing an appropriate field K) one proves that the analytic rank of $E/\mathbb{Q}$ is the same as the rank provided that the analytic rank is less or equal than 1.

It is still an interesting problem, given $E/\mathbb{Q}$ an elliptic curve and K an imaginary quadratic field, to understand the points of E defined over K and its abelian extensions. In [Dar04] it is shown that one can relax the Heegner hypothesis and still construct Heegner points if N is squarefree, all primes dividing N are unramified in K, and the sign of the functional equation of E/K is -1 (such sign is equal to 1 if the the order of vanishing of $L(E/K)$ at $s = 1$ is even and -1 if it is odd). We can factorize $N = N^+N^-$ where N^+ is divisible precisely by the primes that are split in K and N^- is divisible by the inert ones. The fact that $\text{sign}(E, K) = -1$ implies that the number of primes dividing N^- is even. In this situation one can replace the classical modular curve with a Shimura curve $X(N^+, N^-)$, that is the quotient of the upper half plane by the units of an Eichler order of level N^+ in the quaternion algebra over $\mathbb{Q}$ of discriminant N^-. As $X_0(N)$, the Shimura curve $X(N^+, N^-)$ has a moduli interpretation and contains many special algebraic points corresponding to abelian varieties with complex multiplication. Wiles' modularity theorem combined with results from Jacquet-Langlands [JL70] provide a rational modular parametrization

$$\Phi_{N^+,N^-} : X(N^+, N^-) \to E.$$

The image of the special points under Φ_{N^+,N^-} are called Heegner points on E. The Gross-Zagier theorem was generalized to this setting by Zhang [Zha01] and Kolyvagin's theory works in an analogous way. An important remark is that although we can compute explicitly Heegner points coming from $X_0(N)$, many difficulties arise while working with Shimura curves, the main obstacle being that the modular parametrization is hard to compute because of the absence of cusps (and thus the absence of Fourier expansions of modular forms). It is worth noting that we can easily consider the cases where N is squarefree but N is not necessarily relatively prime to the discriminant of K.

The following conjecture, proposed by Darmon, is the main motivation for this

thesis.
[Dar04, Conjecture 3.16]: If $\mathrm{sign}(E,K) = -1$, then there is a non-trivial Heegner system attached to (E,K).

We have explained how to find a Heegner system when N is squarefree. If the conductor is not squarefree, the situation is quite more delicate and it has been studied in full generality by Yuan-Zhang-Zhang [YZZ13], where instead of working with classical Eichler orders, they deal with more general arithmetic groups. The purpose of this thesis is to give explicit constructions of Heegner points for pairs (E,K) as above. By explicit we mean that we can compute numerically the theoretical points in the corresponding abelian extension of K, which restricts us to working only with unramified quaternion algebras (since the modular parametrization is hard to compute for Shimura curves).

Let $\chi : K^\times \backslash K_{\mathbb{A}}^\times \to \mathbb{C}^\times$ be a finite order anticyclotomic Hecke character, and let η be the character corresponding to the quadratic extension $K/\mathbb{Q}$. In order to construct a Heegner point attached to χ in a matrix algebra, for each prime number p the following condition must hold:

$$\epsilon(\pi_p, \chi_p) = \chi_p(-1)\eta_p(-1),$$

where π is the automorphic representation attached to E, and $\epsilon(\pi_p,\chi_p)$ is the local root number of $L(s,\pi,\chi)$ (see [YZZ13, Section 1.3.2]). If we impose the extra condition $\gcd(\mathrm{cond}(\chi), N\,\mathrm{cond}(\eta)) = 1$, then at the primes dividing the conductor of $E/\mathbb{Q}$ the equation becomes

$$\varepsilon_p(E/K) = \eta_p(-1),$$

where $\varepsilon_p(E/K)$ is the local root number at p of the base change of E to K (it is equal to $\varepsilon_p(E)\varepsilon_p(E\otimes\eta)$). This root number is computed using the local information of the elliptic curve E in the following way ([Pac13]).

- If p is unramified in K, then $\eta_p(-1) = 1$ and

$$\varepsilon_p(E/K) = \left(\frac{\mathrm{disc}(K)}{p}\right)^{v_p(N)},$$

  where $v_p(N)$ denotes the valuation of N at p and $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol.

- If $p > 3$ is ramified in K then $\eta_p(-1) = \left(\frac{-1}{p}\right)$ and

$$\varepsilon_p(E/K) = \left(\frac{-1}{p}\right) \cdot \begin{cases} \varepsilon_p(E) & \text{if } v_p(N) = 1, \\ \varepsilon_p(E_p) & \text{if } v_p(N_{E_p}) = 1, \\ 1 & \text{if } E \text{ is P.S.}, \\ -1 & \text{if } E \text{ is S.C.}, \end{cases}$$

  where E_p denotes the quadratic twist of E by the character modulo p $\varkappa$; E is P.S. if the attached automorphic representation is a ramified principal series and E is S.C. if the attached automorphic representation is supercuspidal at p.

This can be better understood using the type of reduction of the elliptic curve $E/\mathbb{Q}_p$. When $v_p(N) = 1$ the reduction is multiplicative (i.e. the reduced curve has a node) while in the rest of the cases the reduction is additive (i.e. the reduced curve has a node). If $v_p(N_{E_p}) = 1$ the curve has potentially multiplicative reduction while the remaining cases have potentially good reduction. The difference between the principal series and the supercuspidal case is that in the first case the curve has potentially good reduction over an abelian extension of $\mathbb{Q}_p$.

In Table 2 we summarize the above equations for $p > 3$, where the sign corresponds to the product $\varepsilon_p(E/K)\eta_p(-1)$.

	p is inert	p splits	p ramifies
Multiplicative reduction	-1	1	$\varepsilon_p(E)$
Multiplicative reduction $\otimes\varkappa_p$	1	1	$\varepsilon_p(E_p)$
Principal series	1	1	1
Supercuspidal	1	1	-1

Table 2: Signs

Our goal is to give an explicit construction in all cases where the local sign of Table 2 is equal to 1.

The main contribution of this thesis is to deal with the cases in light and dark grey. The cells colored in white correspond to the classical Heegner point construction. We do not say anything about the black cell; this lies outside the scope of the techniques developed in this work.

The first chapter of this thesis deals with the light grey cells and is based on the results published in [KP16], jointly with my advisor. The main idea is to replace the

classical modular curves $X_0(N)$ with the so-called Cartan non-split curves. This has two main advantages: the first one is that we can find a right analogue of Heegner points and the second one is that the systems of eigenvalues of classical newforms appear in the cohomology of Cartan non-split curves.

In Sections 1.1 and 1.2 we define the Cartan non-split congruence subgroups and the underlying modular curves and we study their basic properties. In Section 1.3 we give a moduli interpretation for such curves, allowing us to give a clean understanding of Hecke operators and Heegner points. We also study Hecke operators as double coset operators in Section 1.4.

The next step is to show that the systems of eigenvalues of rational elliptic curves appear as systems of eigenvalues for modular forms for Cartan non-split groups. This is stated in Section 1.5, more precisely Theorem 1.5.1. In this section we prove Theorem 1.5.3 which is one of the most crucial theorems in this chapter. This theorem allows us to write the q-expansion of an eigenform for the Cartan non-split group as a linear combination of twists of classical newforms that can be explicitly determined. The determination of these forms is done in Subsection 1.6.1, where we also study the local representations attached to the elliptic curve E. In Section 1.6 we explain how to effectively compute the q-expansions of eigenforms for the Cartan non-split group. We then proceed to study some theoretical properties of these q-expansions in Sections 1.7 and 1.8. More precisely, we give the right definition of *rational* modular form (Definition 1.7.3). This definition requires a choice of normalization (different from the classic "$a_1 = 1$") obtained using Hilbert 90 Theorem (Theorem 1.8.7). These rational modular forms have q-expansions belonging to a cyclotomic field according to Theorem 1.8.6.

The next step, done in Section 1.9, is to study the modular parametrization from the Cartan non-split curve to the elliptic curve E using the Eichler-Shimura construction. The main issue we encounter is that the cusps of these curves are defined over a cyclotomic extension, and thus the naive modular parametrization is not defined over $\mathbb{Q}$. In order to solve this issue we just need to take an average over all conjugate cusps.

In Section 1.10 we study Heegner points on Cartan non-split curves. First we define the Cartan-Heegner hypotheses that allows us to deal with the light grey cells in Table 2. We define Heegner points by means of the moduli interpretation and we show how to obtain them computationally. Finally, by studying the Hecke and Atkin-Lehner actions on Heegner points we end up with the concept of Heegner system, which is a family of points on the elliptic curve subject to certain "norm compatibilities". Using the moduli interpretation we realize that the situation is very similar to the classical case, giving rise to the obvious analogue of Kolyvagin's

theorem (Theorem 1.11.4). Lastly, we invoke Zhang's generalization of Gross-Zagier formula (Theorem 1.11.5) which shows that the trace to K of the Heegner points constructed is non torsion precisely when $L'(E/K, 1) \neq 0$.

We conclude this chapter by giving a concrete example of the Heegner points obtained using these ideas.

The second chapter of this thesis focus on the dark gray cells of Table 2 (more precisely, the scenario when these cells are equal to 1) and is based on the article [KP], which is also a joint work with my advisor.

For technical reasons we require in this case that if 2 ramifies then at most 2^1 divides N, if 3 ramifies at most 3^2 divides N. Besides, we need that the elliptic curve E does not have complex multiplication.

The main idea of this chapter is that in this setting we can find a suitable twist of the modular form f_E associated to E such that the level of the corresponding newform at the unstable primes of E ramifying in K is at most one, putting us in a situation where a classical Heegner construction is available. The main obstacle is that twisting by this character changes the geometric object we are considering and we end up with an abelian variety $A/\mathbb{Q}$ of GL_2 type which has dimension $d = 1, 2$ or 4 over $\mathbb{Q}$. This abelian variety is isogenous to E^d over some small controlled abelian extension $M/\mathbb{Q}$. Then we are left with the task of going back and obtain suitable points on E, as well as showing how we can explicitly compute them.

In Section 2.1 we analyze the existence of these distinguished twists in terms of the local type of representation, as explained in Subsection 1.6.1. Twisting by these characters provides us with a newform g (possibly with nebentypus) of a lower level and with an associated abelian variety A_g. In Proposition 2.1.1 we prove that there is an isogeny between A_g and E^d defined over M, and we explain the behavior of this isogeny under the action of the Galois group $\mathrm{Gal}(M/\mathbb{Q})$.

In Section 2.2 we study Heegner points in classical modular curves that are "between" $X_0(N)$ and $X_1(N)$ which parametrize the abelian variety A_g. Heegner points are precisely preimages of classical Heegner points on $X_0(N)$. We give a moduli interpretation for them, and we study their field of definition in Proposition 2.2.1. This field of definition is precisely the composition of the corresponding ring class field with the abelian extension $M/\mathbb{Q}$.

The next main ingredient is the more general form of Zhang's formula, given in Section 2.3. Studying the interplay of Heegner points and the isogeny between A_g and E^d we end up proving Theorem 2.3.2, which tells us that the (traces to K of the) Heegner points are non-torsion precisely when the derivative of the L-series at the center of symmetry does not vanish, in perfect concordance with both the classical

Heegner point scenario and the situation studied in Chapter 1.

In order to prove an analogue to the classical Kolyvagin's theorem, we need to be a little more careful, and this is carried out in Section 2.4. The compatibility relations are translated verbatim to the abelian variety A_g, but we have to deal with the issue that despite there is a number field K_g acting on A_g, it does not act naturally on E^d. The solution is to restrict the set of primes included in the compatibility relations as in Proposition 2.4.2, and with that choice of primes we check that Kolyvagin's theorem still holds (Theorem 2.4.3).

Next, in Section 2.5 we study the problem of explictly computing a 1-dimensional factor of A_g isogenous to E. First we study the theory of building blocks of Ribet [Rib77] and the explicit computations of Gonzalez-Lario [GL01]. Then we perform the explicit determination of certain "splitting map" that trivializes a 2-cocycle given by Jacobi sums. This splitting map allows us to compute a 1-dimensional factor of A_g and then find an isomorphism with the curve E defined over M. We end the chapter with a section of examples, showing the Heegner points constructed using this technique.

The construction of this chapter is interesting on its own, and can be used to move from a delicate situation to a not so bad one (reducing the conductor of the curve but paying the cost of adding a character in some cases). So, despite we focus on classical modular curves, the methods of this chapter can be easily applied to a wide variety of contexts, for example more general Shimura curves. In particular this construction also works when E_p has multiplicative reduction at p and $\varepsilon_p(E_p) = -1$. In addition, it is worth noting that this construction is fundamentally different from the method studied in [YZZ13].

In the articles [KP16] and [KP] we first dealt with the problem one prime at a time and then we showed how to do the general case. However, in this thesis the results are stated and proved in general, improving considerably the exposition, notation and internal organization of the work. Although this requires an extra layer of abstraction we believe that this manner of presenting the results is more clear and conceptual and will be more useful for reference in future applications.

Chapter 1

Heegner points on Cartan non-split curves

1.1 Cartan non-split groups

Let p be a prime number and let $\varepsilon \in \mathbb{Z}/p^n\mathbb{Z}$ be a quadratic nonresidue (respectively an odd number) if p is odd (respectively even). Given a natural number n we define the Cartan non-split ring modulo p^n as the ring

$$C_{ns}^{\varepsilon}(p^n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/p^n\mathbb{Z}) : a \equiv d, c \equiv b\varepsilon \bmod p^n \right\}$$

if p is odd and as

$$C_{ns}^{\varepsilon}(2^n) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/2^n\mathbb{Z}) : b \equiv a - d, c \equiv b\varepsilon \bmod 2^n \right\}$$

if $p = 2$.

We define the matrices $C_\varepsilon \in M_2(\mathbb{Z}/p^n\mathbb{Z})$ as

$$C_\varepsilon := \begin{cases} \left(\begin{smallmatrix} 0 & 1 \\ \varepsilon & 0 \end{smallmatrix}\right) & \text{if } p > 2, \\ \left(\begin{smallmatrix} 1 & 1 \\ \varepsilon & 0 \end{smallmatrix}\right) & \text{if } p = 2. \end{cases}$$

These matrices are annihilated by the polynomials P_ε, defined as

$$P_\varepsilon := \begin{cases} X^2 - \varepsilon & \text{if } p > 2, \\ X^2 - X - \varepsilon & \text{if } p = 2. \end{cases}$$

Embedding $\mathbb{Z}/p^n\mathbb{Z}$ diagonally into $M_2(\mathbb{Z}/p^n\mathbb{Z})$ we get

$$C_{ns}^{\varepsilon}(p^n) = \mathbb{Z}/p^n\mathbb{Z} + (\mathbb{Z}/p^n\mathbb{Z})C_{\varepsilon},$$

and the set of matrices in $M_2(\mathbb{Z}/p^n\mathbb{Z})$ that commute with C_ε is precisely $C_{ns}^{\varepsilon}(p^n)$. Furthermore, the group of invertible elements $(C_{ns}^{\varepsilon}(p^n))^\times$ is isomorphic to the cyclic group $\mathbb{F}_{p^2}^\times \times \mathbb{Z}/p^{2n-2}\mathbb{Z}$ and $\det : (C_{ns}^{\varepsilon}(p^n))^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$ is surjective. We also define the ring

$$M_{ns}^{\varepsilon}(p^n) := \left\{ A \in \mathrm{M}_2(\mathbb{Z}) \ : \ \bar{A} \in C_{ns}^{\varepsilon}(p^n) \right\},$$

where $\bar{A}$ denotes the reduction modulo p^n. The Cartan non-split group of level p^n, denoted by $\Gamma_{ns}^{\varepsilon}(p^n)$, is the group of determinant 1 matrices in $M_{ns}^{\varepsilon}(p^n)$.

Lemma 1.1.1. *Let $M \in \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ be such that $P_\varepsilon(M) = 0$. Then, there exists $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $\bar{A}M\bar{A}^{-1} = C_\varepsilon$.*

Proof. Clearly there exists $B \in \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ such that $B^{-1}MB = C_\varepsilon$. Since the determinant in $(C_{ns}^{\varepsilon}(p^n))^\times$ is surjective we can change the matrix B by a matrix A' of determinant 1 giving the same relation. The result follows from the fact that the reduction map $\mathrm{SL}_2(\mathbb{Z}) \mapsto \mathrm{SL}_2(\mathbb{Z}/p^n\mathbb{Z})$ is surjective. □

1.2 Cartan non-split curves

Let N and m be relatively prime natural numbers. Suppose that the factorization in primes of N is given by $p_1^{n_1} \dots p_k^{n_k}$. For each $1 \le i \le k$ let $\varepsilon_i \in \mathbb{Z}/p_i^{n_i}\mathbb{Z}$ be a quadratic nonresidue if p_i is odd and an odd number otherwise. Let ε be the vector $(\varepsilon_1, \dots, \varepsilon_k)$. As usual, let $M_0(m)$ be the ring of 2×2 integer matrices such that their $(2,1)$-entry is divisible by m.

Let $M^{\varepsilon}(N,m)$ be the ring $M_0(m) \cap (\cap_{i=1}^k M_{ns}^{\varepsilon_i}(p_i^{n_i}))$ and let $\Gamma^{\varepsilon}(N,m)$ be the group consisting of determinant one matrices inside $M^{\varepsilon}(N,m)$. Let $\mathcal{H}$ be the Poincaré upper half-plane, and consider the complex curve

$$Y^{\varepsilon}(N,m) := \Gamma^{\varepsilon}(N,m)\backslash\mathcal{H},$$

whose compactification obtained by adding a finite number of cusps is

$$X^{\varepsilon}(N,m) := \Gamma^{\varepsilon}(N,m)\backslash\mathcal{H}^*.$$

Let us denote $\hat{\mathbb{Z}} := \prod_p \mathbb{Z}_p$, and for every $\mathbb{Z}$-module R we define the adelization of R as $\hat{R} := R \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$. The complex points of $X^{\varepsilon}(N,m)$ can be identified with the double coset

$$\mathrm{GL}_2^+(\mathbb{Q})\backslash\mathcal{H}^* \times \mathrm{GL}_2(\hat{\mathbb{Z}})/\widehat{M^\varepsilon(N,m)}^\times.$$

Using that $\det : (C_{ns}^\varepsilon(p_i^{n_i}))^\times \to (\mathbb{Z}/p_i^{n_i}\mathbb{Z})^\times$ is surjective for every $1 \leq i \leq k$ we obtain that

$$\det : \widehat{M^\varepsilon(N,m)}^\times \to \hat{\mathbb{Z}}$$

is surjective. Thus, [Shi94, Proposition 6.27] tells us that $X^\varepsilon(N,m)$ is defined over $\mathbb{Q}$.

1.3 Moduli interpretation

We will give a moduli interpretation for the complex points of the Cartan non-split curves $X^\varepsilon(N,m)$. For other moduli interpretations see [Ser97, Appendix 5] and [RW14]. Consider tuples $(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_k)$, where $\mathcal{E}/\mathbb{C}$ is an elliptic curve, Q_m is a cyclic subgroup of order m of $\mathcal{E}$, and $\phi_i \in \mathrm{End}(\mathcal{E}[p_i^{n_i}])$ is such that $P_{\varepsilon_i}(\phi_i) = 0$. We identify two such tuples $(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_k)$, $(\mathcal{E}', Q_m', \phi_1', \ldots, \phi_k')$ if there exists an isomorphism of elliptic curves $\Psi : \mathcal{E} \to \mathcal{E}'$ that respects the level m structure and such that for every $1 \leq i \leq k$ the following diagram is commutative:

$$\begin{array}{ccc} \mathcal{E}[p_i^{n_i}] & \xrightarrow{\phi_i} & \mathcal{E}[p_i^{n_i}] \\ \downarrow{\scriptstyle \Psi} & & \downarrow{\scriptstyle \Psi} \\ \mathcal{E}'[p_i^{n_i}] & \xrightarrow[\phi_i']{} & \mathcal{E}'[p_i^{n_i}] \end{array}$$

Proposition 1.3.1. *The moduli problem of tuples $(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_k)$ is represented by the curve $Y^\varepsilon(N,m)$. The point $\Gamma^\varepsilon(N,m)\tau$ corresponds to $(\mathcal{E}_\tau, \langle \frac{1}{m} \rangle, \phi_{1\tau}, \ldots, \phi_{k\tau})$, where $\mathcal{E}_\tau = \mathbb{C}/\langle \tau, 1 \rangle$ and $\phi_{i\tau}$ is the endomorphism of $\mathcal{E}_\tau[p_i^{n_i}]$ whose matrix in the basis $B_\tau = \left\{ \frac{1}{p_i^{n_i}}, \frac{\tau}{p_i^{n_i}} \right\}$ is equal to the matrix C_{ε_i}.*

Proof. Let τ and τ' be points on $\mathcal{H}$ corresponding to the tuples $(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_k)$ and $(\mathcal{E}', Q_m', \phi_1', \ldots, \phi_k')$ respectively. To prove that the correspondence is well defined and injective it is enough to prove that two such pairs are isomorphic if and only if τ and τ' are equivalent under $\Gamma^\varepsilon(N,m)$. This is true because for every $1 \leq i \leq k$, the matrices that commute with C_{ε_i} are precisely those of $M_{ns}^{\varepsilon_i}(p_i{}^{n_i})$. Hence, the matrix of $\mathrm{SL}_2(\mathbb{Z})$ that gives rise to an isomorphism between $\mathcal{E}$ and $\mathcal{E}'$ must belong to $\Gamma^\varepsilon(N,m)$ as desired.

To prove surjectivity, consider any tuple $(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_k)$. Up to isomorphism we can assume that $\mathcal{E} = \mathbb{C}/\langle \tau, 1 \rangle$, where $\tau \in \mathcal{H}$. For every $1 \leq i \leq k$ Let $B =$

$\left\{\frac{1}{p_i^{n_i}}, \frac{\tau}{p_i^{n_i}}\right\}$ be a basis of $\mathcal{E}[p_i^{n_i}]$. By Lemma 1.1.1, there exists a matrix $A \in \mathrm{SL}_2(\mathbb{Z})$ such that $\bar{A}[\phi_i]_B\bar{A}^{-1} = C_{\varepsilon_i}$. In fact, by the Chinese Remainder Theorem we can take a matrix that works for every i. Therefore, the tuple is represented by the point $A\tau$. □

For any number field K, we say that the point $(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_k)$ is a K-rational point of the curve $X^{\varepsilon}(N, m)$ if $\mathcal{E}$, Q_m and $\{\phi_i\}_{1\leq i\leq k}$ are all defined over K. Recall that ϕ_i is defined over K if $\phi_i^{\sigma} = \phi_i$ for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$, i.e. $\phi_i(P^{\sigma}) = \phi_i(P)^{\sigma}$ for every $P \in \mathcal{E}[p_i^{n_i}]$ and every $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Definition 1.3.2. For every p_i there is an involution $\omega_{p_i}^{\varepsilon_i}$ given by

$$\omega_{p_i}^{\varepsilon_i}(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_i, \ldots, \phi_k) = (\mathcal{E}, Q_m, \phi_1, \ldots, Tr(C_{\varepsilon_i}) - \phi_i, \ldots, \phi_k).$$

These involutions are pairwise commutative, and commute with the classical Atkin-Lehner involutions.

1.4 Modular forms and Hecke operators

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function. If $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ and k is an integer, we define the k-th slash operator

$$f|_k[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)](z) := (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

Let $M_k(\Gamma)$ be the space of holomorphic functions which are invariant under the previous action for all elements in Γ and which are holomorphic at all the cusps, and let $S_k(\Gamma)$ be the subspace of cusp forms, i.e. those forms in $M_k(\Gamma)$ whose q-expansions at all the cusps have vanishing constant coefficient. Consider

$$\Gamma(N, m) := \Gamma(N) \cap \Gamma_0(m),$$

where $\Gamma(N)$ is the principal congruence subgroup of level N. Since this group is a subgroup of $\Gamma^{\varepsilon}(N, m)$ we get a reverse inclusion at the level of modular forms

$$S_k(\Gamma^{\varepsilon}(N, m)) \subset S_k(\Gamma(N, m)).$$

If $\alpha_N := \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $f \in S_k(\Gamma(N, m))$, $\tilde{f} := f|_k[\alpha_N]$ is a modular form with respect to

$$\tilde{\Gamma}(N, m) := (\alpha_N)^{-1}\Gamma(N, m)\alpha_N = \Gamma_0(N^2 m) \cap \Gamma_1(N).$$

Thus, slashing by α_N gives an isomorphism

$$S_k(\Gamma(N,m)) \cong S_k(\tilde{\Gamma}(N,m)).$$

We will specialize to the case $k=2$ from now on.

We want to understand the theory of Hecke operators acting on $S_2(\Gamma^\varepsilon(N,m))$. There are two ways to define them: the geometric way is to define them as correspondences on the modular curve and, via the moduli interpretation, translate this action to an action on modular forms and the algebraic way is to define them in terms of double coset operators. We will give both definitions and at the end of the section we will prove that they agree.

1.4.1 Geometric definition

Let n be a positive integer prime to Nm and let $(\mathcal{E}, Q_m, \phi_1, \ldots, \phi_k)$ be a tuple corresponding to a point on the curve $Y^\varepsilon(N,m)$. Define the Hecke operator

$$\mathscr{T}_n^\varepsilon((\mathcal{E}, Q_m, \ldots, \phi_i \ldots)) := \sum_{\psi:\mathcal{E}\to\mathcal{E}'} \left(\mathcal{E}', \psi(Q_m)\ldots, \frac{1}{n}\psi\circ\phi_i\circ\hat{\psi}, \ldots\right),$$

where the sum is over degree n isogenies $\psi : \mathcal{E} \to \mathcal{E}'$ of cyclic kernel, and $\hat{\psi}$ denotes the dual isogeny.

1.4.2 Algebraic definition

Following Shimura [Shi94] we define

$$\Delta_{Nm} := \{A \in \mathrm{M}_2(\mathbb{Z}) \,:\, \det(A) > 0 \text{ and } \gcd(Nm, \det(A)) = 1\},$$

and $\Delta^\varepsilon(N,m) := \Delta_{Nm} \cap M^\varepsilon(N,m)$. Moreover, consider

$$\Delta(N,m) := \left\{A \in \Delta_{Nm} \,:\, \bar{A} \equiv \left(\begin{smallmatrix}1 & 0\\ 0 & *\end{smallmatrix}\right) \bmod N \;;\; \bar{A} \equiv \left(\begin{smallmatrix}* & *\\ 0 & *\end{smallmatrix}\right) \bmod m\right\}.$$

Let $R(\Gamma^\varepsilon(N,m), \Delta^\varepsilon(N,m))$ and $R(\Gamma(N,m), \Delta(N,m))$ be the Hecke rings as defined in [Shi94, p.54].

Let $n \in \mathbb{Z}$ be relatively prime to Nm and let $B \in \Delta^\varepsilon(N,m)$ be any matrix with determinant congruent to n modulo Nm. Let $A_n^\varepsilon \in \mathrm{SL}_2(\mathbb{Z})$ be such that $A_n^\varepsilon \equiv B\left(\begin{smallmatrix}1 & 0\\ 0 & 1/n\end{smallmatrix}\right) \bmod Nm$. Slashing by the matrix A_n^ε defines an operator that we denote by υ_n^ε.

Lemma 1.4.1. *The operator v_n^ε defines an isomorphism*

$$S_2(\Gamma^\varepsilon(N,m)) \to S_2(\Gamma^{\varepsilon n^2}(N,m))$$

which depends only on the class of n modulo N (we are multiplying by $\bar{n}$ in each coordinate of ε). It is equal to the double coset operator $\Gamma^\varepsilon(N,m)A_n^\varepsilon\Gamma^{\varepsilon n^2}(N,m)$.

Proof. For every $1 \le i \le k$, $\bar{B} \in C_{ns}^{\varepsilon_i}(p_i^{n_i})$, and

$$\left(\begin{smallmatrix}1 & 0\\ 0 & 1/n\end{smallmatrix}\right)^{-1} C_{ns}^{\varepsilon_i}(p_i^{n_i}) \left(\begin{smallmatrix}1 & 0\\ 0 & 1/n\end{smallmatrix}\right) = C_{ns}^{\varepsilon_i n^2}(p_i^{n_i}),$$

thus the first assertion follows. Let B and B' be matrices in $\Delta^\varepsilon(N,m)$ of determinant n and n' respectively with $n \equiv n' \bmod N$. Choose any two matrices A_n^ε and $A_{n'}^\varepsilon$ corresponding to B and B' respectively. Clearly $A_n^\varepsilon {A_{n'}^\varepsilon}^{-1} \in \Gamma^\varepsilon(N,m)$, therefore, this matrix acts trivially. □

Let $h : R(\Gamma(Nm), \Delta(Nm)) \to R(\Gamma^\varepsilon(N,m), \Delta^\varepsilon(N,m))$ be the map given by

$$\Gamma(N,m)\beta\Gamma(N,m) \mapsto \Gamma^\varepsilon(N,m)A_{\det(\beta)}^\varepsilon\beta\Gamma^\varepsilon(N,m).$$

Proposition 1.4.2. *The map h is an isomorphism of Hecke rings.*

Proof. We have a map $h_1 : R(\Gamma^\varepsilon(N,m), \Delta^\varepsilon(N,m)) \to R(\mathrm{SL}_2(\mathbb{Z}), \Delta_{Nm})$ given by

$$\Gamma^\varepsilon(N,m)\alpha\Gamma^\varepsilon(N,m) \mapsto \mathrm{SL}_2(\mathbb{Z})\alpha\,\mathrm{SL}_2(\mathbb{Z}),$$

and a map $h_2 : R(\Gamma(N,m), \Delta(N,m)) \to R(\mathrm{SL}_2(\mathbb{Z}), \Delta_{Nm})$ given by

$$\Gamma(N,m)\beta\Gamma(N,m) \mapsto \mathrm{SL}_2(\mathbb{Z})\beta\,\mathrm{SL}_2(\mathbb{Z}).$$

Both maps are easily seen to be isomorphisms of Hecke rings by the same proof used in [Shi94, Proposition 3.31]. Moreover, h is equal to $h_1^{-1}h_2$, hence it is an isomorphism. □

We can consider the classical Hecke operators T_n acting on $S_2(\tilde{\Gamma}(N,m))$ for n relatively prime to Nm. Slashing by α_N we obtain the corresponding Hecke operator T_n acting on $S_2(\Gamma(N,m))$. In view of the above proposition we define the Hecke operator $\mathscr{T}_n^\varepsilon \in R(\Gamma^\varepsilon(N,m), \Delta^\varepsilon(N,m))$ as $h(T_n)$.

Lemma 1.4.3. *If $\beta \in \Delta(N,m)$, $\Gamma(N,m)\beta\Gamma(N,m)$ restricted to $S_2(\Gamma^{\varepsilon n^2}(N,m))$ is equal to $\Gamma^{\varepsilon n^2}(N,m)\beta\Gamma^\varepsilon(N,m)$.*

Proof. Mimics the proof of Lemma 1.4.1. □

Proposition 1.4.4. *As operators on* $S_2(\Gamma^\varepsilon(N,m))$, $\mathscr{T}_n^\varepsilon = T_n \circ \upsilon_n^\varepsilon$.

Proof. Using [Shi94, Proposition 3.7] we obtain

$$\Gamma^\varepsilon(N,m)A^\varepsilon_{\det(\beta)}\beta\Gamma^\varepsilon(N,m) = \Gamma^\varepsilon(N,m)A_n^\varepsilon\Gamma^{\varepsilon n^2}(N,m)\Gamma^{\varepsilon n^2}(N,m)\beta\Gamma^\varepsilon(N,m),$$

and the result follows from Lemma 1.4.1 and Lemma 1.4.3. □

Corollary 1.4.5. *If* $n \equiv 1 \bmod N$, $\mathscr{T}_n^\varepsilon = T_n$.

Proof. Since the matrix A_n^ε can be taken to be the identity, υ_n^ε is the identity map. □

Exactly in the same way as Proposition 1.4.4 we can prove the following proposition which will be useful for future reference.

Proposition 1.4.6. *For any* n *prime to* Nm, *the operators*

$$T_n : S_2(\Gamma^\varepsilon(N,m)) \to S_2(\Gamma^{\varepsilon/n^2}(N,m))$$

and

$$\upsilon_n^\varepsilon : S_2(\Gamma^\varepsilon(N,m)) \to S_2(\Gamma^{\varepsilon n^2}(N,m))$$

are morphisms of Hecke modules.

Proposition 1.4.7. *The geometric and algebraic definitions of Hecke operators coincide.*

Proof. We can restrict to n prime and relatively prime to Nm. It is enough to see that the set of representatives used in one definition can be taken as representatives for the other one. Take representatives for $\Gamma^\varepsilon(N,m)A_n^\varepsilon \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right) \Gamma^\varepsilon(N,m)$ modulo $\Gamma^\varepsilon(N,m)$. By [Shi94, Lemma 3.29 Part (5)] these are also representatives for

$$\mathrm{SL}_2(\mathbb{Z})A_n^\varepsilon \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right) \mathrm{SL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z}) \left(\begin{smallmatrix} 1 & 0 \\ 0 & n \end{smallmatrix}\right) \mathrm{SL}_2(\mathbb{Z})$$

modulo $\mathrm{SL}_2(\mathbb{Z})$. This set of representatives coincides with a set of representatives of cyclic isogenies of degree n. Each element is given by a matrix A of determinant n, and the dual isogeny is given by the matrix $\mathrm{Adj}(A)$. Both matrices belong to $\Delta^\varepsilon(N,m)$, thus, they commute with the matrix C_{ε_i} modulo $p_i^{n_i}$ and also $A\,\mathrm{Adj}(A) = n\,\mathrm{Id}$. Consequently, the two definitions coincide. □

1.5 Relation with classical newforms

Suppose that we are given a rational elliptic curve E of conductor N^2m without complex multiplication. By Wiles' modularity theorem, this corresponds to a normalized newform $f_E \in S_2(\Gamma_0(N^2m))$ with integer eigenvalues λ_n for the Hecke operators T_n such that $\lambda_p = p + 1 - \#E(\mathbb{F}_p)$ for every prime number p not dividing Nm.

Theorem 1.5.1. *There is a unique abelian subvariety of $Jac(X^\varepsilon(N,m))$ isogenous to E. This isogeny is compatible with the Hecke operators (prime to Nm) on each side.*

Proof. This is [Zha01, Theorem 1.2.2]. More precisely, one can easily check that our choice of Cartan non-split structure is one of the type of groups considered there. The proof relies in the local theory of newforms and test vectors. It is also worth noting that a more geometric version of this theorem is given by Chen-de Smit-Edixhoven ([Che98, Theorem 1], [Edi96, Theorem 1.1] [dSE00, Theorem 2]). □

Consequently, we can find $g_\varepsilon \in S_2(\Gamma^\varepsilon(N,m))$ such that

$$\mathscr{T}_n^\varepsilon\, g_\varepsilon = \lambda_n g_\varepsilon \ \text{ for all } n \text{ relatively prime to } Nm.$$

Theorem 1.5.1 plus "multiplicity one" for classical newforms in $S_2(\Gamma_0(N^2m))$ ([DS05, Theorem 5.8.2]) tell us that g_ε is well defined up to multiplication by a non-zero constant.

Our primary goal is to compute the Fourier expansion of g_ε. Recall that $\tilde{g}_\varepsilon$ belongs to $S_2(\tilde{\Gamma}(N,m))$ and this space has a basis consisting of eigenforms for the Hecke operators T_n with n relatively prime to Nm. Since $\mathscr{T}_n^\varepsilon = T_n$ if $n \equiv 1 \pmod N$, we can write $\tilde{g}_\varepsilon$ as a linear combination of elements in the set

$$\mathfrak{G}_E := \{f \in S_2(\tilde{\Gamma}(N,m)) \text{ eigenform} : \lambda_n = \lambda_n(f) \text{ for all } n \equiv 1 \pmod N\}.$$

An obvious family of elements in $\mathfrak{G}_E$ is obtained by *twisting* the modular form f_E by characters χ modulo N, since $T_n(f_E \otimes \chi) = \lambda_n \chi(n)(f_E \otimes \chi)$, and thus the form $f_E \otimes \chi$ has eigenvalue λ_n for T_n if $n \equiv 1 \pmod N$. In fact, this is essentially how all elements of $\mathfrak{G}_E$ are obtained, as the following proposition shows.

Proposition 1.5.2. *[Raj98, Corollary 1] Let $f \in S_2(\Gamma_0(N^2m), \psi)$ be an eigenform for the classical Hecke algebra, where ψ is a character modulo N. Let $g \in S_2^{new}(\Gamma_0(N^2m))$ be an eigenform without complex multiplication, and suppose that f and g have the same eigenvalues on the set of primes congruent to 1 modulo N. Then, there exists a Dirichlet character χ modulo N such that the eigenforms $g \otimes \chi$ and f have the same eigenvalues outside Nm.*

Applying this result to $g = f_E$ we obtain:

Theorem 1.5.3. *The set $\mathfrak{G}_E$ is the set of eigenforms that agree with $f_E \otimes \chi$ outside Nm for some character χ modulo N and $g_\varepsilon \in S_2(\Gamma^\varepsilon(N,m))$ can be written as a linear combination of the elements in $\mathfrak{G}_E$.*

We will come back to the problem of determining the set $\mathfrak{G}_E$ explicitly in the next section.

1.5.1 An elementary proof of Proposition 1.5.2

Let $A(Nm)$ be the monoid of natural numbers relatively prime to Nm, and let

$$\mathcal{U}_{Nm} := \{\mu : A(Nm) \to \mathbb{C} : \mu(1) = 1, \mu(ab) = \mu(a)\mu(b) \text{ if } a, b \text{ are relatively prime}\}.$$

We say that a function $\mu \in \mathcal{U}_{Nm}$ satisfies the condition $\heartsuit$ if for every $a \in A(Nm)$ there are an infinite number of primes ℓ such that $a \equiv \ell \bmod N$ and such that $\mu(\ell) \neq 0$. It is worth noting that this condition is satisfied whenever μ is a system of Hecke eigenvalues of a non-CM eigenform in $S_2(\Gamma_0(N^2m))$ due to Serre's open image theorem [Ser72].

Let $A^1(N,m)$ be the submonoid of $A(Nm)$ consisting of elements congruent to 1 modulo N.

Proposition 1.5.4. *Let $\mu, \lambda \in \mathcal{U}_{Nm}$ be such that μ is equal to λ when restricted to $A^1(N,m)$. If μ satisfies $\heartsuit$, there exists a Dirichlet character χ modulo N such that*

$$\mu = \chi\lambda.$$

Proof. We will give a proof in several easy steps.

- $\mu(a) = 0 \iff \lambda(a) = 0$:

  If $\lambda(a) = 0$, since μ satisfies $\heartsuit$, we can choose b such that $\gcd(a : b) = 1$, $ab \in A^1(N,m)$, and $\mu(b) \neq 0$. Using that μ and λ agree on $A^1(N,m)$ and μ is multiplicative, we get that $\mu(a) = 0$. For the reverse implication, suppose that $\mu(a) = 0$, and choose b exactly as before. Then, $\lambda(a)\lambda(b) = 0$, but if $\lambda(b)$ was 0 we would have that $\mu(b) = 0$ by the above proof, contradicting the choice of b.

  For $f \in \mathcal{U}_{Nm}$ define $Z_f := \{a \in A(Nm) : f(a) \neq 0\}$. We have just seen that $Z_\mu = Z_\lambda$. Consider $\chi : Z_\mu \to \mathbb{C}^\times$ given by sending a to $\frac{\mu(a)}{\lambda(a)}$.

- χ only depends on the class of a modulo N:

  Given $a, a' \in Z_\mu = Z_\lambda$ congruent modulo N, we can choose, as before, some $b \in Z_\mu$ such that b is relatively prime to aa' and $ab, a'b \in A^1(N, m)$. Since

  $$\mu(a)\mu(b) = \mu(ab) = \lambda(ab) = \lambda(a)\lambda(b),$$

  and the same holds replacing a with a' we obtain

  $$\chi(a) = \frac{\mu(a)}{\lambda(a)} = \frac{\mu(b)}{\lambda(b)} = \frac{\mu(a')}{\lambda(a')} = \chi(a').$$

- If $a, a' \in Z_\mu$, then $\chi(aa') = \chi(a)\chi(a')$:

  Choose b' relatively prime to a such that $b' \equiv a' \bmod N$ and $b' \in Z_\mu$. We have proved that $\chi(aa') = \chi(ab')$ and since both μ and λ are multiplicative this expression is equal to $\chi(a)\chi(b') = \chi(a)\chi(a')$.

- Finally, we extend χ to a character of $A(Nm)$ by $\chi(a) := \chi(a')$ for any $a' \in Z_\mu$ equivalent to a modulo N. This Dirichlet character gives the desired relation.

□

Applying this proposition to the system of Hecke eigenvalues $\{\lambda_n\}$ we obtain another proof of Proposition 1.5.2.

1.6 Computing eigenforms

In order to determine the elements in $\mathfrak{G}_E$ it is enough to know, for every character χ modulo N, the unique newform attached to $f_E \otimes \chi$. This question is purely local; that is, in order to understand when $f_E \otimes \chi$ is new at a prime p dividing N, we only need to study the p-th primary part of χ. This is better understood using the ℓ-adic local representation attached to the elliptic curve $E/\mathbb{Q}_p$.

1.6.1 Local representations

If $\ell \neq p$ is a prime number we consider the ℓ-adic Tate module $T_\ell(E) := \varprojlim E[\ell^n]$ which is a free $\mathbb{Z}_\ell$-module of rank 2. We also define $V_\ell(E) := T_\ell(E) \otimes_{\mathbb{Z}_\ell} \overline{\mathbb{Q}_\ell}$. This vector space comes equipped with an action of the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and we consider the contragradient of the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ on $V_\ell(E)$ given by

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{GL}_2(V_\ell(E)^*).$$

The theory, developed mainly by Grothendieck, Tate, Langlands and Deligne, shows that the ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ are in correspondence with the complex representations of the so called *Weil-Deligne* group of $\mathbb{Q}_p$. We will follow the exposition given by Rohrlich in [Roh94] as it is better suitable for applications to elliptic curves.

The *Weil group* of $\mathbb{F}_p$ is the subgroup $\mathcal{W}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ generated by the Frobenius automorphism. The inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is $I := \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p^{nr})$, where $\mathbb{Q}_p^{nr}$ is the maximal unramified extension of $\mathbb{Q}_p$.. The *Weil group* of $\mathbb{Q}_p$ is the subgroup $\mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ consisting of all elements that act on the residue field of $\overline{\mathbb{Q}_p}$ as a power of Frobenius. Let ϕ be the inverse of Frobenius and let Φ be some lifting of ϕ to $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$. Then,

$$\mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) = \bigcup_{n\in\mathbb{Z}} \Phi^n I.$$

We make $\mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ into a topological group by requiring that I is open, that the topology on I is the one inherited as a subspace of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, and also that left multiplication by Φ is an homeomorphism.

A representation of $\mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ is simply a continuous homomorphism

$$\sigma : \mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{GL}(V),$$

where V is a finite dimensional complex vector space. We say that σ is ramified or unramified depending on whether $\rho|_I$ is non-trivial or trivial respectively. The one dimensional representations are called characters, and we will identify them with characters of ${\mathbb{Q}_p}^\times$ by using the Artin isomorphism (given by sending p to Φ)

$${\mathbb{Q}_p}^\times \simeq \mathcal{W}^{\mathrm{ab}}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p).$$

We can define the Weil-Deligne group as a certain semidirect product between the Weil group and $\mathbb{C}$ but we will content ourselves with the definition of a what a complex representation of the Weil-Deligne group ought to be. This consists on a pair (σ, N) where σ is a representation of the Weil group acting on the finite dimensional complex vector space V and N is a nilpotent endomorphism of V that satisfies

$$\sigma(w)N\sigma(w)^{-1} = \omega(w)N,$$

for every $w \in \mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$, where ω is the unramified character given by sending Φ to p^{-1}.

The main point of this construction, as we remarked earlier, is that there is a one to one correspondence between isomorphism classes of representations of $\mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and isomorphism classes of ℓ-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$.

A representation (σ, N) of the Weil-Deligne group is called admissible if σ is semisimple and its called indecomposable if there is no proper subspace invariant under both $\mathcal{W}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and N.

All admissible representations of the Weil-Deligne group are of the form

$$\bigoplus_{j=1}^{s} \pi_j \otimes \mathrm{sp}(n_j),$$

where π_j is irreducible and sp denotes the special representation. Up to reordering, this decomposition is unique.

Now, coming back to ℓ-adic representations, recall that we had defined a 2-dimensional representation

$$\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{GL}_2(V_\ell(E)^*),$$

whose determinant is equal to ω^{-1} (this is obtained by looking at the Weil-pairing). Composing this representation with some embedding of $\overline{\mathbb{Q}_\ell}$ into $\mathbb{C}$, we obtain a 2-dimensional complex representation which corresponds to a 2-dimensional representation of the Weil-Deligne group, which turns out to to be admissible. Furthermore, a key aspect of the theory, is that this complex representation does not depend on ℓ (as long as $\ell \neq p$).

We will suppose from now on that p is odd. We have two very distinct possibilities for the elliptic curve $E/\mathbb{Q}_p$. It has either potentially multiplicative reduction or potentially good reduction.

- If $E/\mathbb{Q}_p$ has potentially multiplicative reduction there exists a quadratic extension of $\mathbb{Q}_p$ that defines a quadratic character $\varkappa$ of $Gal(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ such that the twist $E^\varkappa$ of E by $\varkappa$ has split multiplicative reduction. Using the theory of the Tate curve one can show that

  $$\rho_E \simeq \chi\omega^{-1} \otimes \mathrm{sp}(2).$$

  Moreover, the character χ is: trivial if $E/\mathbb{Q}_p$ has split multiplicative reduction, unramified but non-trivial if it has non-split multiplicative reduction, and ramified if it has additive reduction.

  These representations are called special (as they involve $sp(2)$) and are the only type in which the nilpotent endomorphism N is not trivial.

- If $E/\mathbb{Q}_p$ has potentially good reduction then we have that $N = 0$ so we just have a representation of the Weil group. If the representation is irreducible we say that is of *supercuspidal* type. On the other hand, if the representation is reducible, it must decompose as the direct sum of two 1-dimensional representations (i.e. characters) $\chi_1 \oplus \chi_2$. In addition, we must have $\chi_1\chi_2 = \omega^{-1}$. These representations are called *principal series*.

  There is a more down-to-earth distinction between these two types of representations, as long as $p > 3$. The principal series representations correspond to elliptic curves that have potentially good reduction over an *abelian* extension of $\mathbb{Q}_p$ and the supercuspidal representations correspond to the opposite scenario ([Roh93, Proposition 2]).

Suppose that $p > 3$. The above characterization allows us to find when $f_E \otimes \chi$ is not new at p, and in those cases, determine the corresponding newform of lower level. If the local representation is special, then one needs to compute the quadratic twist $\varkappa$ and the corresponding elliptic curve. If the representation is supercuspidal, as it is shown in [AL78], every twist will be new at p. Lastly, suppose that the representation is a principal series corresponding to the two characters χ_1, χ_2. Therefore, in order to twist and obtain a lower level newform the only possibilities are to choose either χ_1^{-1} or χ_2^{-1}. This characters, restricted to the inertia group, can be regarded as Dirichlet characters modulo p. We can explicitly compute them and the corresponding newform from the elliptic curve E using the results in [DD11, Example 5] as follows.

1. Compute v_p, the valuation at p of the discriminant of E. The order of the characters χ_1, χ_2 is $e := \frac{12}{\gcd(12, v_p)}$.

2. Let $L := \mathbb{Q}(x)/(x^e - p)$. Then, E attains good reduction at the prime ideal (x). Compute the characteristic polynomial $\chi_L(t) = t^2 - a_p t + p$ of Frobenius at such prime ideal by counting the number of points over the finite field. The two roots are the p-th coefficients we are looking for (since there are two forms, conjugate to each other), but we need to match each root with its corresponding character.

3. Let g be a generator of $\mathbb{F}_p^\times$, and let $L' := \mathbb{Q}(x)/(x^e - g \cdot p)$. As before, compute the characteristic polynomial $\chi_{L'}(t)$ for the prime ideal (x) (the curve is again unramified). Then the product of a root of $\chi_L(t)$ multiplied by the correct character (evaluated at g) must be a root of $\chi_{L'}(t)$.

For the primes $p = 2, 3$ we can do a similar analysis or just use brute force in order to look for the corresponding newforms.

Remark 1.6.1. The study of the ℓ-adic and Weil-Deligne representations is the key tool in order to define the L and ϵ-factors, the conductor, and the root number of an elliptic curve as shown in [Roh94].

1.6.2 Computing the Fourier expansion

In order to compute the Fourier expansion of G_ε we first compute all elements of $\mathfrak{G}_E$ as we explained in the previous subsection. Then, we take a formal linear combination of the forms in $\mathfrak{G}_E$ with variables x_j. Theorem 1.5.3 guarantees the existence of a linear combination of these forms giving rise to $\tilde{g}_\varepsilon$. Elements in $\mathfrak{G}_E$ are already invariant under $\Gamma(N) \cap \Gamma_0(m)$. In order to obtain forms invariant under the whole $\Gamma^\varepsilon(N, m)$ we take generators $\{\alpha_i\}_i$ of $\Gamma^\varepsilon(N, m)/(\Gamma(N) \cap \Gamma_0(m))$ and we try to impose invariance under the α_i's (evaluating at some points in $\mathcal{H}$). This gives a system of linear equations in the x_j's, whose solution set gives rise to a set S of modular forms containing g_ε. This set S is generated by the eigenforms in $S_2(\Gamma^\varepsilon(N, m))$ with the same eigenvalues as f_E for $n \equiv 1 \pmod N$. Since eigenforms in $S_2(\Gamma^\varepsilon(N, m))$ are in correspondence with newforms in $S_2(\Gamma_0(N^2 m))$, Proposition 1.5.2 says that S is generated by $\{g \otimes \varkappa\}_\varkappa$ where $\varkappa$ are *quadratic* characters modulo N such that $g \otimes \varkappa$ are again newforms of level $N^2 m$.

In order to pin down g_ε, let $p \mid N$ be an odd prime number such that $f_E \otimes \varkappa_p$ is new of level $N^2 m$, where $\varkappa_p$ is the quadratic character modulo p. If q is a non-square modulo p, the operator $\mathscr{T}_q^\varepsilon = T_q \upsilon_q^\varepsilon$ acts as λ_q on the subspace spanned by g_ε and as $-\lambda_q$ on the subspace spanned by the eigenform corresponding to $(f_E \otimes \varkappa_p)$. For $p = 2$ a similar computation can be done. Each condition halves the dimension and altogether they determine g_ε up to a constant.

Remark 1.6.2. If π_p is supercuspidal it is easier to halve the dimension. If $\epsilon_p = 1$ (resp. $\epsilon_p = -1$) then the sum is supported at twists of f_E with even p-part (resp. odd p-part). The reason for this is that the sign of the classical Atkin Lehner involution at p_i is the same as the sign of the corresponding involution $\omega_{p_i}^{\varepsilon_i}$, which can be realized as a matrix A_n^ε with $n \equiv -1 \bmod p_i^{n_i}$ and $n \equiv 1 \bmod N/p_i^{n_i}$.

By [Pac13, Corollary 3.3], the local sign at p changes when twisting f_E by $\varkappa_p$ like $-\left(\frac{-1}{p}\right) = -\varkappa_p(-1)$. Therefore, the supports of the forms corresponding to f_E and $f_E \otimes \varkappa_p$ are disjoint.

1.7 The field of modular functions

For $a \in \mathbb{Q}^2$ and $z \in \mathcal{H}$ define

$$f_a(z) := \frac{g_2(z,1)g_3(z,1)}{\Delta(z,1)} \wp(a \left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right); z, 1),$$

where $\wp(-;\omega_1,\omega_2)$ is the classical Weierstrass function associated to the lattice $L = \langle \omega_1, \omega_2 \rangle$; $g_2(L) = 60G_4(L)$, and $g_3(L) = 140G_6(L)$ correspond to the lattice functions $G_{2n}(L) := \sum_{w \in L} \frac{1}{w^{2n}}$ ([Shi94, Section 6.1]). These functions satisfy $f_a(\gamma(z)) = f_{a\gamma}(z)$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. For every $n \in \mathbb{N}$, let $\mathcal{F}_n$ be the field of modular functions of level n rational over $\mathbb{Q}(\xi_n)$ (where ξ_n is a primitive n-th root of unity), which by [Shi94, Proposition 6.1] is equal to

$$\mathcal{F}_n = \mathbb{Q}(j, f_a \mid a \in (n^{-1}\mathbb{Z}^2)/\mathbb{Z}^2, a \notin \mathbb{Z}^2).$$

In addition, set $\mathcal{F} := \cup_n \mathcal{F}_n$.

Proposition 1.7.1 ([Shi94], Proposition 6.21)**.** *For every $u \in \mathrm{GL}_2(\hat{\mathbb{Z}})$ there exists an element $\tau(u) \in \mathrm{Gal}(\mathcal{F}/\mathcal{F}_1)$ such that $f_a^{\tau(u)} = f_{au}$ for every non-zero $a \in \mathbb{Q}^2/\mathbb{Z}^2$, τ coincides with the Artin map given by class field theory on $\overline{\mathbb{Q}}$ and $h^{\tau(\gamma)} = h \circ \gamma$ for all $h \in \mathcal{F}$ and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.*

Consider the field

$$\mathcal{F}^{\varepsilon}(N,m) := \left\{ h \in \mathcal{F} \,:\, h^{\tau(u)} = h,\ \forall u \in \mathbb{Q}^{\times} \widehat{M^{\varepsilon}(N,m)}^{\times} \right\}.$$

Since

$$\mathbb{Q}^{\times}\Gamma^{\varepsilon}(N,m) = (\mathbb{Q}^{\times} \widehat{M^{\varepsilon}(N,m)}^{\times}) \cap \mathrm{GL}_2^{+}(\mathbb{Q}),$$

$\mathcal{F}^{\varepsilon}(N,m)$ is the field of rational modular functions for $\Gamma^{\varepsilon}(N,m)$ ([Shi94, Proposition 6.27]). We also define the field of rational modular functions for $\Gamma(N,m)$ as

$$\mathcal{F}(N,m) := \left\{ h \in \mathcal{F} \,:\, h^{\tau(u)} = h,\ \forall u \in \mathbb{Q}^{\times} \widehat{M(N,m)}^{\times} \right\}.$$

Elements in $\mathcal{F}(N,m)$ have a q-expansion with respect to $q = e^{\frac{2\pi i z}{N}}$ with coefficients belonging to $\mathbb{Q}(\xi_N)$. Since $\mathcal{F}^{\varepsilon}(N,m) \subset \mathcal{F}(N,m)$, the rational modular functions for $\Gamma^{\varepsilon}(N,m)$ have the same property.

For every n relatively prime to N consider the automorphism $\sigma_n \in Gal(\mathbb{Q}(\xi_N)/\mathbb{Q})$ given by

$$\sigma_n(\xi_N) = {\xi_N}^{n^{-1}}.$$

This Galois automorphism depends only on the class of n modulo N and its action on f_a is given by $f_{a\left(\begin{smallmatrix}1 & 0\\ 0 & n^{-1}\end{smallmatrix}\right)}$ ([Shi94, Theorem 6.6]).

Recall that

$$A_n^\varepsilon \equiv B\left(\begin{smallmatrix}1 & 0\\ 0 & n^{-1}\end{smallmatrix}\right) \bmod Nm,$$

where $B \in \Delta^\varepsilon(N,m)$. Combining this with Proposition 1.7.1 we find that the elements h of $\mathcal{F}^\varepsilon(N,m)$ satisfy that

$$\sigma_n(h) = h|[A_n^\varepsilon].$$

Conversely, elements of $\mathcal{F}(N,m)$ that satisfy this last relation belong to $\mathcal{F}^\varepsilon(N,m)$, since

$$\mathbb{Q}^\times \widehat{M^\varepsilon(N,m)}^\times = \Delta^\varepsilon(N,m)\mathbb{Q}^\times \widehat{M(N,m)}^\times.$$

Remark 1.7.2. This argument applies to weight 2 modular forms, dividing by the (meromorphic) Eisenstein series E_2 that has integer Fourier coefficients and transforms nicely under the full modular group.

Definition 1.7.3 (Rational Modular Forms)**.** A form $f \in S_2(\Gamma^\varepsilon(N,m))$ is called *rational* if its q-expansion at every cusp belongs to $\mathbb{Q}(\xi_N)$ and $\sigma_n(f) = f|_2[(A_n^\varepsilon)]$ for every n relatively prime to Nm.

1.7.1 Cusps

An analogous computation to the characterization of rational modular forms shows that the curve $X^\varepsilon(N,m)$ has $\phi(N)$ cusps over the ∞ cusp, all of them defined over $\mathbb{Q}(\xi_N)$ and conjugate by $\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})$. If $\sigma_n \in \mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})$, then $\sigma_n(\infty) = A_n^\varepsilon\infty$.

1.7.2 Rational differential forms

Recall that if X is a curve defined over $\mathbb{Q}$, a differential form defined over $\mathbb{Q}$ is a differential form which is locally of the form fdg, where f and g are meromorphic functions defined over $\mathbb{Q}$.

Proposition 1.7.4. *If $f \in S_2(\Gamma^\varepsilon(N,m))$ is rational, it defines a rational meromorphic differential form $f(q)\frac{dq}{q}$ on $X^\varepsilon(N,m)$, where $q = e^{\frac{2\pi iz}{N}}$.*

Proof. Note that

$$f(q)\frac{dq}{q} = \frac{2\pi i}{N} f(z)dz = \frac{f(z)}{\frac{Nj'(z)}{2\pi i}}dj.$$

Since $\frac{Nj'}{2\pi i}$ is a rational meromorphic function with respect to $\mathrm{SL}_2(\mathbb{Z})$ (of weight two), $\frac{f}{\frac{Nj'}{2\pi i}}$ lies in $\mathcal{F}^\varepsilon(N,m)$. Also j belongs to $\mathcal{F}^\varepsilon(N,m)$ so $f(q)\frac{dq}{q}$ is rational. □

1.8 Normalization

Proposition 1.8.1. *Let $f \in \mathbb{C}\mathcal{F}^\varepsilon(N,m)$. Let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ satisfy $\sigma|_{\mathbb{Q}(\xi_N)} = \sigma_n$. Then $\sigma(f) \in \mathbb{C}\mathcal{F}^{\varepsilon n^2}(N,m)$*

Proof. This follows from the fact that the groups $\Gamma^\varepsilon(N,m)$ and $\Gamma^{\varepsilon n^2}(N,m)$ are conjugate by the matrix $\left(\begin{smallmatrix}1 & 0\\ 0 & n^{-1}\end{smallmatrix}\right)$.

□

Proposition 1.8.2. *Let $f \in \mathbb{C}\mathcal{F}^\varepsilon(N,m)$ and let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ satisfy $\sigma|_{\mathbb{Q}(\xi_N)} = \sigma_n$. Then $\sigma(v_t^\varepsilon(f)) = v_t^{\varepsilon n^2}(\sigma(f))$.*

Proof. Choose A_t^ε in such a way that its $(1,2)$ entry is divisible by n. It is easy to see that $\left(\begin{smallmatrix}1 & 0\\ 0 & n\end{smallmatrix}\right) A_t^\varepsilon \left(\begin{smallmatrix}1 & 0\\ 0 & 1/n\end{smallmatrix}\right)$, which belongs to $\mathrm{SL}_2(\mathbb{Z})$ by our choice of A_t^ε, gives the same action on f_a as $A_t^{\varepsilon n^2}$ (since both matrices are easily seen to be equivalent modulo Nm). □

Corollary 1.8.3. *We have that $\mathscr{T}_t^{\varepsilon n^2}(\sigma(f)) = \sigma(\mathscr{T}_t^\varepsilon(f))$.*

Proof. This follows from the previous proposition and the fact that σ commutes with T_t (this is easily obtained by looking at the action on q-expansions). □

As we remarked before, these arguments apply to weight 2 also.

Corollary 1.8.4. *$\sigma(g_\varepsilon) \in S_2(\Gamma^{\varepsilon n^2}(N,m))$ has the same eigenvalues as g_ε, i.e.*

$$\mathscr{T}_t^{\varepsilon n^2}(\sigma(g_\varepsilon)) = \lambda_t \sigma(g_\varepsilon).$$

Corollary 1.8.5. *If t is relatively prime to Nm where $tn \equiv 1 \bmod N$ then there exists $c_t \in \mathbb{C}$ such that $T_t g_\varepsilon = c_t \sigma(g_\varepsilon)$.*

Proof. By Proposition 1.4.6, $T_t(g_\varepsilon)$ is an eigenform in $S_2\left(\Gamma^{\varepsilon n^2}(N,m)\right)$ with the same eigenvalues as g_ε. By Corollary 1.8.3, $\sigma(g_\varepsilon)$ is an eigenform whose eigenvalues are the same as those from g_ε. The result now follows from multiplicity one. □

We normalize g_ε in such a way that its first Fourier coefficient is 1. In that case we have the following theorem.

Theorem 1.8.6. *g_ε has a q-expansion belonging to $\mathbb{Q}(\xi_N)$.*

Proof. Let $\ell \equiv 1 \bmod N$ be such that $\lambda_\ell \neq 0$, and let $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}(\xi_N))$ be arbitrary. By Corollary 1.8.5, there exists $c_\ell \in \mathbb{C}$ such that

$$T_\ell g_\varepsilon = c_\ell \sigma(g_\varepsilon).$$

We know that $T_\ell g_\varepsilon = \lambda_\ell g_\varepsilon$ (by Corollary 1.4.5). Looking at the first Fourier coefficient, we get that $c_\ell = \lambda_\ell$ and hence $g_\varepsilon = \sigma(g_\varepsilon)$. Since $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{Q}(\xi_N))$ is arbitrary it follows that the q-expansion of g_ε lies in the desired extension. □

Theorem 1.8.7. *There exists a non-zero constant $d \in \mathbb{Q}(\xi_N)$ such that dg_ε is rational. Such constant is unique up to multiplication by a non-zero rational number.*

Proof. By Serre's open image theorem, every number n relatively prime to N is equivalent modulo N to a n' such that $\lambda_n \neq 0$. Then for each n prime to Nm there exists $c_n \in \mathbb{Q}(\xi_N)$, which only depends on the class of n modulo N, such that $T_n g_\varepsilon = \lambda_n c_n \sigma_{n^{-1}}(g_\varepsilon)$. This defines

$$c : \mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q}) \to (\mathbb{Q}(\xi_N))^\times$$

by sending $\sigma_{n^{-1}}$ to c_n. This is a 1-cocycle in $H^1(\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q}), (\mathbb{Q}(\xi_N))^\times)$, which is trivial by Hilbert's 90 theorem. Thus, c is a 1-coboundary, that is, there exists some $d \in (\mathbb{Q}(\xi_N))^\times$ such that $c(\sigma) = \sigma(d)/d$, and it is clear that d satisfies the required conditions. The last statement is obvious. □

Note that even for a rational modular form, it is not clear how to choose the rational multiple of it which should correspond to "$a_1 = 1$" in the classical case. The best one can do is to choose the coefficients to be algebraic integers and have no common rational integer factor.

Definition 1.8.8. The *proper normalization* of g_ε is the unique (up to sign) normalization G_ε of g_ε that satisfies:

- G_ε is a rational newform.
- The Fourier expansion of G_ε has algebraic integer coefficients.
- If $n \in \mathbb{Z}$ and $n \geq 2$, $\frac{G_\varepsilon}{n}$ does not have integral coefficients.

Remark 1.8.9. Once we know the q-expansion of g_ε, using the explicit version of Hilbert's 90 Theorem we easily obtain a proper-normalization. If $\gcd(n, N) = 1$, the n-th coefficient b_n of G_ε satisfies

$$b_n = \lambda_n \sigma_{n^{-1}}(b_1).$$

Thus, we can obtain the *exact* Fourier expansion once we have found $b_1 \in \mathbb{Q}(\xi_N)$ and the coefficients at the various p_i's.

1.9 Eichler-Shimura

The Eichler-Shimura construction associates to G_ε the abelian variety

$$\mathscr{A}_{G_\varepsilon} := \mathrm{Jac}(X^\varepsilon(N,m))/(I_{G_\varepsilon}\,\mathrm{Jac}(X^\varepsilon(N,m))),$$

where I_{G_ε} is the kernel of the morphism $R(\Gamma^\varepsilon(N,m),\Delta^\varepsilon(N,m)) \to \mathbb{Z}$ which is given by sending $\mathscr{T}_n^\varepsilon$ to the eigenvalue λ_n. For every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})$ we have the diagram

$$\begin{array}{ccc} X^\varepsilon(N,m) & \xhookrightarrow{i_\sigma} & \mathrm{Jac}(X^\varepsilon(N,m)) \\ & \searrow^{\Phi^\varepsilon_{N,m,\sigma}} & \downarrow \\ & & \mathscr{A}_{G_\varepsilon} \end{array}$$

where i_σ is the map sending P to $(P)-(\sigma(\infty))$ and the vertical map is the classical Abel-Jacobi map given by integrating the differential form $G_\varepsilon(q)\frac{dq}{q}$ against paths induced by divisors. By Proposition 1.7.4 this differential is rational, thus the abelian variety $\mathscr{A}_{G_\varepsilon}$ is of dimension 1, and by Theorem 1.5.1 it is isogenous to E. This elliptic curve is called the optimal quotient of $\mathrm{Jac}(X^\varepsilon(N,m))$. The lattice Λ_ε formed by the integrals of closed paths in $X^\varepsilon(N,m)$ of the form $G_\varepsilon\frac{dq}{q}$ is called the lattice of periods of G_ε and we have $\mathscr{A}_{G_\varepsilon} = \mathbb{C}/\Lambda_\varepsilon$.

Since the cusps of the Cartan curve are defined over $\mathbb{Q}(\xi_N)$ (and are Galois conjugate over that field) the maps i_σ will not be defined over $\mathbb{Q}$. Nevertheless, we can consider the following diagram

$$\begin{array}{ccc} X^\varepsilon(N,m) & \xhookrightarrow{\iota} & \mathrm{Jac}(X^\varepsilon(N,m)) \\ & \searrow^{\Phi^\varepsilon_{N,m}} & \downarrow \\ & & \mathscr{A}_{G_\varepsilon} \end{array}$$

where ι is the map sending P to $\sum_{\sigma\in\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})}(P)-(\sigma(\infty))$. Therefore, the dot map (which we still call *modular parametrization*) is defined over $\mathbb{Q}$.

If ω_ε is a holomorphic differential on $\mathbb{C}/\Lambda_\varepsilon$ its pullback under $\Phi^\varepsilon_{N,m,\sigma}$ is a constant multiple of $G_\varepsilon(q)\frac{dq}{q}$ (by multiplicity one), where $q = e^{\frac{2\pi i z}{N}}$. This constant c_ε will be called the *Manin constant*, and it does not depend on the choice of σ. Moreover, since $\mathscr{A}_{G_\varepsilon}$ and $G_\varepsilon(q)\frac{dq}{q}$ are rational and $\Phi^\varepsilon_{N,m} = \sum_\sigma \Phi^\varepsilon_{N,m,\sigma}$ is defined over $\mathbb{Q}$, the Manin constant must be a rational number.

Proposition 1.9.1. *Let $\Phi_\omega : \mathbb{C}/\Lambda_\varepsilon \to E$ be the Weierstrass uniformization. Then*

$\Phi^{\varepsilon}_{N,m}(\tau) = \Phi_{\omega}(z_\tau)$, *where*

$$z_\tau = c_\varepsilon \left(\frac{2\pi i}{N} \left(\sum_{\sigma_n \in \mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})} \int_{\infty}^{(A_n^{\varepsilon})^{-1}\tau} \sigma_n(G_\varepsilon)(z)dz \right) \right).$$

Proof. This follows from [Dar04, Proposition 2.11] and the identity

$$\int_{\sigma_n(\infty)}^{\tau} G_\varepsilon(q)\frac{dq}{q} = \int_{\infty}^{(A_n^{\varepsilon})^{-1}\tau} G_\varepsilon|_2[A_n^{\varepsilon}](q)\frac{dq}{q} = \int_{\infty}^{(A_n^{\varepsilon})^{-1}\tau} \sigma_n(G_\varepsilon(q))\frac{dq}{q}.$$

□

1.10 Heegner points

Let $E/\mathbb{Q}$ be an elliptic curve and let $\mathscr{O} = \langle 1, \omega \rangle$ be an order in an imaginary quadratic field K. We say that the pair $(E, \mathscr{O})$ satisfies the *Cartan-Heegner hypothesis* if the following holds:

- The conductor of E is $N^2 m$ where $\gcd(N, m) = 1$.
- The discriminant d of $\mathscr{O}$ is prime to Nm.
- Every prime dividing m is split in $\mathscr{O}$.
- Every prime dividing N is inert in $\mathscr{O}$.

Note that $\mathscr{O}$ satisfies the classical Heegner hypothesis at the primes dividing m but not at the primes dividing N, therefore, we will not be able to construct Heegner points on $X_0(N^2 m)$ if $N > 1$. Given a pair $(E, \mathscr{O})$ satisfying the Cartan-Heegner hypothesis we will use the letters N and m to denote the factorization of the conductor of E as in the definition and we also say that $\mathscr{O}$ satisfies the Cartan-Heegner hypothesis with respect to (N, m).

Definition 1.10.1. A Heegner point on $X^{\varepsilon}(N, m)$ is a tuple $[\mathscr{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha]$ where

- $\mathscr{O}$ satisfies the Cartan-Heegner hypothesis with respect to (N, m),
- $[\mathfrak{a}]$ is an element in $\mathrm{Pic}(\mathscr{O})$ (this defines an elliptic curve $E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ with complex multiplication by $\mathscr{O}$),

- $\mathfrak{m}$ is a cyclic ideal in $\mathscr{O}$ of norm m,
- multiplication by $\alpha \in \mathscr{O}/N$ gives rise to $\phi_\alpha \in \prod_{p_i|N} \mathrm{End}(E_\mathfrak{a}[p_i^{n_i}])$ such that $\phi_{\alpha i}$ is a root of P_{ε_i} for every $1 \leq i \leq k$.

A Heegner point on E with endomorphism ring $\mathscr{O}$ is the image of a Heegner point with endomorphism ring $\mathscr{O}$ in $X^\varepsilon(N,m)$ under the modular parametrization $\Phi^\varepsilon_{N,m}$.

Note that since every prime dividing m is split in $\mathscr{O}$, there is a cyclic ideal of norm $\mathfrak{m}$ and since every prime divding N is inert we can find α with the desired properties.

From the classical theory of complex multiplication it is clear that Heegner points belong to $X^\varepsilon(N,m)(H_\mathscr{O})$ where $H_\mathscr{O}$ is the ring class field associated to $\mathscr{O}$. Moreover, we have the following proposition that describes the Galois and Atkin-Lehner actions on them.

Proposition 1.10.2. *Let $[\mathscr{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha]$ be a Heegner point.*

1. *If τ denotes complex conjugation, then $(\mathscr{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha)^\tau = (\mathscr{O}, [\mathfrak{a}^{-1}], \overline{\mathfrak{m}}, \phi_{\bar{\alpha}})$*
2. *Let $[\mathfrak{b}]$ be a fractional ideal, and let $\sigma_\mathfrak{b} \in \mathrm{Gal}(H_\mathscr{O}/K)$ be the Artin symbol associated to $[\mathfrak{b}]$. Then*

$$(\mathscr{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha)^{\sigma_\mathfrak{b}} = (\mathscr{O}, [\mathfrak{a}\mathfrak{b}^{-1}], \mathfrak{m}, \phi_\alpha)$$

3. *Consider $\omega_N := \prod_{i=1}^k \omega_{p_i}^{\varepsilon_i}$. Then,*

$$\omega_N(\mathscr{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha) = (\mathscr{O}, [\mathfrak{a}], \mathfrak{m}, \phi_{\bar{\alpha}}).$$

4. *The classical Atkin-Lehner operator ω_m acts as*

$$\omega_m(\mathscr{O}, [\mathfrak{a}], \mathfrak{m}, \phi_\alpha) = (\mathscr{O}, [\mathfrak{a}\mathfrak{m}^{-1}], \overline{\mathfrak{m}}, \phi_\alpha).$$

Proof. The first two items follow from [Ser67] (since $\mathfrak{m}$ and α are defined over K); the third one follows from the definition of the $\omega_{p_i}^{\varepsilon_i}$ and the last one is [Gro84, Formula 5.2]. □

Remark 1.10.3. Fixing a CM elliptic curve $E_\mathfrak{a}$ we have 2^k choices for α, and also we have different choices for $\mathfrak{m}$ as in the classical case. These choices are permuted simply transitively by the corresponding Atkin-Lehner involutions.

We will give another description of Heegner points on $X^{\varepsilon}(N,m)$ that is more suitable for our computations.

Recall that a matrix $M \in M_2(\mathbb{Z})$ with $\mathrm{Tr}(M) = \mathrm{Tr}(\omega)$ and $\det(M) = \mathrm{Nm}(\omega)$ provides an embedding $\mathscr{O} \hookrightarrow M_2(\mathbb{Z})$ given by sending ω to M. Heegner points on $X^{\varepsilon}(N,m)$ with endomorphism ring $\mathscr{O}$ are precisely the points τ on the upper half plane which are fixed by a matrix $M \in M^{\varepsilon}(N,m)$ satisfying the above conditions.

More precisely, let $\{\mathfrak{a}_i\}$ be a set of representatives of the class group of $\mathscr{O}$ and let $\omega_i \in \mathcal{H}$ be such that $\mathfrak{a}_i = \langle 1, \omega_i \rangle$. Let M_{ω_i} be the set of matrices in $M_2(\mathbb{Z})$ that fixes ω_i, which is an order isomorphic to $\mathscr{O}$. Then, M_{ω_i} contains a matrix N_i satisfying $\mathrm{Tr}(N_i) = \mathrm{Tr}(\omega)$ and $\det(N_i) = \mathrm{Nm}(\omega)$. We will show that there exists $A_i \in \mathrm{SL}_2(\mathbb{Z})$ such that $A_i N_i {A_i}^{-1} \in M^{\varepsilon}(N,m)$. In that case, the point $\tau_i = A_i\omega_i$ is a Heegner point on $X^{\varepsilon}(N,m)$ with endomorphism ring $\mathscr{O}$ as wanted.

The matrices A_i are computed in the following way:

- At a prime p dividing m, we chose $A_i^{(p)}$ modulo $p^{v_p(m)}$ of determinant one, taking N_i to an upper triangular matrix. This can be done, since the roots of the characteristic polynomial of N_i are different and they both belong to $\mathbb{Z}/p^{v_p(m)}$ (since every prime that divides m splits in $\mathscr{O}$).

- At an odd prime p_i dividing N, since p_i is inert in K, the characteristic polynomial of N_i is irreducible. If $N_i = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$, then we want the matrix A_i to satisfy

$$A_i \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) = \begin{pmatrix} \frac{\alpha+\delta}{2} & \sqrt{\frac{D}{4\varepsilon_i}} \\ \varepsilon_i\sqrt{\frac{D}{4\varepsilon_i}} & \frac{\alpha+\delta}{2} \end{pmatrix} A_i \text{ (modulo } p_i^{n_i}),$$

  where D is the discriminant of $\mathscr{O}$. We just chose A_i as a matrix in 4 indeterminates and search for a non-zero solution of the system (the determinant of this system is zero, so there is always such a solution). If the determinant is not 1, we just multiply the matrix via an appropriate matrix, as in the proof of Lemma 1.1.1. If 2 divides N we can make an analogous computation.

Lastly, the Chinese Remainder Theorem gives a matrix in $\mathrm{SL}_2(\mathbb{Z}/N^2m\mathbb{Z})$ satisfying our hypotheses, and we lift it to the matrix A_i in $\mathrm{SL}_2(\mathbb{Z})$.

It is worth noting that the above construction depends on the choice of a square root of $D/4\varepsilon_i$ modulo $p_i^{n_i}$. In order to obtain a whole orbit under the action of $\mathrm{Gal}(H_{\mathscr{O}}/K)$ one has to be careful and choose the same square root for each representative.

1.11 Heegner systems

Using the geometric interpretation of Hecke operators as described in section 1.4.1 we have the following formula for Hecke operators acting on Heegner points, analogous to the one given in [Gro84, Section 6]:

Proposition 1.11.1. *For ℓ relatively prime to Nm we have that*

$$\mathscr{T}_\ell^\varepsilon[\mathscr{O}, \mathfrak{a}, \mathfrak{m}, \phi_\alpha] = \sum_{\mathfrak{a}/\mathfrak{b}\cong\mathbb{Z}/\ell} [End(\mathfrak{b}), \mathfrak{b}, \mathfrak{m} \cdot End(\mathfrak{b}) \cap End(\mathfrak{b}), \phi_\alpha].$$

Fix an elliptic curve E as before, and let K be an imaginary quadratic field with maximal order $\mathscr{O}_K$ such that the pair $(E, \mathscr{O}_K)$ satisfies the Cartan-Heegner hypothesis. Let n be a positive integer relatively prime to $\mathrm{Cond}(E) \cdot \mathrm{disc}(K)$. Let $\mathscr{O}_n$ be the unique order in K of conductor n and let H_n be the corresponding ring class field. Then, $(E, \mathscr{O}_n)$ satisfies the Cartan-Heegner hypothesis, so, it gives rise to a set of Heegner points $\mathrm{HP}(n) \subset E(H_n)$.

Proposition 1.11.2. 1. *Let n be an integer and let ℓ be a prime number, both relatively prime to $\mathrm{Cond}(E) \cdot \mathrm{disc}(K)$. Consider any $P_{n\ell} \in \mathrm{HP}(n\ell)$. Then, there exist points $P_n \in E(H_n)$ and (when $\ell \mid n$) $P_{n/\ell} \in \mathrm{HP}(n/\ell)$ such that*

- *If $\ell \nmid n$ is inert in K,*
$$Tr_{H_{n\ell}/H_n} P_{n\ell} = \lambda_\ell P_n,$$
- *If $\ell = \lambda\bar{\lambda} \nmid n$ is split in K,*
$$Tr_{H_{n\ell}/H_n} P_{n\ell} = (\lambda_\ell - Frob_\lambda - Frob_\lambda^{-1}) P_n.$$
- *If $\ell \mid n$,*
$$Tr_{H_{n\ell}/H_n} P_{n\ell} = \lambda_\ell P_n - P_{n/\ell}.$$

2. *There exists $\sigma \in \mathrm{Gal}(H_n/K)$ such that*

$$P_n{}^\tau \equiv -\operatorname{sign}(E, \mathbb{Q}) P_n{}^\sigma \bmod E(H_n)_{tors},$$

where τ denotes complex conjugation.

Proof. From Proposition 1.10.2, Proposition (1.11.1) and the discussion in between, the result follows quite formally. See for example [Gro91, Propositions 3.7 and 5.3] or [Dar04, Section 3.4] and [GZ86, Section II.1]. □

Definition 1.11.3. A *Heegner system* attached to (E, K) is a collection of points $P_n \in E(H_n)$ (one for each positive integer n relatively prime to $\mathrm{Cond}(E) \cdot \mathrm{disc}(K)$) which satisfies the conditions of the previous proposition.

If $(E, \mathscr{O}_K)$ satisfies the Cartan-Heegner hypothesis, we can obtain a Heegner system by choosing the same $\mathfrak{m}$, $\alpha \in \mathscr{O}_K$, and the trivial class in $H_{\mathscr{O}_n}$ for every $\mathscr{O}_n$ with n relatively prime to $\mathrm{Cond}(E) \cdot \mathrm{disc}(K)$. More precisely, consider

$$x_n := [\mathscr{O}_n, [1], \mathfrak{m} \cap \mathscr{O}_n, \phi_\alpha],$$

and set $P_n := \Phi^{\varepsilon}_{N,m}(x_n) \in E(H_n)$, which satisfies the required conditions. Given a Heegner system, we can apply Kolyvagin's machinery to get the following result:

Theorem 1.11.4 ([Dar04], Theorem 10.1)**.** *Let $\{P_n\}$ be the Heegner system attached to $(E, \mathscr{O})$ as constructed above. Suppose that E does not have complex multiplication. Define $P_K = Tr_{H_1/K} P_1 \in E(K)$. If P_K is non-torsion then:*

- *The Mordell-Weil group $E(K)$ is of rank one.*
- *The Shafarevich-Tate group of E/K is finite.*

Lastly, we have the following version of Gross-Zagier formula.

Theorem 1.11.5 ([Zha01])**.** *The point P_K is non-torsion if and only if*

$$L'(E/K, 1) \neq 0.$$

Remark 1.11.6. Zhang's formula provides a precise relation between $L'(E/K, 1)$ and the height of the Heegner point on the *Jacobian* of the Cartan non-split curve. In order to obtain a relation between this and the height of the Heegner point on the elliptic curve (and thus giving an explicit version of the BDS conjecture in this context) we need to have a better understanding of the periods of newforms, the Manin constant and the degree of the modular parametrization.

1.12 Examples

Consider the elliptic curve $E = 75.c1$ (in [LMF13] notation) given by the equation

$$y^2 + y = x^3 - x^2 - 8x - 7$$

and let f_E be the corresponding newform of level 75. Fix $\varepsilon = 2$, which is a non-square modulo 5. The local representation at the prime $p = 5$ is supercuspidal, so when we are looking for the q-expansion of the modular form $G_2 \in S_2(\Gamma^2(5,3))$ as in Theorem 1.5.3 we only have to consider a linear combination of the four twists of f_E by characters of conductor 5, and in fact, we only need to consider the odd characters since the local sign at 5 is equal to -1, as explained in Section 1.6. Solving the system we find that the first Fourier coefficient (after applying the normalization procedure) is equal to $\xi_5 + 2{\xi_5}^2 - 2{\xi_5}^3 - {\xi_5}^4$. The n-th Fourier coefficient is equal to 0 if n is divisible by 5 (since no oldforms appear in the supercuspidal case) and for n relatively prime to 5 we use the formula $b_n = \lambda_n \sigma_{n^{-1}}(b_1)$. The elliptic curve E is the optimal quotient in this case, and the Manin constant is equal to $1/5$.

- The maximal order in the field $K = \mathbb{Q}(\sqrt{-2})$ satisfies the Cartan-Heegner hypothesis, and it has class number 1. The point $\tau = (5 + \sqrt{-2})/9$ is fixed by the matrix $\left(\begin{smallmatrix} 5 & -3 \\ 9 & -5 \end{smallmatrix}\right) \in \Gamma^2(5,3)$ and it has the same characteristic polynomial as $\sqrt{-2}$. Computing $\Phi^2_{5,3}(\tau)$ we obtain a numerical approximation of the point

$$\left[\frac{311}{288}, \frac{-1}{2} - \frac{5 \cdot 3823\sqrt{-2}}{2^8 \cdot 3^3}\right],$$

  which is a non-torsion point on $E(K)$.

- The maximal order in the field $K = \mathbb{Q}(\sqrt{-23})$ satisfies the Cartan-Heegner hypothesis, and it has class number 3. A set of representatives of an orbit of Heegner points under the class group is given by $\tau_1 = (25 + \sqrt{-23})/12, \tau_2 = (5 + \sqrt{-23})/12, \tau_3 = (-785 + \sqrt{-23})/162$. The image under the modular parametrization of each of these points lies in $E(H)$, where H is generated by $\mathbb{Q}(\sqrt{-23})$ and a root of $X^3 - X - 1$. The x-coordinates of these points are the three roots of $263327X^3 + 1235357X^2 + 2186718X + 2200495$. Furthermore, adding these points together we find a non-torsion point on $E(K)$

$$\left[\frac{-27687600319369}{23 \cdot 2^6 \cdot 3^6 \cdot 37^2 \cdot 73^2}, \frac{-1}{2} + \frac{5 \cdot 25992536347803546497\sqrt{-23}}{23^2 \cdot 2^9 \cdot 3^9 \cdot 37^3 \cdot 73^3}\right].$$

Chapter 2

The ramified case

2.1 Twisting by characters

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N^2m where $\gcd(N,m)=1$ and N is the product of pairwise distinct odd primes $p_1,\dots,p_k$. We will assume that E does not have complex multiplication.

If E has potentially multiplicative reduction at a prime p dividing N, then there exists a newform $g_p \in S_2(\Gamma_0((N^2/p)m))$, such that $f_E = g_p \otimes \varkappa_p$, where $\varkappa_p$ is the unique quadratic character modulo p.

If E has potentially good reduction over an abelian extension at a prime dividing N, as we explained in Subsection 1.6.1, we have that

$$\rho_{E,\ell}|_I = \psi_p \oplus \psi_p^{-1}$$

Note that since the representation is independent of ℓ, the trace lies in $\mathbb{Q}$. Therefore, ψ_p satisfies a quadratic relation, hence its image lies in a quadratic field contained in a cyclotomic extension (because ψ_p has finite order). This gives the following possibilities for the order of inertia of ψ_p: 1, 2, 3, 4 or 6.

- Clearly ψ_p cannot have order 1 (since otherwise the representation is unramified at p).
- If ψ_p has order 2, ψ_p must be the (unique) quadratic character ramified at p. In this case the quadratic twist E_p of E by ψ_p has good reduction.
- If ψ_p has order 3, 4 or 6, there exists a newform $g_p \in S_2(\Gamma_0((N^2/p)m), \psi_p^{-2})$, such that $f_E = g_p \otimes \psi_p$.

Doing this for every prime dividing N, we obtain a character $\psi := \prod_i \psi_{p_i}$ and a newform $g \in S_2(\Gamma_0(N' \cdot m), \psi^{-2})$ such that $f_E = g \otimes \psi$, where N' is the divisor of N consisting precisely of the prime factors p of N such that E_p does not have good reduction at p. The field of coefficients K_g of the newform g will be the same as the field generated by the image of the character ψ. Since the characters ψ_p have order $2, 3, 4$ or 6, K_g can be equal to $\mathbb{Q}, \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(i)$ or $\mathbb{Q}(i, \sqrt{-3})$. Let d be the degree of K_g over $\mathbb{Q}$ and let $g = \sum a_n q^n$ be the q-expansion of g at the infinity cusp.

There is an abelian variety $A_g/\mathbb{Q}$ attached to g via the Eichler-Shimura construction with an action of K_g on it, i.e. there is an embedding $\theta : K_g \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A_g) \otimes \mathbb{Q}$. The variety A_g can be defined as the quotient $J_1(N' \cdot m)/I_g J_1(N' \cdot m)$ where I_g is the annihilator of g under the Hecke algebra acting on the Jacobian. Moreover, the L-series of A_g satisfies the relation

$$L(A_g/\mathbb{Q}, s) = \prod_{\sigma \in \mathrm{Gal}(K_g/\mathbb{Q})} L(\sigma(g), s).$$

The variety A_g has dimension d and is $\mathbb{Q}$-simple. However, it is not absolutely simple. The variety A_g is isogenous over $M := \overline{\mathbb{Q}}^{\ker \psi}$ to E^d. In fact, over the extension M the character ψ becomes trivial, so we have the equality of L-series $L(A_g/M, s) = L(E, s)^d$ which implies, by Falting's isogeny theorem, that A_g and E^d are isogenous over M. The abelian extension $M/\mathbb{Q}$ is of exponent t (where t is a divisor of 12) and we have an embedding

$$\iota : \mathbb{Z}[\mu_t] \hookrightarrow K_g,$$

where μ_t is a primitive t-th root of unity. Following the work of Kida [Kid95], we define for every $\chi \in \widehat{\mathrm{Gal}(M/\mathbb{Q})} := \mathrm{Hom}(\mathrm{Gal}(M/\mathbb{Q}), \mathbb{C}^\times)$ an abelian variety $A_{g,\chi}$ (called the twist of A_g by χ), which is an abelian variety defined over $\mathbb{Q}$ together with a map $\Theta_\chi : A_g \to A_{g,\chi}$ that is an isomorphism defined over M and such that

$$\Theta_\chi^\tau \iota \chi(\tau) = \Theta_\chi,$$

for every $\tau \in \mathrm{Gal}(M/\mathbb{Q})$. Moreover, we have that

$$A_g \hookrightarrow \mathrm{Res}_{M/\mathbb{Q}}(A_g \otimes_{\mathbb{Q}} M) \sim \prod_{\chi \in \widehat{\mathrm{Gal}(M/\mathbb{Q})}} A_{g,\chi}.$$

In addition, by looking at the L-series side, for every character χ of the form $\sigma(\psi)$ with $\sigma \in \mathrm{Gal}(K_g/\mathbb{Q})$ we have that $L(A_{g,\chi}, s)$ has a factor of the form $L(E, s)$. Combining this with the above diagram we obtain the following crucial result:

Proposition 2.1.1. *There is an isogeny $\omega : A_g \to E^d$ defined over M such that*

$$(\pi_i\omega)^\tau \iota\sigma_i(\psi)(\tau) = \pi_i\omega,$$

where π_i denotes the i-th projection and $\{\sigma_i\}_i$ is some ordering of $\mathrm{Gal}(K_g/\mathbb{Q})$.

2.2 Heegner points

Let $\mathscr{O}_c$ be the order of conductor c in an imaginary quadratic field K. We say that the pair $(E, \mathscr{O}_c)$ satisfies the *ramified Heegner hypothesis* if the following hold:

- c is prime to $N'm$.
- Every prime dividing m is split in $\mathscr{O}$.
- Every prime dividing N' is ramified in $\mathscr{O}$.
- If a prime p divides N' and ψ_p has order 2, then the local sign of $E \otimes \psi_p$ is equal to 1.

This hypothesis corresponds precisely to the dark grey cells in Table 2.

We can consider the character ψ as a Dirichlet character $\psi : (\mathbb{Z}/N')^\times \to \mathbb{C}^\times$. Extend the character to $(\mathbb{Z}/N' \cdot m)^\times$ by composing with the canonical projection $(\mathbb{Z}/N' \cdot m)^\times \to (\mathbb{Z}/N')^\times$ and define

$$\Gamma_0^\psi(N' \cdot m) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N' \cdot m) : \psi^{-2}(a) = 1 \right\}.$$

Let $X_0^\psi(N' \cdot m)$ be the modular curve obtained as the quotient of the extended upper half plane $\mathcal{H}^*$ by this group. This modular curve has a model defined over $\mathbb{Q}$ and it coarsely represents the moduli problem of parametrizing quadruples $(\mathcal{E}, Q, C, [s])$ where

- $\mathcal{E}$ is an elliptic curve over $\mathbb{C}$,
- Q is a cyclic subgroup of $\mathcal{E}(\mathbb{C})$ of order m,
- C is a cyclic subgroup of $\mathcal{E}(\mathbb{C})$ of order N',
- $[s]$ is an orbit in $C \setminus \{0\}$ under the action of $\ker(\psi^{-2}) \subset (\mathbb{Z}/N')^\times$.

There is a canonical map $\Pi : X_0^{\psi}(N' \cdot m) \to X_0(N' \cdot m)$ which is the forgetful map in the moduli interpretation. This map has degree $[L : \mathbb{Q}]$, where $L := \overline{\mathbb{Q}}^{ker(\psi^2)}$.

As in the classical case, there exists a rational modular parametrization

$$\Phi_g : X_0^{\psi}(N' \cdot m) \to A_g$$

given by sending a point into the Jacobian by choosing the rational ∞ cusp and then projecting onto A_g using the classical Abel-Jacobi map.

Our strategy is to construct Heegner points on $X_0^{\psi}(N' \cdot m)$, which will be the preimages of the classical Heegner points under Π, push them through the modular parametrization Φ_g to the abelian variety A_g and finally project them onto the elliptic curve E.

Since $(E, \mathscr{O}_c)$ satisfies the ramified Heegner hypothesis there is a cyclic ideal $\mathfrak{n}'$ of norm N' (which is unique since there is only one prime of K above each prime divisor of N') and a cyclic ideal $\mathfrak{m}$ of norm m (there are several choices, permuted by the classical Atkin-Lehner operators w_q for the primes q dividing m).

A classical Heegner point on $X_0(N' \cdot m)$ corresponds to a triple

$$P_{\mathfrak{a}} = (\mathscr{O}_c, \mathfrak{n}'\mathfrak{m}, [\mathfrak{a}]) \in X_0(N' \cdot m)(H_c),$$

where $[\mathfrak{a}] \in \mathrm{Pic}(\mathscr{O}_c)$. Such point is represented by the elliptic curve $E_{\mathfrak{a}} = \mathbb{C}/\mathfrak{a}$ and its $\mathfrak{n}'\mathfrak{m}$ torsion points $E_{\mathfrak{a}}[\mathfrak{n}'\mathfrak{m}]$ (which are isomorphic to $(\mathfrak{a}(\mathfrak{n}'\mathfrak{m})^{-1}/\mathfrak{a})$) are defined over H_c. Using the aforementioned moduli interpretation, points on $X_0^{\psi}(N' \cdot m)$ are represented by quadruples $(\mathscr{O}_c, \mathfrak{n}'\mathfrak{m}, [\mathfrak{a}], [t])$ where $[t]$ is an orbit under $\ker(\psi^{-2})$ inside $(\mathscr{O}_c/\mathfrak{n}')^{\times}$.

The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/H_c)$ on $E_{\mathfrak{a}}[\mathfrak{n}'\mathfrak{m}]$ gives a map $\mathrm{Gal}(\overline{\mathbb{Q}}/H_c) \to (\mathfrak{a}(\mathfrak{n}'\mathfrak{m})^{-1}/\mathfrak{a})^{\times}$. Composing such map with the character ψ^{-2} gives

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/H_c) \to (\mathfrak{a}(\mathfrak{n}'\mathfrak{m})^{-1}/\mathfrak{a})^{\times} \overset{\psi^{-2}}{\to} \mathbb{C}^{\times}.$$

Its kernel corresponds to an extension of degree $[L : \mathbb{Q}]$ of H_c. Let $\tilde{H}_c = H_c M$.

Proposition 2.2.1. *The $[L : \mathbb{Q}]$ points $\Pi^{-1}(P_{\mathfrak{a}})$ lie on $X_0^{\psi}(N' \cdot m)(\tilde{H}_c)$ and are permuted transitively under the action of $\mathrm{Gal}(\tilde{H}_c/H_c)$.*

Proof. By the theory of complex multiplication Heegner points lie in the composition of H_c and the ray class field $K_{\mathfrak{n}'}$. This is equal to $H_c(\xi_{N'})$, where $\xi_{N'}$ is a N'-th root of unity. It is enough to understand what happens one prime at a time. Take any prime p dividing N' and set $L_p := \overline{\mathbb{Q}}^{ker(\psi_p^2)}$. We are looking for an extension of H_c of degree $[L_p : \mathbb{Q}]$ contained inside $H_c(\mu_p)$. By genus theory, $\mathbb{Q}(\sqrt{p^*}) \subset H_c$, therefore the desired extension is $H_c\overline{\mathbb{Q}}^{ker(\psi_p)}$. Composing these extensions we end up with $H_c\overline{\mathbb{Q}}^{ker(\psi)} = H_c M = \tilde{H}_c$. □

2.3 Zhang's formula

Let $(E, \mathscr{O}_c)$ satisfy the ramified Heegner hypothesis. Let χ be a ring class character of $\mathrm{Gal}(H_c/K)$ and consider the character $\tilde{\chi} : \mathrm{Gal}(\tilde{H}_c/K) \to \mathbb{C}^\times$ given by $\tilde{\chi} = \chi\psi$. This satisfies $\tilde{\chi}|_{\mathbb{A}_\mathbb{Q}^\times} = \psi^2$.

Theorem 2.3.1. *With the above notation $L(g, \tilde{\chi}, s)$ vanishes at odd order at $s = 1$. Furthermore, consider the Heegner point*

$$(\mathscr{O}_c, \mathfrak{n}'\mathfrak{m}, [\mathfrak{a}], 1) \in X_0^\psi(N' \cdot m)(\tilde{H}_c),$$

and denote by P_c its image under the modular parametrization Φ_g. Then

$$P^{\tilde{\chi}} = \sum_{\sigma \in \mathrm{Gal}(\tilde{H}_c/K)} \bar{\tilde{\chi}}(\sigma) P_c^\sigma \in (A_g(\tilde{H}_c) \otimes \mathbb{C})^{\tilde{\chi}}$$

is non-torsion if and only if $L'(g, \tilde{\chi}, 1) \neq 0$. If $L'(g, \tilde{\chi}, 1) \neq 0$, $P^{\tilde{\chi}}$ generates $(A_g(\tilde{H}_c) \otimes \mathbb{C})^{\tilde{\chi}}$ over $K_g \otimes \mathbb{C}$.

Proof. See [TZ03, Theorem 4.3.1], [Zha10], and [YZZ13, Theorem 1.4.1]. □

We can compute the projection $\pi_1\omega$ to the elliptic curve E using Proposition 2.1.1 as follows.

$$\pi_1\omega(P^{\tilde{\chi}}) = \sum_{\sigma \in \mathrm{Gal}(\tilde{H}_c/K)} \bar{\chi}(\sigma)\pi_1\omega(\bar{\psi}(\sigma)P^\sigma) = \sum_{\sigma \in \mathrm{Gal}(\tilde{H}_c/K)} \bar{\chi}(\sigma)(\pi_1\omega(P))^\sigma.$$

This point will be non-torsion if and only if $P^{\tilde{\chi}}$ is non-torsion, since in that case $(A_g(\tilde{H}_c) \otimes \mathbb{C})^{\tilde{\chi}}$ has rank one over $K_g \otimes \mathbb{C}$ and there are $[K_g : \mathbb{Q}]$ projections.

Note that the point $\pi_1\omega(P^{\tilde{\chi}})$ belongs to $(E(H_c) \otimes \mathbb{C})^\chi$. Finally, since $L(g, \tilde{\chi}, s)$ is equal to $L(E, \chi, s)$, and using Theorem 2.3.1 we have proved the following theorem.

Theorem 2.3.2. *The point $\pi_1\omega(P^{\tilde{\chi}})$ belongs to $(E(H_c) \otimes \mathbb{C})^\chi$. In addition, it is non-torsion if and only if $L'(E/K, \chi, 1) \neq 0$.*

2.4 Heegner systems

As in the classical case, the family of Heegner points constructed using different orders satisfy certain compatibilities.

Proposition 2.4.1. *Let ℓ be a prime such that $\ell \nmid N' \cdot m$ and ℓ is inert in K. Then for every Heegner point $P_{c\ell} \in A_g(\tilde{H}_{c\ell})$ there exists a Heegner point $P_c \in A_g(\tilde{H}_c)$ with*

$$\mathrm{Tr}_{\tilde{H}_{c\ell}/\tilde{H}_c} P_{c\ell} = \theta(a_\ell) P_c, \tag{2.1}$$

where a_ℓ is the ℓ-th Fourier coefficient of g.

Proof. The proof mimics the classical case one (see [Gro91, Proposition 3.7]). □

To construct a point on E, we have to apply $\pi_1\omega$ to a point on A_g. But K_g does not act on E! To overcome this problem, we restrict to primes ℓ which split completely in L. Let $Q_c := \mathrm{Tr}_{\tilde{H}_c/H_c} \pi_1\omega(P_c) \in E(H_c)$.

Proposition 2.4.2. *Let ℓ be a prime such that $\ell \nmid N' \cdot m$, ℓ is inert in K and ℓ splits completely in L. Then for every Heegner point $Q_{c\ell} \in E(H_{c\ell})$ there exists a Heegner point $Q_c \in E(H_c)$ such that*

$$\mathrm{Tr}_{H_{c\ell}/H_c} Q_{c\ell} = a_\ell Q_c.$$

Proof. Apply $\mathrm{Tr}_{\tilde{H}_c/H_c} \pi_1\omega$ to equation (2.1). Since $M \subset \tilde{H}_c$, ω commutes with the trace from $\tilde{H}_{c\ell}/\tilde{H}_c$. Furthermore, since ℓ splits completely in L we know that $a_\ell \in \mathbb{Q}$. Combining these observations we get

$$\mathrm{Tr}_{\tilde{H}_c/H_c} \mathrm{Tr}_{\tilde{H}_{c\ell}/\tilde{H}_c} \pi_1\omega(P_{c\ell}) = a_\ell Q_c.$$

Lastly,

$$\mathrm{Tr}_{\tilde{H}_c/H_c} \mathrm{Tr}_{\tilde{H}_{c\ell}/\tilde{H}_c} \pi_1\omega(P_{c\ell}) = \mathrm{Tr}_{H_{c\ell}/H_c} \mathrm{Tr}_{\tilde{H}_{c\ell}/H_{c\ell}} \pi_1\omega(P_{c\ell}),$$

and this expression equals $\mathrm{Tr}_{H_{c\ell}/H_c} Q_{c\ell}$ as claimed. □

The previous results are enough for proving a Kolyvagin-type theorem.

Theorem 2.4.3 (Kolyvagin, Bertolini-Darmon)**.** *If $\pi_1(\omega(P^{\tilde{\chi}}))$ is non-torsion, then* $\dim_{\mathbb{C}}(E(H_c) \otimes \mathbb{C})^\chi = 1$.

Proof. The proof is very similar to the one given in [BD90, Theorem 2.2] with the following remarks (using their notation and terminology): any p-descent prime is automatically unramified in L hence $K(E[p])$ and L are disjoint. We also require special rational primes ℓ to split completely in $L/\mathbb{Q}$. Recall that L is totally real, hence such condition is compatible with the other ones and special primes do exist. The first assertion of Proposition 3.2 in [BD90] is exactly our Proposition 2.4.2, and the second one follows from [Gro91] (proof of Proposition 3.7). With these modifications, the proof of [BD90] holds. □

2.5 Splitting maps

The goal of this section is to explicitly determine a 1-dimensional factor of A_g over M corresponding to the elliptic curve E, in order to compute some numerical examples.

The modular form g has inner twists [Rib77, Proposition 3.2]. More precisely, for $\sigma \in \mathrm{Gal}(K_g/\mathbb{Q})$, we know that $\sigma(a_\ell) = a_\ell \chi_\sigma(\ell)$ for every ℓ not dividing the level of g, where $\chi_\sigma(\ell) = \sigma(\psi^{-1})(\ell)/(\psi^{-1}(\ell))$.

We partition the set of primes dividing N into three mutually disjoint subsets:

- $A := \{p \mid N : \psi_p^2 \text{ has order } 1\}$
- $B := \{p \mid N : \psi_p^2 \text{ has order } 2\}$
- $C := \{p \mid N : \psi_p^2 \text{ has order } 3\}$

Moreover, define $\psi_A := \prod_{p \in A} \psi_p$ and define ψ_B, ψ_C in an analogous way. Note that $\psi = \psi_A \psi_B \psi_C$. Also, define generators σ_B, σ_C of $\mathrm{Gal}(\mathbb{Q}(i, \sqrt{-3})/\mathbb{Q})$ by

$$\sigma_B(i) = -i,\ \sigma_B(\sqrt{-3}) = \sqrt{-3},$$
$$\sigma_C(i) = i,\ \sigma_C(\sqrt{-3}) = -\sqrt{-3}.$$

With these definitions we have

- $\chi_{\sigma_B}^{-1} = \psi/\sigma_B(\psi) = \psi_B/\bar{\psi_B} = \psi_B^2$,
- $\chi_{\sigma_C}^{-1} = \psi_C^2$,
- $\chi_{\sigma_B\sigma_C}^{-1} = \psi_B^2\psi_C^2$.

Recall that we had defined

$$L = \overline{\mathbb{Q}}^{\ker \psi^2} = \overline{\mathbb{Q}}^{\cap_\sigma \ker \chi_\sigma}.$$

Following the work of González and Lario [GL01], this is the field of definition of all endomorphisms of the abelian variety A_g and, in particular, the abelian variety A_g is isogenous over L to some power of an elliptic curve, called a building block of A_g. We want to obtain an explicit description of this building block. Afterward it will be easy to find an isomorphism (defined over M) between the building block and E.

Let f_σ be the conductor of the Dirichlet character χ_σ. If η is an endomorphism of $J(\Gamma_1(N' \cdot m))$ (or one of its quotients), we denote by η^* the pullback it induces

on differential forms. For every $\sigma \in \mathrm{Gal}(K_g/\mathbb{Q})$ we will consider the element $\eta_\sigma \in \mathbb{Q} \otimes \mathrm{End}_L(A_g)$ whose action on differentials is given by

$$\eta_\sigma^* := \sum_{u \bmod f_\sigma} \chi_\sigma^{-1}(u) a_u,$$

where a_u denotes the operator given by slashing by the matrix $\left(\begin{smallmatrix} 1 & u/f_\sigma \\ 0 & 1 \end{smallmatrix}\right)$.

Consider the 2-cocycle $c(\sigma, \tau)$ given by

$$\frac{G(\chi_\sigma^{-1}) G(\sigma(\chi_\tau^{-1}))}{G(\chi_{\sigma\tau}^{-1})},$$

where $G(\chi)$ denotes the Gauss sum of the character χ. In [GL01] the authors show the existence of a suitable splitting map $\beta : \mathrm{Gal}(K_g/\mathbb{Q}) \to {K_g}^\times$ such that

$$c(\sigma, \tau) = \frac{\beta(\sigma)\sigma(\beta(\tau))}{\beta(\sigma\tau)},$$

for every $\sigma, \tau \in \mathrm{Gal}(K_g/\mathbb{Q})$.

We define the element

$$w := \sum_\sigma \beta(\sigma)^{-1} \eta_\sigma.$$

This gives rise to the abelian subvariety wA_g, which is a building block. Moreover, we have an explicit action of this element in terms of the Fourier expansions of g and its Galois conjugates and the map β ([GL01, Theorem 2.1]). So we are left with the task of finding such map β explicitly.

It is clear that $\beta(Id) = 1$, and evaluating the cocycle c at pairs of the form (σ, σ^{-1}) we obtain, using that a Gauss sum of conductor M has absolute value $\sqrt{M}$ and that the characters χ_σ are even, that $\beta(\sigma)\beta(\sigma)^\sigma = \mathrm{cond}(\chi_\sigma^{-1})$. In order to find such elements we prove the following lemma.

Lemma 2.5.1. *Let $p \in B \cup C$ and let a_p be the p-th Fourier coefficient of g. Then $a_p \in \mathbb{Q}(i)$ if $p \in B$ and $a_p \in \mathbb{Q}(\sqrt{-3})$ if $p \in C$. In any case a_p has norm p.*

Proof. Looking at the curve E over $\mathbb{Q}_p$, the coefficient a_p is one of the roots of the characteristic polynomial attached to the Frobenius element in the minimal (totally ramified) extension where E acquires good reduction (see for example Section 3 of [DD11]). Since the norm of the local uniformizer in such extension is p (because the extension ramifies completely) the result follows. □

According to the previous remarks it is sensible to define

$$\beta(\sigma_B) := \prod_{p\in B} a_p; \quad \beta(\sigma_C) := \prod_{p\in C} a_p.$$

Computing $c(\sigma_B, \sigma_C)$ and using that if χ, χ' are two characters of conductors M and M' with $(M : M') = 1$, we have

$$G(\chi \cdot \chi') = \chi(M')\chi'(M)G(\chi)G(\chi'),$$

we are forced to set

$$\beta(\sigma_B\sigma_C) := \left(\prod_{p\in B\cup C} a_p\right)\left(\psi_B^2(\prod_{p\in C} p)\right)\left(\psi_C^2(\prod_{p\in B} p)\right).$$

With this definition it is easy to see that β satisfies the desired relations, providing us with the explicit splitting map that allows to effectively determine the building block. Once we have obtained the building block, we find the 1-dimensional lattice of periods, from which we can compute explicitly the isomorphism (defined over M) with our original elliptic curve E.

Remark 2.5.2. Different choices of the splitting map β give rise to different building blocks.

Remark 2.5.3. It can be easily seen that with this choice of splitting map, the maps $\beta(\sigma_B)^{-1}\eta_{\sigma_B}$ and $\beta(\sigma_C)^{-1}\eta_{\sigma_C}$ coincide with the Atkin-Lehner operators $W_{\prod_{p\in B} p}$ and $W_{\prod_{p\in C} p}$ respectively.

2.6 Examples

Consider the elliptic curve $E = 575.c1$ given by the equation

$$y^2 + y = x^3 - x^2 - 458x + 3943,$$

and let f_E be the corresponding newform of level 575. The local representation at the prime $p = 5$ is a principal series and we find, as explained in Subsection 1.6.1, the newform $g \in S_2(\Gamma_0(23), \chi_5)$. It has $a_5 = 2 + i$, which is an element of $K_g = \mathbb{Q}(i)$ of norm 5. Using this element we compute the corresponding splitting map β, defined just by $\beta(\sigma_B) = 2 + i$. Applying the operator $w = Id + (2 + i)^{-1}\eta_{\sigma_\beta}$ to both g and $\bar{g}$ we find the building block wA_g and the corresponding isomorphism defined over $M := \mathbb{Q}(\xi_5)$ with the elliptic curve E.

- The maximal order in the field $K = \mathbb{Q}(\sqrt{-5})$ satisfies the ramified Heegner hypothesis in this context (5 is ramified and 23 is split), and it has class number 2. The class field is equal to $\mathbb{Q}(\sqrt{-5}, i)$. The point $\tau = (-15 + \sqrt{-5})/(5 \cdot 23)$ is fixed by the matrix $\left(\begin{smallmatrix} 15 & -2 \\ 5\cdot 23 & -15 \end{smallmatrix}\right) \in \Gamma_0(5 \cdot 23)$ and it has the same characteristic polynomial as $\sqrt{-5}$. Then, computing the modular parametrization and projecting onto E we obtain the point

$$\left[2 - 20i, \frac{-1 - 80\sqrt{-5} - 85\sqrt{5}}{2}\right] \in E(H).$$

  Its trace to $E(K)$ yields the point

$$\left[\frac{-1637}{2^6}, \frac{-1}{2} - \frac{3 \cdot 5^2 \cdot 127\sqrt{-5}}{2^9}\right].$$

- We can also take the maximal order in $K = \mathbb{Q}(\sqrt{-30})$, whose class field is $H = \mathbb{Q}(\sqrt{2}, \sqrt{-3}, \sqrt{5})$. Taking the Heegner point $\tau = (50 + \sqrt{-30})/(5 \cdot 23)$ we obtain the point

$$[-13 + \frac{35\sqrt{2}}{2} + 5\sqrt{-3} - \frac{5\sqrt{-6}}{2}, \frac{-1}{2} - \frac{65\sqrt{5}}{2} + 25\sqrt{10} - 25\sqrt{-15} + 15\sqrt{-30}]$$

  on $E(H)$. The trace of this point to K is equal to

$$\left[\frac{-1073213}{2^3 \cdot 3 \cdot 23^2}, \frac{-1}{2} + \frac{5 \cdot 13 \cdot 97 \cdot 76507\sqrt{-30}}{2^5 \cdot 3^2 \cdot 23^3}\right].$$

Bibliography

[AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li. Twists of newforms and pseudo-eigenvalues of W-operators. *Invent. Math.*, 48(3):221–243, 1978.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[BD90] Massimo Bertolini and Henri Darmon. Kolyvagin's descent and Mordell-Weil groups over ring class fields. *J. Reine Angew. Math.*, 412:63–74, 1990.

[Che98] Imin Chen. The Jacobians of non-split Cartan modular curves. *Proc. London Math. Soc. (3)*, 77(1):1–38, 1998.

[Dar04] Henri Darmon. *Rational points on modular elliptic curves*, volume 101 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004.

[DD11] Tim Dokchitser and Vladimir Dokchitser. Euler factors determine local Weil representations. *arXiv:1112.4889*, 2011.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[dSE00] Bart de Smit and Bas Edixhoven. Sur un résultat d'Imin Chen. *Math. Res. Lett.*, 7(2-3):147–153, 2000.

[Edi96] Bas Edixhoven. On a result of Imin Chen. *arXiv:alg-geom/9604008*, 1996.

[GL01] Josep González and Joan-C. Lario. $\mathbf{Q}$-curves and their Manin ideals. *Amer. J. Math.*, 123(3):475–503, 2001.

[Gro84] Benedict H. Gross. Heegner points on $X_0(N)$. In *Modular forms (Durham, 1983)*, Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., pages 87–105. Horwood, Chichester, 1984.

[Gro91] Benedict H. Gross. Kolyvagin's work on modular elliptic curves. In *L-functions and arithmetic (Durham, 1989)*, volume 153 of *London Math. Soc. Lecture Note Ser.*, pages 235–256. Cambridge Univ. Press, Cambridge, 1991.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[JL70] H. Jacquet and R. P. Langlands. *Automorphic forms on* GL(2). Lecture Notes in Mathematics, Vol. 114. Springer-Verlag, Berlin-New York, 1970.

[Kid95] Masanari Kida. Galois descent and twists of an abelian variety. *Acta Arith.*, 73(1):51–57, 1995.

[Kol90] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[KP] Daniel Kohen and Ariel Pacetti. On Heegner points for primes of additive reduction ramifying in the base field. *Trans. Amer. Math. Soc.* To appear. With an appendix by Marc Masdeu.

[KP16] Daniel Kohen and Ariel Pacetti. Heegner points on Cartan non-split curves. *Canad. J. Math.*, 68(2):422–444, 2016.

[LMF13] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2013. [Online; accessed 16 September 2013].

[Pac13] Ariel Pacetti. On the change of root numbers under twisting and applications. *Proc. Amer. Math. Soc.*, 141(8):2615–2628, 2013.

[Raj98] C. S. Rajan. On strong multiplicity one for l-adic representations. *Internat. Math. Res. Notices*, (3):161–172, 1998.

[Rib77] Kenneth A. Ribet. Galois representations attached to eigenforms with Nebentypus. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 17–51. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[Roh93] David E. Rohrlich. Variation of the root number in families of elliptic curves. *Compositio Math.*, 87(2):119–151, 1993.

[Roh94] David E. Rohrlich. Elliptic curves and the Weil-Deligne group. In *Elliptic curves and related topics*, volume 4 of *CRM Proc. Lecture Notes*, pages 125–157. Amer. Math. Soc., Providence, RI, 1994.

[RW14] Marusia Rebolledo and Christian Wuthrich. A moduli interpretation for the non-split Cartan modular curve. *arXiv:1402.3498*, 2014.

[Ser67] J.-P. Serre. Complex multiplication. In *Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965)*,, pages 292–296. Thompson, Washington, D.C., 1967.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser97] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[TZ03] Ye Tian and Shou-wu Zhang. *Euler system of CM-points on Shimura curves*. preparation, 2003.

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

[YZZ13] Xinyi Yuan, Shou-Wu Zhang, and Wei Zhang. *The Gross-Zagier formula on Shimura curves*, volume 184 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2013.

[Zha01] Shou-Wu Zhang. Gross-Zagier formula for GL_2. *Asian J. Math.*, 5(2):183–290, 2001.

[Zha10] Shou-Wu Zhang. Arithmetic of Shimura curves. *Sci. China Math.*, 53(3):573–592, 2010.