INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

Vanishing and Non-Vanishing of L-Series of Elliptic Curves Twisted by Dirichlet Characters

Jack Fearnley

A Thesis

in

The Department

of

Mathematics and Statistics

Presented in Partial Fulfilment of the Requirements
for the degree of Doctor of Philosophy at
Concordia University
Montreal, Quebec, Canada

February 2001

ABSTRACT

Vanishing and Non-Vanishing of L-Series of Elliptic Curves Twisted by Dirichlet Characters

Jack Fearnley, Ph.D.
Concordia University, 2001

We study the behaviour of L-series of elliptic curves twisted by Dirichlet characters. In particular, we study the vanishing and non-vanishing of these L-series at the critical point. We present empirical results indicating the vanishing behaviour of cyclic twists of orders $3, 5, 7$ and conductors up to 5000 for elliptic curves of conductor less than 100. We prove results for vanishing in the case of cyclic cubic twists and non-vanishing in the case of cyclic twists of arbitrary prime order.

Let $L(E, s)$ be the L-series of an elliptic curve $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$.

If there exists a cyclic cubic character χ such that $L(E, 1, \chi) = 0$ or if $L(E, 1) = 0$ then the L-series vanishes for an infinite number of cyclic cubic characters.

With finite exceptions, if $L(E, 1) \neq 0$ there exist an infinite number of cyclic twists ψ of prime order k such that $L(E, 1, \psi) \neq 0$ for every order k.

ACKNOWLEDGEMENTS

My warmest thanks goes to all my teachers who, over the years, have fostered and developed my mathematical interests. I recall with pleasure the lectures of B. Neumann, P. J. Hilton, W. Ledermann and K. Mahler of my undergraduate days in Manchester.

I would particularly like to thank Ram Murty who awakened my interest in elliptic curves in 1988 and inspired me to pursue graduate studies. I am also grateful to Professors C. David and H. Darmon and to A. Akbary for valuable conversations and invaluable teaching.

But my special thanks must go to those who put up with me the longest. I acknowledge my deep gratitude to my supervisor, Hershy Kisilevsky, for his patience and generosity in answering my questions, filling the thirty year gaps in my mathematical knowledge and staying with me to the completion of this thesis. Most of all I must thank my wife, Françoise, who has encouraged me every step of the way and never begrudged the time it has taken.

I would like to thank J. F. Mestre and M. Kuwata for useful conversations about the geometric constructions in Chapter 4.

I would like to thank CICMA and FCAR and my supervisor for the financial support I have received.

Contents

List of Tables

Chapter 1

Introduction

1.1 Overview of this thesis

The purpose of this thesis is to study higher order twists of the L-functions associated with elliptic curves. It is conjectured that the value of the L-function at its critical point supplies important information about the elliptic curve and, in particular, the vanishing or non-vanishing of this value is related to the rank of the elliptic curve.

This chapter defines key aspects of this relationship and describes what is known and what is conjectured about these L-functions. Chapter 2 is of an empirical nature and describes computations estimating the fraction of L-functions which vanish for a range of cyclic twists of orders $3, 5$ and 7. The computational techniques are described, and summarized results are displayed.

The balance of the thesis is of a more theoretical nature. Chapter 3 surveys the various techniques which have been used to study twisted L-functions, mostly for quadratic twists. Chapter 4 proves results for the vanishing of cyclic cubic twists and chapter 5 proves non-vanishing results for cyclic twists of prime order.

The final brief chapter mentions some results for vanishing of twists of order 5 and 6. Appendices give more detailed results for vanishing twists and a listing of the computer programs used in the calculations.

1.2 Elliptic curves

An elliptic curve E over a field K is a genus one curve with at least one K-rational point. With an appropriate choice of coordinates which places the identified point at infinity, the curve E can be explicitly written down in *Weierstrass form*. The affine version of this form is

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with the coefficients $a_1, a_2, a_3, a_4, a_6 \in K$. For fields of characteristic other than 2 or 3, we can simplify this by rational transformations of the variables to the *short Weierstrass form*

$$y^2 = x^3 + Ax + B$$

The points of E satisfy an addition law which give the curve the structure of an abelian group. In 1922 Mordell [24] proved that the group $E(\mathbb{Q})$ of rational points is finitely generated and in 1930 Weil [42] extended this proof to any number field K. We have

$$E(K) \simeq \mathbb{Z}/t_1\mathbb{Z} \times \mathbb{Z}/t_2\mathbb{Z} \times \mathbb{Z}^r$$

where r is the rank of $E(K)$ and $\mathbb{Z}/t_1\mathbb{Z} \times \mathbb{Z}/t_2\mathbb{Z}$ is the subgroup of torsion points.

1.3 The Birch and Swinnerton-Dyer conjectures

Let E be an elliptic curve of conductor N defined over $\mathbb{Q}$. The Birch and Swinnerton-Dyer conjectures as originally stated relate the rank of the elliptic curve over $\mathbb{Q}$ to the order of vanishing of its L-function as follows:

Define N_p to be the number of points on E over the finite field $\mathbb{F}_p$ and let $a_p = p + 1 - N_p$ if $p \nmid N$ and $a_p = p - N_p$ if $p \mid N$. Then we define

$$\begin{aligned} L(E,s) \quad &: \quad = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \mid N} (1 - a_p p^{-s})^{-1} \\ &= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad \text{for } \Re(s) > 3/2 \end{aligned}$$

to be the L-function of the elliptic curve. By the theorems of Wiles [43] and Taylor-Wiles [39] and subsequent refinements, this L-function is the Mellin transform of a weight two cusp form

$$f(z) = \sum_{n=1}^{\infty} a_n \exp(2\pi i n z).$$

The L-functions of these modular forms satisfy a functional equation which permits their continuation to the whole complex plane and, in particular to the critical point $s = 1$.

Conjecture 1.3.1 (Birch and Swinnerton-Dyer I) *The order of vanishing, r, of $L(E, s)$ at the critical value $s = 1$ is equal to the rank of the Mordell-Weil group of the elliptic curve.*

In order to state the more precise version of the Birch and Swinnerton-Dyer conjecture we will need to define some invariants of E and a height function which measures the arithmetic complexity of points on E. The arithmetic complexity of a point P can be measured by a naive *height* function $h(P)$ such as the number of digits in the numerator of the x coordinate. A more useful measure of height is the Néron (or canonical) height given by

$$\hat{h}(P) = \lim_{n \to \infty} \frac{h(2^n P)}{4^n}$$

which gives $\hat{h}$ the structure of a quadratic form. We further define a *height pairing* of two points P, Q

$$\langle P, Q \rangle = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q).$$

Let the points $P_1, P_2, \ldots P_r$ be a basis for the free part of the Mordell-Weil group of E. Then we define the regulator of the curve to be

$$R = \det\left(\langle P_i, P_j \rangle\right).$$

Another invariant of E is the period

$$\Omega = \int_{e_3}^{\infty} \frac{dx}{\sqrt{x^3 + Ax + B}}$$

where e_3 is the greatest real root of $x^3 + Ax + B = 0$.

A further invariant of the curve is Ш, the Tate-Shafarevitch group, which measures the failure of the local-global principle for elliptic curves. It is conjecturally finite. The c_p are integers related to the primes of bad reduction and are called the Tamagawa numbers (See below). With these parameters in hand we can now state the precise version of the conjecture:

Conjecture 1.3.2 (Birch and Swinnerton-Dyer II)

$$\lim_{s\to 1} L(E,s)/(s-1)^r = \frac{\Omega\,|\,Ш|\,R}{|E(\mathbb{Q})_{tor}|^2}\prod_{p|N} c_p$$

These conjectures were first formulated in 1963 and there is, by now, extensive numerical evidence in favour of them but they have so far resisted complete proof. In 1977 Coates and Wiles [5] showed

Theorem 1.3.3 *Let E be an elliptic curve over a field K with complex multiplication. K may be the field of rational numbers or the field of complex multiplication. Then if $E(K)$ is infinite, we have $L_K(E,1) = 0$.*

R. Greenberg later gave a partial converse of this result: namely that if the L-function vanishes with odd multiplicity at $s = 1$, then either the rank is positive or Ш is infinite. The preceding theorems and further results particularly by Gross, Zagier and Rubin were extended and unified by work of Kolyvagin [17] in 1988 summarized in the following theorem:

Theorem 1.3.4 (Kolyvagin) *For an elliptic curve $E/\mathbb{Q}$, if $L(E,1) \neq 0$ then the rank of E is zero. If $L(E,1) = 0$ and $L'(E,1) \neq 0$ then the rank of E is one. Furthermore, in both these cases, Ш is finite.*

This theorem was further generalized by Kato to abelian extensions (see theorem 8.1 in [32])

Theorem 1.3.5 (Kato) *Suppose E is modular and E does not have complex multiplication.*

(i) *If $L(E,1) \neq 0$ then $E(\mathbb{Q})$ and Ш are finite*

(ii) *If K is a finite abelian extension of $\mathbb{Q}$, χ is a character of $Gal(K/\mathbb{Q})$, and $L(E,1,\chi) \neq 0$ then $E(K)^\chi$ and the corresponding part of Ш are finite.*

The case where E has complex multiplication was covered by Rubin [32]. Very little is known about the conjectures for ranks greater than or equal to two.

The Birch and Swinnerton-Dyer conjectures can be generalized to abelian varieties over number fields as follows (see [20] section III §5):

Let A be an abelian variety defined over a number field F. In order to generalize the above conjectures we must give appropriate meanings to the terms found in the L-function and to the terms in the expression on the right hand side of the second conjecture.

Let $\mathcal{O}_v$ be the local ring of integers in F at some discrete valuation where A has good reduction. Let $k(v)$ be the residue class field and G_v be a decomposition group. We construct the L-function as follows

- $\mathbf{N}v = |k(v)|$
- Frob_v = Frobenius element in G_v acting on $A(\overline{k(v)})$
- $\alpha_{i,v}$ =the eigenvalues of Frob_v
- $P_v(T) = \prod_{i=1}^{2d}(1 - \alpha_{i,v}T)$ for places of good reduction of A
- $P_v(T)$ for places of bad reduction of A (These are polynomials)
- $\mathcal{S} = \mathcal{S}_{\mathrm{bad}} \cup \mathcal{S}_\infty$ the set of all places of bad reduction of A and all archimedean places of A

Then the Euler product

$$L_{\mathcal{S}}(A,s) = \prod_{v \notin \mathcal{S}_\infty} \frac{1}{P_v(\mathbf{N}v^{-s})} = \prod_{v \in \mathcal{S}_{\mathrm{bad}}} \frac{1}{P_v(\mathbf{N}v^{-s})} \prod_{v \notin \mathcal{S}} \prod_{i=1}^{2d} (1 - \alpha_{i,v}\mathbf{N}v^{-s})^{-1}$$

converges for $\Re(s) > 3/2$.

Conjecture 1.3.6 (Generalized Birch and Swinnerton-Dyer I) *The function may be analytically continued to the whole complex plane and its order of vanishing, r, at the critical value $s = 1$ is equal to the rank of $A(F)$.*

In order to present the second conjecture in generalized form we must identify factors equivalent to the period, regulator and Tamagawa numbers in this more general framework.

- PERIOD: At each absolute value v the completion F_v is a locally compact field and so we can choose a Haar measure μ_v such that, for almost all v, $\mu_v(\mathcal{O}_v) = 1$. We can choose an invariant differential form ω of degree d on A/F and define the v-adic period

$$\pi_v = \int_{A(F_v)} |\omega|_v \, \mu_v^d$$

The measures μ_v define a measure $\mu = \prod \mu_v$ on A_F/F, the quotient of the adeles of F with F and we define the norm $\|\mu\| = \mu(A_F/F)$. The value

$$\frac{\prod_{v \in S} \pi_v}{\|\mu\|^d}$$

takes the place of the period in the original conjecture.

- REGULATOR: The regulator is defined to be

$$R_A = |\det \langle P_i, P_j \rangle|$$

where $\{P_1, \ldots, P_r\}$ is a basis for $A(F)$ modulo torsion and $\langle P_i, P_j \rangle$ is the height pairing

- TAMAGAWA NUMBERS: Let $\mathbf{A}$ be the Néron model of A_F over $\mathcal{O}_F$, with connected Néron model $\mathbf{A}^0$. For v finite we define

$$c_v = \left[\mathbf{A}_{k(v)}(k(v)) : \mathbf{A}^0_{k(v)}(k(v))\right]$$

The Tamagawa number, c_v is thus the index of the subgroup of points in the residue class field on the connected component of the special fibre in the full group of $k(v)$-rational points on the whole fibre of the Néron model.

We now have

$$\lim_{s \to 1} L(A, s)/(s-1)^r = \frac{\prod_{v \in S} \pi_v}{\|\mu\|^d} \frac{|Ш| \, R_A}{|A(F)_{\text{tor}}|^2} \prod_{v \in S_{\text{bad}}} c_v$$

1.4 Twists

The definition of the L-function may also include an additional variable representing a *twist*. This twist can be a Dirichlet character χ or, more generally, a character ρ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in some $GL_n(K)$. The generalized twisted version of the first conjecture can be found in Rohrlich [31]. The twisted L-function provides information about the analytic rank of the elliptic curve over a finite extension of the base field. Let K be a finite abelian extension of $\mathbb{Q}$, then

$$L(E/K, s) = L(E/\mathbb{Q}, s) \prod_{\chi} L(E/\mathbb{Q}, s, \chi)$$

where the product is taken over all non-principal primitive characters $\chi \in (\widehat{\mathbb{Z}/m\mathbb{Z}})^*$ for a given conductor m. More generally, let A be an abelian variety over $\mathbb{Q}$ and let ρ be a continuous finite-dimensional complex representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. There is an extension $H/\mathbb{Q}$ with an embedding in $\mathbb{C}$ where ρ is realized. Thus ρ can be viewed as a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on a finite dimensional space V over H. Rohrlich defines the twisted L-function as a product of local twisted L-functions

$$L(s, A, \rho) = \prod_{p} L_p(s, A, \rho).$$

For each prime p fix an ideal $\mathfrak{p}$ of H lying above p, and let $I(\mathfrak{p})$ and $\mathrm{Frob}(\mathfrak{p})$ be the inertia group and Frobenius at $\mathfrak{p}$ respectively. Now choose a different prime ℓ and $\lambda \in H$ above ℓ and consider the vector space

$$W = (H_\lambda \otimes_{\mathbb{Z}_\ell} T_\ell(A)) \otimes_{H_\lambda} (H_\lambda \otimes_H V)$$

where H_λ is the completion of H at λ. The Tate module $T_\ell(A)$ is the inverse limit of the ℓ^k division points on the variety A.

The local L-function is now given by

$$L_p(s, A, \rho) = \det(1 - p^{-s}\rho(\mathrm{Frob}(\mathfrak{p})) \mid W_{I(p)}).$$

Here the restriction $W_{I(p)}$ refers to the largest quotient of W on which $I(\mathfrak{p})$ acts trivially. The generalized conjecture states that

Conjecture 1.4.1 (Twisted Birch and Swinnerton-Dyer conjecture)

$$ord_{s=1} L(s, A, \rho) = \textit{multiplicity of } \rho \textit{ in } \mathbb{C} \otimes A(\overline{\mathbb{Q}}).$$

Specializing to one dimensional characters, let χ be a Dirichlet character of degree k and conductor m prime to N. Then the twisted L-function of an elliptic curve $E/\mathbb{Q}$ of conductor N is

$$\begin{aligned} L(E,s,\chi) &= \sum_{n=1}^{\infty} \frac{a_n \chi(n)}{n^s} \\ &= \prod_{p \nmid N} (1 - a_p \chi(p) p^{-s} + \chi^2(p) p^{1-2s})^{-1} \prod_{p \mid N} (1 - a_p \chi(p) p^{-s})^{-1}. \end{aligned}$$

As $L(E,s)$ corresponds to a weight two eigenform in $S_2(\Gamma_0(N))$ so $L(E,s,\chi)$ corresponds to a weight two form in $S_2(\Gamma_0(Nm^2),\chi^2)$ [35, Prop. 3.64]. For $(m,N)=1$, this twisted L-function can be holomorphically continued to the whole complex plane and satisfies a functional equation [35, Thm. 3.66].

$$\Lambda(E,s,\chi) = -\chi(N)\tau(\chi)^2 m^{-1} \Lambda(E, 2-s, \overline{\chi})$$

where

$$\Lambda(E,s,\chi) = \left(\frac{m\sqrt{N}}{2\pi}\right)^s \Gamma(s) L(E,s,\chi)$$

and $\tau(\chi)$ is the Gauss sum $\tau(\chi) = \sum_{c=0}^{m-1} \chi(c) \exp(2\pi i c/m)$.

Chapter 2

Empirical results for twisted L-series

2.1 Computational considerations

Let $L(E, s, \chi)$ as previously defined be the L-function for an elliptic curve $E/\mathbb{Q}$ of conductor N twisted by a Dirichlet character χ of conductor m prime to N. Let $f(z) = \sum a_n \exp(2\pi i n z)$ be the modular form of weight two and level N associated to the elliptic curve in question. We are interested in the vanishing or non-vanishing of $L(f, 1, \chi)$. There are three possible ways to compute this function

- We can compute directly from the definition

$$L(f, 1, \chi) = \sum_{n=1}^{\infty} \frac{a_n \chi(n)}{n}.$$

  While not absolutely convergent, this series is conditionally convergent [26] but extremely slowly. An experimental calculation to 200,000 terms yielded only single digit accuracy.

- We can use a series representation derived from the functional equation (here, $\tau(\chi)$ is the Gauss sum and $\varepsilon = \pm 1$ is the root number)

$$L(f, 1; \chi) = \sum_{n=1}^{\infty} \frac{a_n}{n} \exp\left(-\frac{2\pi n}{m\sqrt{N}}\right)\left(\chi(n) + \varepsilon\chi(N)\frac{\tau(\chi)^2}{m}\overline{\chi}(n)\right)$$

This series is rapidly convergent for small values of $m\sqrt{N}$ and has an easily computable bound on the truncation error after k terms, namely

$$\frac{4}{1-\rho}\rho^k \text{ where } \rho = \exp\left(-\frac{2\pi}{m\sqrt{N}}\right).$$

However, although we can unequivocally state that a given result is non-zero, we can never prove that very small value is a true zero.

- Finally, we can use the modular symbol expression more fully explained in a subsequent chapter

$$L(f,1,\chi) = \frac{\tau(\chi)}{m}\sum_{a \bmod m}\overline{\chi}(a)\left\{\infty, \frac{a}{m}\right\}.$$

2.1.1 Using the L-series

By expressing this twisted L-function as the Mellin transform of the associated modular form we can show that it satisfies a functional equation

$$\Lambda(E,s,\chi) = -\varepsilon\chi(N)\tau(\chi)^2 m^{-1}\Lambda(E,2-s,\overline{\chi})$$

where $\varepsilon = \pm 1$ is the root number (the eigenvalue of the Fricke involution) and

$$\Lambda(E,s,\chi) = \left(\frac{m\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(E,s,\chi),$$

where N is the conductor of E and $\tau(\chi)$ is the Gauss sum $\tau(\chi) = \sum_{c=0}^{m-1}\chi(c)\exp(2\pi ic/m)$. Using this property we can develop a series for $L(E,s,\chi)$ which is absolutely convergent for all values of s. Let $f(t,\chi) = \sum a_n\chi(n)\exp(2\pi int)$.

$$\begin{aligned}
\left(\frac{m\sqrt{N}}{2\pi}\right)^s \Gamma(s)L(E,s,\chi) &= \int_0^\infty t^s f(t,\chi)\frac{dt}{t} \\
&= \int_0^{1/m\sqrt{N}} + \int_{1/m\sqrt{N}}^\infty t^s f(t,\chi)\frac{dt}{t} \\
&= \int_\infty^{1/m\sqrt{N}} t^s f(t,\chi)\frac{dt}{t} \\
&\quad -\chi(N)\tau(\chi)^2 m^{-1}\int_\infty^{1/m\sqrt{N}} t^s f(t,\overline{\chi})\frac{dt}{t}.
\end{aligned}$$

Here we have used the Fricke involution property of the twisted modular form and the functional equation to bring both integrals to the same limits. Expanding f in its Fourier series and integrating term by term gives a complicated expression in incomplete gamma functions (see [26] for the analogous untwisted expression) which, at $s = 1$, simplifies to

$$L(E, \chi, 1) = \sum_{n=1}^{\infty} \frac{a_n}{n} \left(\chi(n) + \varepsilon C_\chi \overline{\chi(n)} \right) \exp\left(\frac{-2\pi n}{m\sqrt{N}} \right)$$

where $C_\chi = \chi(N)\tau(\chi)^2/m$. The remainder after k terms of this series is dominated by that of a geometric series in $\rho = \exp(-2\pi/m\sqrt{N})$. Note that $|a_n/n| < d(n)n^{-1/2} < 2$ where $d(n)$ is the number of divisors of n and the term in brackets has absolute value < 2. So the remainder after k terms is less than $\frac{4}{1-\rho}\rho^k$.

Going back to the complicated expression in incomplete gamma functions we can also derive a series for the derivative of the twisted L-function analogous to the untwisted version computed in [3]. While the general form is very complicated, the resulting series at $s = 1$ is

$$L'(E, \chi, 1) = \sum_{n=1}^{\infty} \frac{a_n}{n} \left(\chi(n) - \varepsilon C_\chi \overline{\chi(n)} \right) E_1\left(\frac{2\pi n}{m\sqrt{N}} \right),$$

where $E_1(x) = \int_x^\infty e^{-t}\frac{dt}{t}$ is the exponential integral. This has even better convergence than the series for $L(E, \chi, 1)$ since $E_1(x) \sim e^{-x}/x$.

2.1.2 Using modular symbols

Modular symbols were originally introduced by Birch and further developed by Manin. They have since been used for a number of purposes:

- Mazur, Tate and Teitelbaum [22] demonstrate the usefulness of modular symbols in computing twists of L-functions associated with weight k modular forms.
- Cremona [6] uses them to compute the homology of $X_0(N)$, a key step in producing his catalogue of elliptic curves.
- Cremona again uses modular symbols to determine the degree of the modular parametrization of elliptic curves [8], [7].

We will be interested in the first of these uses with weight two forms.

Let $f(z)$ be a weight two cusp form. The path integral $2\pi i \int_\alpha^\beta f(z)dz$ with $\alpha, \beta \in \mathcal{H}$ is called a *modular symbol*.

In [22] the weight two modular symbol is defined to be

$$\left\{\infty, \frac{a}{m}\right\} = 2\pi i \int_\infty^{-a/m} f(z)dz$$

(where we have suppressed a polynomial argument which has degree zero in the weight two case and simplified the notation).

The twisted L-function can be expressed as a finite linear combination of modular symbols using Birch's lemma.

Let χ be a Dirichlet character mod m. Using the Gauss sum $\tau(n,\chi) := \sum_{a \bmod m} \chi(a)\exp(2\pi i n a/m)$ and the fact that $\tau(n,\chi) = \overline{\chi}(n)\tau(1,\chi)$ and putting $\tau(\chi) := \tau(1,\chi)$ we may derive (with Birch)

$$L(f,1,\chi) = \frac{\tau(\chi)}{m} \sum_{a \bmod m} \bar{\chi}(a)\left\{\infty, \frac{a}{m}\right\}$$

Assuming we can compute the values of the modular symbols, this gives us a finite sum representation for the twisted L-function at the critical values.

The calculation of a modular symbol involves a reduction step to express it as a sum of *basic* symbols (called Manin symbols by Cremona [6]) and then a lookup into a suitable table of pre-computed basic symbols. Goldfeld [11] explains these two basic steps for weight two forms over $\Gamma_0(N)$ for square free N.

The reduction step

Given a path $\{\alpha, \beta\}$ between cusps in the upper half plane we can always associate a matrix σ such that $\beta = \sigma(\alpha)$. This matrix is not necessarily in $SL_2(\mathbb{Z})$. We need to break the path down to a number of paths satisfying this requirement. Since $\{\alpha,\beta\} = \{0,\beta\} - \{0,\alpha\}$ we may reduce to the case $\{0,\alpha\}$.

Let

$$\frac{p_{-2}}{q_{-2}}, \frac{p_{-1}}{q_{-1}}, \frac{p_0}{q_0}, \cdots, \frac{p_\tau}{q_\tau} = \alpha$$

be the successive convergents in the continued fraction expansion of α starting with

$$\frac{p_{-2}}{q_{-2}} = \frac{0}{1}, \frac{p_{-1}}{q_{-1}} = \frac{1}{0}, \frac{p_0}{q_0} = \frac{p_0}{1}, \cdots.$$

These convergents have the well known property that

$$p_r q_{r-1} - p_{r-1} q_r = (-1)^{r-1}$$

So we can write

$$\{0, \alpha\} = \sum_{r=1}^{\tau} \left\{ \frac{p_{r-1}}{q_{r-1}}, \frac{p_r}{q_r} \right\} = \sum_{r=1}^{\tau} \{\sigma_r(0), \sigma_r(i\infty)\}$$

where

$$\sigma_r = \begin{pmatrix} (-1)^{r-1} p_r & p_{r-1} \\ (-1)^{r-1} q_r & q_{r-1} \end{pmatrix} \in SL_2(\mathbb{Z})$$

The problem is reduced to evaluating a finite number of integrals of the form

$$2\pi i \int_0^{i\infty} f(\sigma(z)) d(\sigma(z))$$

for each $\sigma \in \Gamma_0(N) \backslash SL_2(\mathbb{Z})$.

Calculation of the basic symbols

The calculation of a basic symbol corresponding to each σ is similar to calculating the value of an L-series at its critical point. Goldfeld uses the functional equation of $f(z) = \sum a_n \exp(2\pi i n z)$ of *squarefree* level N to give a complicated but reasonably rapidly convergent expression for the modular symbol. Let $\lambda_p := -a_p$ for prime p and be fully multiplicative otherwise. Goldfeld computes intermediate values M, M_h, h, l from the elements of σ giving

$$-\sum_{n=1}^{\infty} \frac{a_n}{n} \lambda_M \exp\left[-\frac{2\pi n \sqrt{M_h}}{\sqrt{MN}} \right] \left\{ \exp\left[\frac{2\pi i n h}{M} \right] - \lambda_N \lambda_{M/M_h} \exp\left[-\frac{2\pi i n l M_h}{M} \right] \right\}$$

as the value of the basic symbol corresponding to σ.

We also have the useful fact proved by Shimura and mentioned by Goldfeld that for forms whose Fourier coefficients are rational

$$2\pi i \int_0^{i\infty} f(\sigma(z)) d(\sigma(z)) = c_1 \Omega_1 + c_2 \Omega_2$$

where $c_1, c_2 \in \mathbb{Q}$ with bounded denominators and the Ω are periods of the associated elliptic curve. When the modular symbols are used to compute the value of a twisted L-function, one of the periods always cancels out leaving the L-function proportional to the real period in the case of even characters or the imaginary period for odd characters.

Identification of zeros

In principle, calculations with modular symbols can be performed entirely in integers using the algebraic form of the L-series which is discussed more fully in Chapter 5. However, even with real arithmetic computations, we can bound non-zero results away from true zero to sufficient accuracy to rigorously identify vanishing.

Let E be an elliptic curve of conductor N and consider an L-series twisted by a character χ cyclic of order k and conductor m. We shall establish an upper bound on the Manin symbols using Goldfeld's construction and then compute a lower bound on the value of a non-zero L-function. Note that in Goldfeld's formula we maximize by setting $M = N, M_h = 1$ and noting that $|a_n| < n$ and $|\lambda_n| < 1$. We bound the size of the Manin symbols as follows:

$$\left|\sum_{n=1}^{\infty} \frac{a_n}{n} \lambda_M \exp\left[-\frac{2\pi n\sqrt{M_h}}{\sqrt{MN}}\right]\left\{\exp\left[\frac{2\pi i n h}{M}\right] - \lambda_N \lambda_{M/M_h} \exp\left[-\frac{2\pi i n l M_h}{M}\right]\right\}\right|$$

$$\begin{aligned}
&\leq \left|\sum_{n=1}^{\infty} \exp\left[-\frac{2\pi n}{N}\right]\left|\exp\left[\frac{2\pi i n h}{M}\right] + \exp\left[-\frac{2\pi i n l M_h}{M}\right]\right|\right| \\
&\leq 2\left|\sum_{n=1}^{\infty} \exp\left[-\frac{2\pi}{N}\right]^n\right| \\
&\leq 2\left(\frac{N}{2\pi} - \frac{1}{2} + O(1/N)\right) \\
&\leq N/\pi
\end{aligned}$$

Now as we shall see in Chapter 5 we can adjust the formula

$$L(E,1,\chi) = \frac{\tau(\chi)}{m} \sum_{a \bmod m} \overline{\chi}(a)\left\{\infty, \frac{a}{m}\right\}$$

to

$$2L(E,1,\chi) = \frac{\tau(\chi)\Omega}{m} \sum_{a \bmod m} \overline{\chi}(a)\Lambda(a,m)$$

where the $\Lambda(a,m)$ are integers and so the inner sum lies in $\mathbb{Z}[\zeta_k]$. These modular symbols are related to the Manin symbols by the continued fraction

algorithm described above and so each modular symbol may be computed in terms of not more than $\log m$ Manin symbols. We therefore have

$$\frac{2m}{\tau(\chi)\Omega}L(E,1,\chi)=\sum_{j=0}^{k-1}c_j\zeta_k^j$$

with each c_j being a sum of less than m symbols each of which is the sum of not more than $\log(m)$ Manin symbols and so $|c_j|\leq m(\log m)N/\pi$. Not all the coefficients are zero since we are assuming a non-zero L-function.

We shall first treat the twists of order 3. Since the values of cyclic cubic twists lie $\mathbb{Q}\left(\sqrt{-3}\right)$, the norm of $\sum_{j=0}^{2}c_j\zeta_3^j$ must be a non-zero rational integer and so we have

$$\left|\frac{2m}{\tau(\chi)\Omega}L(E,1,\chi)\right|\geq 1$$

giving

$$|L(E,1,\chi)|\geq\frac{\Omega}{2\sqrt{m}}.$$

Hence, even at the extreme range of our calcations with $m=100000$ we have $|L(E,1,\chi)|\geq 1.5\times 10^{-3}$. The 28 digit accuracy used in all calculations is therefore more than sufficient to unequivocally identify the zeroes.

For higher degree twists we shall consider the Galois conjugates of $\sum_{j=0}^{k-1}c_j\zeta_k^j$. First we observe that for the case of cyclic extensions of odd order these values group into complex conjugate pairs of equal absolute values. The product of all these conjugates is a positive rational integer and so ≥ 1. Hence

$$\left|\sum_{j=0}^{k-1}c_j\zeta_k^j\right|\geq(m(\log m)N/\pi)^{-\frac{k-3}{2})}$$

This gives a lower bound on the value of the twisted L-function of

$$|L(E,1,\chi)|>\frac{\Omega}{2\sqrt{m}}(m(\log m)N/\pi)^{-\frac{k-3}{2})}.$$

Substituting the maximum values for $N=100$, $m=5000,\Omega=1$ and $k=7$ used in the majority of calculations we find

$$|L(E,1,\chi)|>10^{-16}.$$

All calculations with modular symbols in the following tables have been carried out to 28 decimal places (and even summing over 5000 terms would not lose more than four more digits of accuracy) hence the zeroes may be determined unequivocally.

2.2 Computational results

The following tables were prepared using these definitions programmed in the Pari-GP system [2]. The tables are computed using the modular symbols method when the elliptic curve has square free conductor. In the cases where the elliptic curve does not have square free conductor, the L -series method was used with sufficient terms in the series to guarantee ten digit accuracy. In each case the tables cover the 92 elliptic curves of conductor less than 100 and cyclic twists of conductor up to 5000. Curves of rank 1 are indicated by a minus sign in front of the conductor of the curve.

2.2.1 Cyclic cubic twists

Table 2.1 shows the number of cubic twists of conductor less than 5000 for which vanishing occurs.

There are 795 conductors corresponding to unique cyclic cubic field extensions below 5000. Computed over 92 elliptic curves this gives a total of 73140 L-functions of which 3629 or 4.96% indicate vanishing.

Extended computations were performed for four elliptic curves (E11, E17, E37A and E37B) testing twists of conductors up to 30,000 as shown in table 2.2. In the case of E11 this was further extended to conductors up to 100,000 as seen in table 2.3. Here the zeroes are true zeroes since they are computed using modular symbols. In these tables the fraction of vanishing is between 2.5% and 0.4% with an average of 1% over the whole range.

For some vanishing cubic twists, the first derivative also vanishes thus indicating a rank of two or greater. These results are summarized in table 2.4. Of the 3629 vanishing L-functions, 113 or 3.11% had a vanishing first derivative.

2.2.2 Cyclic quintic twists

Table 2.5 shows the number of quintic twists of prime conductor less than 5000 for which vanishing occurs. A search for vanishing in the first derivative found no occurrences below conductor 5000.

There are 320 conductors corresponding to unique cyclic quintic field extensions below 5000. Computed over 92 elliptic curves this gives a total of 29440 L-functions of which 141 or .48% indicate vanishing. No search was made for vanishing derivatives.

2.2.3 Degree 7 twists

When we reach degree 7, vanishing twists are very rare. Table 2.6 shows the occurrence for elliptic curves of conductor below 100 and primes less than 5000. A blank entry means that no twist of conductor less than 5000 vanishes for this curve.

There are 165 conductors corresponding to unique cyclic degree seven field extensions below 5000. Computed over 92 elliptic curves this gives a total of 15180 L-functions of which 23 or .15% indicate vanishing. No search was made for vanishing derivatives.

2.3 Conclusions from the numerical computations

The computations described above represent a very small sample from the infinity of possibilities. What overall conclusions can be drawn?

- Unlike quadratic twists which are conjectured to vanish half of the time, vanishing of higher degree twists is quite rare.
- The probability of a vanishing twist seems to decrease quite rapidly with increasing order.
- Nevertheless there appears to be sufficient evidence to suggest that cubic twists might vanish infinitely often for each elliptic curve over $\mathbb{Q}$. For elliptic curves of conductor below 100 it was always possible to find a vanishing cubic twist of conductor less than 1000.
- There is insufficient evidence to suggest that higher order twists vanish infinitely often.

N	#	N	#	N	#	N	#
11A	26	42A	42	62A	37	-82A	49
14A	63	-43A	40	63A	17	-83A	27
15A	49	44A	37	64A	6	84A	31
17A	36	45A	31	-65A	34	84B	11
19A	56	46A	14	66A	71	85A	38
20A	77	48A	35	66B	31	-88A	50
21A	29	49A	3	66C	28	-89A	33
24A	58	50A	14	67A	11	89B	64
26A	62	50B	73	69A	23	90A	60
26B	36	51A	20	70A	36	90B	73
27A	40	52A	16	72A	19	90C	95
30A	65	-53A	26	73A	58	-91A	23
32A	6	54A	53	75A	4	-91B	67
33A	30	54B	113	75B	36	92A	42
34A	54	55A	71	75C	27	-92B	58
35A	50	56A	47	76A	10	94A	22
36A	16	56B	13	-77A	25	96A	66
-37A	37	-57A	40	77B	53	96B	18
37B	107	57B	52	77C	12	98A	8
38A	74	57C	17	78A	15	-99A	25
38B	66	-58A	45	-79A	36	99B	21
39A	49	58B	39	80A	46	99C	31
40A	56	-61A	45	80B	42	99D	12

Table 2.1: Number of vanishing cubic twists for distinct cyclic cubic fields of conductor below 5000

Range	# of twists	E11		E17		E37A		E37B	
0-5000	795	26	3.3%	36	4.5%	37	4.7%	107	13.5%
5000-10000	797	14	1.8%	25	3.1%	25	3.1%	54	6.8%
10000-15000	788	8	1.0%	17	2.2%	13	1.6%	53	6.7%
15000-20000	785	14	1.8%	8	1.0%	18	2.3%	38	4.8%
20000-25000	797	14	1.8%	13	1.6%	17	2.1%	39	4.9%
25000-30000	783	12	1.5%	10	1.3%	10	1.3%	44	5.6%
Total	4745	88	1.9%	109	2.3%	120	2.5%	335	7.1%

Table 2.2: Number of vanishing cubic twists of conductor below 30000.

Range	# of twists	E11	E11%
0-10000	1592	40	2.5%
10000-20000	1573	22	1.4%
20000-30000	1580	26	1.6%
30000-40000	1589	14	0.9%
40000-50000	1589	8	0.5%
50000-60000	1588	7	0.4%
60000-70000	1585	10	0.6%
70000-80000	1585	12	0.8%
80000-90000	1596	12	0.8%
90000-100000	1574	14	0.9%
Total	15851	165	1.0%

Table 2.3: Number of vanishing cubic twists for E11 of conductor below 100000

N	#	N	#	N	#	N	#
11A		42A	1	62A		-82A	1
14A		-43A	1	63A	2	-83A	1
15A	1	44A		64A	2	84A	
17A	1	45A	4	-65A		84B	
19A	1	46A		66A	5	85A	
20A	4	48A		66B		-88A	3
21A	1	49A		66C	1	-89A	
24A	1	50A	2	67A		89B	4
26A	1	50B	3	69A		90A	2
26B		51A		70A		90B	1
27A	2	52A		72A		90C	8
30A		-53A	2	73A	1	-91A	1
32A	2	54A	3	75A		-91B	6
33A		54B	5	75B	2	92A	
34A	2	55A		75C		-92B	
35A		56A		76A		94A	
36A	3	56B		-77A		96A	1
-37A		-57A	2	77B	4	96B	
37B	7	57B	1	77C	1	98A	1
38A	2	57C		78A	2	-99A	
38B		-58A	1	-79A	2	99B	
39A	2	58B		80A	1	99C	
40A	1	-61A	2	80B	1	99D	2

Table 2.4: Number of cases for which the cubic twist and its derivative both vanish for conductors below 5000

N	#	N	#	N	#	N	#
11A	1	42A	2	62A		-82A	3
14A	3	-43A	3	63A	1	-83A	
15A	4	44A		64A		84A	1
17A	3	45A		-65A	2	84B	
19A		46A		66A		85A	1
20A	2	48A	1	66B		-88A	7
21A	2	49A		66C	3	-89A	5
24A	2	50A	2	67A		89B	1
26A		50B	3	69A		90A	
26B	3	51A	2	70A		90B	3
27A		52A	1	72A		90C	1
30A		-53A	3	73A	1	-91A	
32A	1	54A	3	75A	1	-91B	3
33A	1	54B	4	75B		92A	1
34A	1	55A	1	75C	1	-92B	3
35A	1	56A	4	76A		94A	
36A		56B		-77A	1	96A	1
-37A	5	-57A	7	77B		96B	4
37B		57B		77C		98A	
38A	2	57C	1	78A		-99A	3
38B	4	-58A	6	-79A	4	99B	1
39A	1	58B	1	80A	1	99C	2
40A	2	-61A	4	80B		99D	

Table 2.5: Number of vanishing quintic twists for distinct cyclic fields of conductor below 5000

N	m	N	m	N	m	N	m
11A	2857	42A		62A	29	-82A	
14A		-43A		63A		-83A	
15A		44A		64A		84A	
17A		45A		-65A		84B	
19A		46A		66A		85A	
20A		48A		66B		-88A	
21A		49A		66C		-89A	
24A	491	50A		67A	3221	89B	
26A	4999	50B		69A		90A	71
26B		51A		70A		90B	3683
27A		52A		72A		90C	
30A		-53A		73A		-91A	
32A		54A		75A		-91B	
33A		54B		75B		92A	
34A		55A		75C		-92B	
35A		56A		76A		94A	
36A		56B		-77A		96A	29, 113
-37A	1421	-57A	2857	77B		96B	29, 113
37B	2003	57B	29	77C		98A	1471
38A		57C		78A		-99A	4999
38B	71	-58A	71	-79A	29	99B	3907
39A		58B		80A		99C	
40A		-61A	2339	80B		99D	4649

Table 2.6: Conductors of vanishing degree seven twists for distinct cyclic fields of conductor below 5000

Chapter 3

Analytic results for twisted L-series

Let E be an elliptic curve with coefficients in $\mathbb{Q}$ and let K be an abelian extension of $\mathbb{Q}$ and G =Gal$(K/\mathbb{Q})$. We have

$$L_K(E,s) = \prod_{\chi \in \widehat{G}} L(E,s,\chi)$$

where the product is taken over all primitive characters $\chi \in \widehat{G} \subseteq (\widehat{\mathbb{Z}/m\mathbb{Z}})^*$ for a given conductor m. In the case that $K/\mathbb{Q}$ is a cyclic cubic field there are only two non-trivial characters and they are complex conjugates so the above statement reduces to

$$L_K(E,s) = L(E,s)L(E,s,\chi)L(E,s,\overline{\chi})$$

Numerous authors have used analytic methods to establish asymptotic estimates of the number of vanishing or non-vanishing of twisted L-series of elliptic curves for various classes of characters. In the present chapter we shall gather together some of the known results.

3.1 Quadratic twists

The fact that Dirichlet characters of order two take values over the rational integers makes this case more accessible.

A quadratic twist of an elliptic curve over $\mathbb{Q}$ corresponds to another elliptic curve over $\mathbb{Q}$. Let $E/\mathbb{Q}$ be given in Weierstrass form by

$$E : y^2 = x^3 + Ax + B$$

and let χ be the quadratic Dirichlet character of conductor D, then the L-function of E twisted by χ is the same as the L-function of the elliptic curve

$$E_D : Dy^2 = x^3 + Ax + B$$

or equivalently, with a minor change of variable

$$E_D : y^2 = x^3 + D^2Ax + D^3B.$$

Goldfeld has made specific conjectures related to quadratic twists [10]:

Conjecture 3.1.1 (Goldfeld) *For each elliptic curve $E/\mathbb{Q}$ asymptotically half the quadratic twists E_D have rank zero and half have rank one.*

Weaker forms of this conjecture are:

Conjecture 3.1.2 (Algebraic Non-vanishing) *For each elliptic curve $E/\mathbb{Q}$ there are an infinity of quadratic twists D such that E_D has rank zero.*

Conjecture 3.1.3 (Algebraic Vanishing) *For each elliptic curve $E/\mathbb{Q}$ there are an infinity of quadratic twists D such that E_D has non-zero rank.*

Parallel to these algebraic conjectures about ranks of elliptic curves (and in line with the Birch and Swinnerton-Dyer conjectures) we have similar conjectures about the associated L-functions.

Conjecture 3.1.4 (Analytic Non-vanishing) *For each L-series there are an infinity of quadratic twists χ such that $L(E, 1, \chi) \neq 0$.*

Conjecture 3.1.5 (Analytic Vanishing) *For each L-series there are an infinity of quadratic twists χ such that $L(E, 1, \chi) = 0$.*

Goldfeld's conjecture is the strongest of the above conjectures but is a long way from any proof. Ono and Skinner [29] have shown that the non-vanishing conjecture is true with positive density of prime quadratic twists for each elliptic curve of conductor less than 100. The vanishing conjecture has been proven for certain families of elliptic curves Ono [28], Stewart & Top [39].

James [13] and Vatsal [41] have shown a positive density of vanishing for specific elliptic curves.

3.2 The Shimura correspondence and Waldspurger's theorem

A cornerstone of the theory of quadratic twists is the Shimura correspondence between modular forms of even weight 2λ and modular forms of half integral weight $\lambda + 1/2$. This enabled Waldspurger [42] to establish non-vanishing for an infinity of quadratic twists of elliptic curves over $\mathbb{Q}$.

The classical theta series

$$\Theta(\tau) = \sum q^{n^2}$$

satisfies transformation rules similar to a modular form of weight $k = 1/2$ if we restrict the transformations to $\Gamma_0(4)$. Within the congruence group $\Gamma_0(4)$, it is possible to construct modular forms of any half-integer weight and level N with transformation properties similar to the whole integer forms.

Specifically: let N be a positive integer divisible by 4 and define

$$\begin{aligned} \varepsilon_d &= 1 \text{ for } d \equiv 1 \bmod 4 \\ &= i \text{ for } d \equiv 3 \bmod 4. \end{aligned}$$

Let χ be a Dirichlet character mod N and define an extended Kronecker-Legendre symbol

$$\begin{aligned} \left(\frac{c}{d}\right) &= -\left(\frac{c}{|d|}\right) \text{ for } c, d < 0 \\ &= \left(\frac{c}{|d|}\right) \text{ otherwise.} \end{aligned}$$

Then a meromorphic function $f(z)$ on $\mathfrak{H}$ is called a modular form of half integer weight $\lambda + 1/2$ and character χ if

$$f\left(\frac{az+b}{cz+d}\right) = \chi(d)\left(\frac{c}{d}\right)^{2\lambda+1} \varepsilon_d^{-1-2\lambda}(cz+d)^{\lambda+1/2} f(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. The set of such forms which are holomorphic on the upper half plane is called $M_{\lambda+1/2}(N, \chi)$ and has the structure of a finite dimensional $\mathbb{C}$-vector space. Similarly we denote $S_{\lambda+1/2}(N, \chi) \subseteq M_{\lambda+1/2}(N, \chi)$ for those forms which vanish at the cusps. One can define Hecke operators

which preserve these spaces, however they are only defined for square indices. Specifically

$$f(z)|T_{p^2} = \sum_{n=0}^{\infty} \left(a(p^2 n) + \chi(p) \left(\frac{(-1)^\lambda n}{p} \right) p^{\lambda-1} a(n) + \chi(p^2) p^{2\lambda-1} a(n/p^2) \right) q^n$$

where we have temporarily replaced the usual a_n by $a(n)$ to accommodate the complicated arguments. As in the integer weight case $f(z)$ is called an eigenform if, for each prime p, there exists $\lambda_p \in \mathbb{C}$ such that

$$f(z)|T_{p^2} = \lambda_p f(z).$$

Shimura established a relationship between forms of weight $\lambda + 1/2$ and integer forms of weight 2λ as follows:

Let $\lambda \geq 1$ be an integer and χ a Dirichlet character modulo N with $4|N$. Let

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \in S_{\lambda+1/2}(\Gamma_0(N), \chi)$$

be an eigenform for T_{p^2} for all primes p with corresponding eigenvalue λ_p : $T_{p^2} f = \lambda_p f$. Define a function

$$g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$$

by the formal identity

$$\sum_{n=1}^{\infty} b_n n^{-s} = \prod_{p} \left(1 - \lambda_p p^{-s} + \chi(p)^2 p^{2\lambda-1-2s}\right)^{-1}.$$

Then $g \in M_{2\lambda}(N/2, \chi^2)$. If $\lambda \geq 2$ then g is a cusp form. This association between f and g is known as the Shimura correspondence [37].

With $\lambda = 1$ this expresses a relationship between the weight 2 forms corresponding to elliptic curves and certain modular forms of weight 3/2. Broadly speaking, the coefficients a_n in the 3/2 weight form f are proportional to the critical values of the L-functions of the elliptic curve associated to g, twisted by a quadratic character mod n. In particular, these twists can only vanish when $a_n = 0$. This is a particular case of Waldspurger's theorem. Conversely, given a weight two form, the existence of a corresponding weight 3/2 form was settled by Kohnen [16].

3.3 Applications of Waldspurger's theorem

Ono, James and Vatsal have used special cases of Waldspurger's theorem to prove that a positive density of prime quadratic twists do not vanish, for specific sets of elliptic curves.

Let

$$f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+1/2}(N, \chi).$$

Let t be a positive square free integer and define

$$\psi_t(n) = \chi(n)\left(\frac{-1}{n}\right)^{\lambda}\left(\frac{t}{n}\right).$$

Now define $A_t(n)$ by the formal product

$$\sum_{n=1}^{\infty}\frac{A_t(n)}{n^s} = L(f, s-\lambda+1, \psi_t)\sum_{n=1}^{\infty}\frac{a(tn^2)}{n^s}.$$

In particular

$$A_t(p) = a(tp^2) + \psi_t(p)p^{\lambda-1}a(t).$$

Shimura proved that the Mellin transform of this product (Call it $S_t(f(z)) = \sum_{n=1}^{\infty} A_t(n)q^n$) is a weight 2λ modular form in $M_{2\lambda}(N/2, \chi^2)$. If f is an eigenform for all the square Hecke operators then

$$a(t_1)S_{t_2}(f(z)) = a(t_2)S_{t_1}(f(z)).$$

Theorem 3.3.1 (Waldspurger) *Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_{\lambda+1/2}(N, \chi)$ be an eigenform for square Hecke operators and let $S_1(f(z)) = F(z) = \sum_{n=1}^{\infty} A(n)q^n \in S_{2\lambda}^{new}(M, \chi^2)$ for an appropriate positive integer M. ($N/2$ will probably be sufficient). Let n_1, n_2 be two positive square-free integers such that $\frac{n_1}{n_2} \in \mathbb{Q}_p^{\times 2}$ for all $p|N$. Then*

$$a^2(n_1)L\left(F, \lambda, \left(\frac{-1}{\cdot}\right)^{\lambda}\chi^{-1}\chi_{n_2}\right)\chi(n_2/n_1)n_2^{\lambda-1/2}$$

$$= a^2(n_2)L\left(F, \lambda, \left(\frac{-1}{\cdot}\right)^{\lambda}\chi^{-1}\chi_{n_1}\right)n_1^{\lambda-1/2}.$$

Where χ_{n_i} is the quadratic character for $\mathbb{Q}(\sqrt{n_i})/\mathbb{Q}$.

Theorem 3.3.2 *Specializing the above to $\lambda = 1$ we have*

$$\begin{aligned} & a^2(n_1)L\left(F,1,\left(\frac{-1}{\cdot}\right)\chi^{-1}\chi_{n_2}\right)\chi(n_2/n_1)\sqrt{n_2} \\ = \; & a^2(n_2)L\left(F,1,\left(\frac{-1}{\cdot}\right)\chi^{-1}\chi_{n_1}\right)\sqrt{n_1}. \end{aligned}$$

Or

$$L\left(F,1,\left(\frac{-n_2}{\cdot}\right)\chi^{-1}\right) = L\left(F,1,\left(\frac{-n_1}{\cdot}\right)\chi^{-1}\right)\left(\frac{a(n_2)}{a(n_1)}\right)^2\chi(n_1/n_2)\sqrt{\frac{n_1}{n_2}}.$$

Hence, if we know an n_1 for which the L-function does not vanish and such that $a(n_1) \neq 0$ then

$$L\left(F,1,\left(\frac{-n_2}{\cdot}\right)\chi^{-1}\right) = 0 \text{ if and only if } a(n_2) = 0.$$

So to prove infinite non-vanishing we only need to show an infinity of non-zero coefficients $a(n_2)$ satisfying $\frac{n_1}{n_2} \in \mathbb{Q}_p^{\times 2}$ for all $p|N$. If the twist χ has order k and conductor m then the character $\left(\frac{-n_2}{\cdot}\right)\chi^{-1}$ has order dividing $2k$ and conductor dividing $4mn_2$.

3.4 Averaging methods

The proof of Kolyvagin's theorem [17] requires the vanishing of certain derivatives of quadratic twists. Using the explicit formula method established by Riemann and adapted to modular forms by A. Weil, K. & R. Murty [25] have shown the existence of an infinity of such twists by establishing bounds on the average values of the derivatives of L-series twisted by quadratic characters. That is,

$$\sum_{\substack{0<-D\leq Y \\ D\equiv 1 \bmod 4N}} L'(E,1,\chi_D) = CY\log Y + o(Y\log Y)$$

where C is an effective constant depending only on E. They also compute a weaker average for the twisted L-series itself which is nevertheless sufficiently strong to prove the non-vanishing of an infinite number of twists.

$$\frac{1}{Y}\int_1^Y \sum_{\substack{|D|<t \\ D\equiv a \bmod 8N}} L(E,1,\chi_D)dt = CY\log Y + O\left(\frac{Y}{(\log Y)^\nu}\right)$$

with $0 < \nu < .0652\ldots$. They also show, under the generalized Riemann hypothesis, that not more than half of all twists can vanish. That is, they show that $L(f, 1, \chi) = 0$ can not happen for more than $\varphi(q)/2$ characters of conductor q.

While the present thesis concentrates on L-functions for twists of given order but varying conductor, asymptotic estimates have been made with twists of limited conductor where the order is allowed to increase. Rohrlich [30] has studied twisted L-functions where the characters are unramified outside a finite set of primes but the orders are allowed to increase arbitrarily. He shows that only finitely many of such twists vanish at the critical point. Stefanicki [38] establishes lower bounds on the non-vanishing of twisted L-functions for a fixed form and varying twists. Akbary [1] on the other hand generalizes results of Duke [9] concerning forms of weight two of given level for a fixed twist χ to forms of general weight k.

Let

$$L(f, s, \chi) = \sum_{n=1}^{\infty} \frac{a_n \chi(n)}{n^s}$$

then Stefanicki establishes for some $\alpha < 1$,

$$\sum_{\chi \bmod q} L(f, s, \chi) = q\psi(q) + O(d(q)q^{\alpha})$$

where the sum is over primitive characters and $q\psi(q)$ is the number of primitive characters mod q. He further shows that the number of non-vanishing twists is bounded below

$$\#\{\chi, L(f, \chi, 1) \neq 0\} \gg \frac{q\psi(q)^2}{2^{\nu(q)} \log q}$$

Akbary shows that for a form f_N of weight k and prime level $N > C_{k,q}$ and a fixed character χ of conductor q with $(N, q) = 1$

$$\#\{f_N, L(f_N, k/2, \chi) \neq 0\} \gg \frac{N}{(\log N)^2}.$$

($C_{k,q}$ is a constant depending only on k and q.)

3.5 $GL(n)$ methods

In [4], Bump, Friedberg and Hoffstein review the work which they and others have done on double Dirichlet series. Let

$$D(s,w) = \sum_n \frac{a_n(s)}{n^w}$$

where the $\{a_n(s)\}$ are themselves Dirichlet series or automorphic series on $GL(m)$. They are able to show analytic continuation in various special cases and deduce bounds on the average values of such functions. Let $a_n(s) = L(s, f, \chi_n)$ where f is an automorphic function on $GL(m)$ and χ_n is a sequence of quadratic twists. They conjecture meromorphic continuation of $D(s,w)$. This conjecture leads to infinite non-vanishing results for quadratic twists of general Langlands L-functions. In order to extend these results to higher order twists it is necessary to extend the ground field. Results can only be obtained for twists of order r when the ground field is extended to include r^{th} roots of unity (see [4] section 5).

X. She [35] has shown infinite non-vanishing in the specific case of cubic twists on $X_0(11)$ over $\mathbb{Q}(\sqrt{-3})$ using these techniques.

3.6 Spectral Theory

Over the last twenty years, based on results of Montgomery [23], Odlyzko [27] has studied the spacing of the zeroes of the Riemann zeta function and has observed that the spacings, properly scaled, follow the same distribution as the eigenvalues of large unitary matrices. Let the n^{th} zero of $\zeta(s)$ be at $\frac{1}{2} + \gamma_n i$ then it was known to Riemann that

$$\#\{j : 0 \leq \gamma_j \leq T\} \sim \frac{T \log T}{2\pi}, \text{ as } T \to \infty.$$

In order to study their statistical distribution, the spacing of these zeroes is normalized. Set

$$\hat{\gamma}_j = \frac{\gamma_j \log \gamma_j}{2\pi}$$

then the spacings $\delta_j = \hat{\gamma}_{j+1} - \hat{\gamma}_j$, have asymptotic mean one. Odlyzko plotted the distribution of these normal spacings for 70 million zeroes of $\zeta(s)$ in the region $10^{20} < j < 10^{20} + 7 * 10^7$ and found that they closely

fitted the Gaudin curve which is the curve describing the distribution of the suitably scaled eigenvalues of large random unitary matrices (the gaussian unitary ensemble). This work has been extended by Katz and Sarnak [15] to Dirichlet L-functions and L-series associated to quadratic twists of a variety of modular forms . It has been observed that in each case the scaled spacing distribution corresponds to the eigenvalue distribution of specific gaussian ensembles.

Let $\mathcal{F}_X$ be a suitable set of cusp forms of weight k and level $< X$ and let ε_f be the root number of $f \in \mathcal{F}_X$. The main consequences of this conjectural theory are that

$$\lim_{X\to\infty} \frac{\#\{f \in \mathcal{F}_X | \varepsilon_f = 1, L(k/2, f) \neq 0\}}{\#\{f \in \mathcal{F}_X | \varepsilon_f = 1\}} = 1$$

and

$$\lim_{X\to\infty} \frac{\#\{f \in \mathcal{F}_X | \varepsilon_f = -1, L'(k/2, f) \neq 0\}}{\#\{f \in \mathcal{F}_X | \varepsilon_f = -1\}} = 1$$

for a wide variety of sets $\mathcal{F}_X$. These include modular forms corresponding to quadratic twists of elliptic curves and quadratic twists of higher weight modular forms such as the weight 12 cusp form Δ. An important implication of this theory is that elliptic curves of rank > 1 would have zero density. This contrasts with some empirical studies by Kramartz and Zagier [18] which show a low but positive density of higher rank curves of about 3%. Of course, both results could be asymptotically consistent.

3.7 Kummer surfaces

M. Kuwata [19] has used a geometric approach to produce points on Kummer surfaces. The relevance of this geometric approach to the study of vanishing of cubic twists has been pointed out by Kisilevsky and is central to the results of the following chapter.

Chapter 4

Vanishing of Cyclic Twists

Our goal in this chapter is to investigate the behaviour of the L-functions of elliptic curves at their critical point, when twisted by Dirichlet characters of order three. Equivalently, subject to the Birch & Swinnerton-Dyer conjectures, we may examine the nature of points on the curve over cyclic cubic extensions.

Let

$$E : y^2 = x^3 + Ax + B$$

be the short Weierstrass form of an elliptic curve over $\mathbb{Q}$. Let $K/\mathbb{Q}$ be a cyclic cubic extension. In a cyclic cubic extension, for any non-rational element x the set $\{1, x, x^2\}$ forms a power basis with respect to which any other element may be expressed as a linear combination. Therefore, any K-rational point on E takes the form $P = (x, a + bx + cx^2)$ with $a, b, c \in \mathbb{Q}$. We will show below (Proposition 4.0.1) that, without loss of generality, we may assume $c = 0$. Since P is on the curve, x satisfies the polynomial equation

$$f(x) = x^3 + Ax + B - (a + bx)^2 = 0.$$

Furthermore, since x is in a cyclic cubic extension, f must have a square discriminant. Say

$$\begin{aligned} D(a, d, b; A, B) \quad : \quad & d^2 = -27a^4 - 4b^3a^3 + (54B - 30Ab^2)a^2 + \\ & (36Bb^3 + 24A^2b - 4Ab^5)a + \\ & A^2b^4 - 4A^3 - 27B^2 + 4Bb^6 - 18ABb^2. \end{aligned}$$

For fixed b, D may be considered as a curve in (a,d), say $C(a,d;b,A,B)$. C has genus one and, if a rational point could be found, C would be an elliptic curve over $\mathbb{Q}$.

Proposition 4.0.1 *Let $E/\mathbb{Q}$ be an elliptic curve and let $K/\mathbb{Q}$ be a cyclic cubic extension. If there exists a K-rational point R on E. then there exists a K-rational point P on E such that the coordinates of P may be expressed as $(x, a+bx)$, $x \in K$, $a,b \in \mathbb{Q}$.*

Proof. If the point R is a rational point in $\mathbb{Q}$, then R itself is trivially expressible in the form $(x, a+bx)$ required by the statement of the proposition and we are done. If R is not rational then, since K is a Galois extension, consider the conjugate points $R, R^\sigma, R^{\sigma^2}$. The sum $Q = R + R^\sigma + R^{\sigma^2}$ is a $\mathbb{Q}$-rational point on E since it is invariant under Galois action. If $Q \neq 0$ set $P = 3R - Q$. Then

$$\begin{aligned} P + P^\sigma + P^{\sigma^2} &= 3(R + R^\sigma + R^{\sigma^2}) - 3Q \\ &= 3Q - 3Q \\ &= 0. \end{aligned}$$

Otherwise, when Q is already zero, we simply set $P = R$. P is now a *trace zero* point. It remains to show that the coordinates of a trace zero point may be expressed as $(x, a+bx)$. We note that the property $P + P^\sigma + P^{\sigma^2} = 0$ means that P is collinear with its conjugates. The equation of this line must have rational coefficients since any Galois conjugate permutation of the three points determines the same line and this completes the proof. Alternatively and more explicitly, assuming the general form $P = (x, a + bx + cx^2)$ with $a, b, c \in \mathbb{Q}$ this collinearity implies

$$\begin{vmatrix} x & a + bx + cx^2 & 1 \\ x^\sigma & a + bx^\sigma + cx^{2\sigma} & 1 \\ x^{\sigma^2} & a + bx^{\sigma^2} + cx^{2\sigma^2} & 1 \end{vmatrix} = 0.$$

Subtracting a times the third column from the second column and then subtracting b times the first column from the second column and factoring out c gives

$$c^3 \begin{vmatrix} x & x^2 & 1 \\ x^\sigma & x^{2\sigma} & 1 \\ x^{\sigma^2} & x^{2\sigma^2} & 1 \end{vmatrix} = 0.$$

But this determinant is the discriminant of the cyclic cubic extension K and cannot be zero when x is not rational. Therefore $c = 0$ as was to be proven. Note that $P, P^{\sigma}, P^{\sigma^2}$ are again seen to be *rationally* collinear. ■

The Jacobian of $C(a, d; b, A, B)$

The elliptic curve, if it exists, is isomorphic to its jacobian which is straightforward to compute by a classic construction [6]. The quartic curve

$$y^2 = \alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + \varepsilon$$

has syzygies

$$I = 12\alpha\varepsilon - 3\beta\delta + \gamma^2$$

$$J = 72\alpha\gamma\varepsilon + 9\beta\gamma\delta - 27\alpha\delta^2 - 27\varepsilon\beta^2 - 2\gamma^3$$

which reduce the quartic curve to the isomorphic cubic curve

$$y^2 = x^3 - 27Ix - 27J.$$

From this form we can write down the j-invariant of the curve

$$j = \frac{2^8 3^3 I^3}{4I^3 - J^2}.$$

Performing these calculations for the curve $C(a, d; b, A, B)$ gives a j-invariant of

$$j = \frac{4}{(4A^3 + 27B^2)} \left[\frac{12(18b^4A^2 + 54Bb^2A + 243B^2 - 18b^6B + 27A^3 - b^8A)}{(27A^2 - 18b^4A - 108Bb^2 - b^8)} \right]^3.$$

This demonstrates that the family of jacobians parametrized by b are not all isomorphic to each other.

4.1 Finding points on $D(a, d, b; A, B)$

If, for a given value of b, the discriminantal curve C has rational points $(a_0, \pm d_0)$ then C is an elliptic curve and can be put in Weierstrass form by a rational map W sending $(a_0, -d_0)$ to infinity. This elliptic curve will be isomorphic to the jacobian described above. The point $P = W(a_0, d_0)$ will then be a rational point on the curve. It may be a torsion point but this

can only happen for a finite number of choices of b and so, without loss of generality, we can assume that P is not a point of finite order and that $(a_n, d_n) = W^{-1}(nP),\ n = 2, 3, \ldots$ are an infinite supply of further points on C.

We know of no general way to find a rational point on the discriminantal surface D in all cases. If however E has positive rank we can use rational points on E to find a point on D.

Let $P_1(x_1, y_1), P_2(x_2, y_2)$ be two rational points on E. Then the line $y = a + bx$ passing through P_1 and P_2 must intersect E at a third rational point say $(x_3, a + bx_3)$. Hence

$$\begin{aligned} f(x) &= x^3 + Ax + B - (a + bx)^2 \\ &= (x - x_1)(x - x_2)(x - x_3) \end{aligned}$$

with square discriminant. This provides values

$$\begin{aligned} a &= \frac{y_1 x_2 - x_1 y_2}{x_2 - x_1} \\ b &= \frac{y_2 - y_1}{x_2 - x_1} \\ d &= \pm(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \end{aligned}$$

such that the curve C in a, d has a point and is therefore an elliptic curve. While not itself generating a cyclic cubic extension ($f(x)$ is not irreducible), this point (a_0, d_0) can start the process described above to generate an infinite sequence of cyclic cubic extensions K_n for which E has K_n-rational points. Let $\mathcal{K}$ be the set of all such fields lying in all possible sequences.

We note that this method provides an infinite supply of b values each of which potentially gives rise to an infinite set of (a_i, d_i) values. The condition that the line $y = a + bx$ intersects the curve $E : y^2 = x^3 + Ax + B$ in three distinct points is that discriminant$((a + bx)^2 = x^3 + Ax + B\ ) < 0$. That is

$$\begin{aligned} 0 \ > \ & -27a^4 - 4b^3a^3 + (54B - 30Ab^2)a^2 \\ & +(36Bb^3 + 24A^2b - 4Ab^5)a + A^2b^4 - 4A^3 - 27B^2 + 4Bb^6 - 18ABb^2. \end{aligned}$$

For a given A, B this describes a non-empty open region $\mathcal{R}$ in a, b space. We will think of a, b space as parametrizing lines of slope b and y-intercept a. In particular, we will call lines with $a, b \in \mathbb{Q}$ *rational* lines.

The main theorem will follow if we can prove that the set of cubic fields generated in the above manner is infinite.

Theorem 4.1.1 *Let E be an elliptic curve of positive rank over $\mathbb{Q}$, then E increases its rank for an infinite number of cyclic cubic extensions.*

We will prove this theorem by showing that the condition that two of the fields generated by the above method are identical gives rise to a curve which is generally of genus three or greater and that any specializations of the parameters a, b which decrease the genus below three lie in a Zariski closed set. On the other hand we will show that the set of available rational values of $a, b \in \mathcal{R}$ is Zariski dense.

Since $\mathcal{R}$ is open, there exists $\varepsilon > 0$ such that a square box of side ε lies entirely within $\mathcal{R}$. We will need some lemmas.

Lemma 4.1.2 *Suppose E is an elliptic curve over $\mathbb{Q}$ with positive rank. The set of rational points on $E(\mathbb{Q})$ is dense on the connected component of the identity.*

Proof. Let P be a rational point of infinite order on the connected component of the identity of E. Suppose $P = (\wp(z), \wp'(z))$ for some $z \in \mathbb{C}/\Lambda_E$. In fact z is real since the connected component of the identity is mapped from the real axis. Integer multiples of z map to multiples of P on E and so z must be $\mathbb{Q}$-linearly independent of the real period of E (otherwise multiples of z would eventually repeat making P a torsion point). Now the set of all integer multiples of $z \bmod \Omega_1$ is dense on $(0, \Omega_1)$ and so, since $\wp$ is a continuous function, the set of multiples of P is correspondingly dense on E. ■

Lemma 4.1.3 *Given a line joining three distinct points of the connected component of the identity on $E(\mathbb{R})$ there exists a rational line arbitrarily close to it connecting points in $E(\mathbb{Q})$.*

Proof. Let $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$ be points on E. The line $y = a + bx$ joining these two points has

$$\begin{aligned} a &= \frac{x_2 y_1 - x_1 y_2}{x_2 - x_1} \\ b &= \frac{y_2 - y_1}{x_2 - x_1} \\ (a, b) &\in \mathcal{R}. \end{aligned}$$

We may choose an open box of side ε within this region. We wish to show that there is always a line $y = a' + b'x$ which joins points of $E(\mathbb{Q})$ such that

the point (a', b') lies within this open box. Since the set of rational points on the connected component is dense we can find points $(x_1', y_1'), (x_2', y_2') \in E(\mathbb{Q})$ arbitrarily close to $(x_1, y_1), (x_2, y_2)$. It is now a matter of elementary algebraic manipulation to show that $|a - a'|$ and $|b - b'|$ are suitably small. ■

Lemma 4.1.4 *Suppose E is an elliptic curve over $\mathbb{Q}$ with positive rank. The rational lines joining three distinct rational points of $E(\mathbb{Q})$ are Zariski dense in a, b space.*

Proof. Choose an arbitrary real point (p, q) in the open ε-box described above. Let $(w_1, z_1), (w_2, z_2) \in E(\mathbb{R})$ be points of intersection of E with the line $y = p + qx$. Using the same argument as the previous lemma we can find a rational line joining points of $E(\mathbb{Q})$ arbitrarily closely and thus a rational point (p', q') arbitrarily close to (p, q). Therefore, the rational points so constructed are dense in the ε-box in the usual topology and so are *a fortiori* Zariski dense. ■

Lemma 4.1.5 *The set of fields in $\mathcal{K}$ is infinite.*

Proof. Let $(x_1, a + bx_1)$ be a point on E in a cyclic cubic field $K \in \mathcal{K}$ derived from a rational point (a, d) on the elliptic curve $C(a, d; b, A, B)$. That is,

$$f_1 : x_1^3 + Ax_1 + B - (a + bx_1)^2 = 0$$

And let $(x_2, a' + bx_2)$ be another point in the field $K' \in \mathcal{K}$ derived from the rational point (a', d') so that

$$f_2 : x_2^3 + Ax_2 + B - (a' + bx_2)^2 = 0$$

Suppose that both $x_2 \in K'$ and $x_2 \in K$.

Since x_1, x_2 are both in K we can express x_2 in the power basis of x_1. Let

$$x_2 = p + qx_1 + rx_1^2 \text{ with } p, q, r \in \mathbb{Z}.$$

We may use the above three relations to establish a polynomial equation in a, a', b, r which may be viewed as a curve in the variables a', r for specific values of a and b. The simplest way to do this is to express the sums of powers of roots of f_1, f_2 in terms of a, a', A, B and then relate them using the

power basis. Let e_1, e_2, e_3 be the roots of f_1 and let e'_1, e'_2, e'_3 be the roots of f_2. We have

$$\begin{aligned} e'_1 + e'_2 + e'_3 &= b^2 \\ e'^2_1 + e'^2_2 + e'^2_3 &= b^4 + 4a'b - 2A \\ e'^3_1 + e'^3_2 + e'^3_3 &= b^6 + 6b^3a' - 3b^2A - 3B + 3a'^2 \end{aligned}$$

and similarly for the roots of f_1.We can then use the substitution

$$e'_i = p + qe_i + re_i^2$$

to generate three equations in the variables p, q, r, a, a', b and then by successive eliminations, arrive at a single polynomial relation involving a', r, a, b. These operations are best performed in Maple and the details can be found in Appendix C. Since smoothness is an open condition, outside a Zariski closed set of the base space, the curve obtained by a specialization of a, b is smooth. For special values of b the curve was found to have genus three. Since specialization can never increase the genus, the curve has genus at least three for general values of a and b. Conditions on a and b which cause the genus to drop occur at ramification points on the curve and are expressed as the vanishing of discriminants, that is, curves in a and b or isolated values of a or b. Now each field in $\mathcal{K}$ is generated from rational lines which we have seen are Zariski dense in a, b space. On the other hand, the conditions for fields to coincide places these lines on curves of high genus which, by Faltings' theorem can only have a finite number of rational points or on curves of lower genus which are Zariski closed. Consequently the set of distinct fields is infinite. ■

Proof of theorem 4.1.1 In the above lemmas we have constructed an infinite set of distinct fields K corresponding to points in a, b space such that $E(K)$ has K-rational points over and above the rational points of $E(\mathbb{Q})$. Suppose that these K-rational points are torsion points. Since the order of torsion points over all cubic fields is uniformly bounded by Kamienny's theorem [14], there is a multiple M such that $MP = 0$ for all cyclic cubic torsion points P on the curve E. This means that the x-coordinates of all these torsion points satisfy a polynomial equation and therefore the points in a, b space giving rise to them lie in a Zariski closed (indeed finite) set. Hence there remains an infinite set of distinct fields $K \in \mathcal{K}$ such that $E(K)$ has non-rational points of infinite order. ■

We may express the theorem in terms of L-series.

Proposition 4.1.6 *Let E be an elliptic curve such that $E(\mathbb{Q})$ has positive rank. Let χ be a cyclic cubic character and let*

$$L(E,s,\chi)=\sum_{n=1}^{\infty}\frac{a(n)\chi(n)}{n^s}.$$

Then $L(E,1,\chi)=0$ for an infinite number of characters χ.

Proof. Since $E(\mathbb{Q})$ has positive rank there are an infinite number of cyclic cubic fields K where the rank of E increases. Let the Dirichlet character χ_K correspond to each of these fields. By Kato's theorem (**1.3.5**) and its extensions, elliptic curves whose ranks over an abelian extension exceed their $\mathbb{Q}$-ranks have vanishing twisted L-functions. Hence, $L(E,1,\chi_K)=0$ for these characters. ■

4.2 Curves of zero rank

The theorems of the previous section depend upon the Zariski density of rational points in a,b space and were proved assuming non-zero rank of the elliptic curve over $\mathbb{Q}$. We shall now study elliptic curves of zero rank for which we nevertheless have found a rational point on the $D(a,d,b;A,B)$ surface. (Examples would be curves of square discriminant Δ where we can find points $(a=0,d=\pm\sqrt{\Delta},b=0)$.) Such a point can provide the "seed" for a set of fields $\mathcal{K}$ such that $E(K)$ for $K\in\mathcal{K}$ has positive rank.

Let P be a non-rational point of infinite order on the connected component of $E(K)$. Without loss of generality we can assume this to be a trace zero point. If P^σ is a Galois conjugate then we have shown in proposition 4.0.1 that the line PP^σ is rational.

Lemma 4.2.1 *Given a line joining pairs of points on the connected component of $E(\mathbb{R})$ as described above, there exists a rational line arbitrarily close to it joining a cyclic cubic point P to its Galois conjugate point P^σ.*

Proof. Let z,z' be the inverse images of P,P^σ under the analytic parameterization in $\mathbb{C}/\Lambda_E$. Since K is a real field, z,z' both lie in the real interval $(0,\Omega_1)$. The values Ω_1,z,z' are $\mathbb{Q}$-linearly independent because the points P,P^σ generate a rank 2 $\mathbb{Z}$-module (if rank 0 z,z' would translate to torsion points and if rank 1 they would translate to rational points). Consider the

points mz, mz' for $m = 1, 2, 3 \ldots$. they are individually dense in $(0, \Omega_1)$ and, by Kronecker's theorem (see for example, [12]) given any pair of points x, y in the interval $(0, \Omega_1)$ there is an m such that $|x - mz|$ and $|y - mz'|$ are simultaneously arbitrarily small. Consequently, any pair of points on E can be approximated by a conjugate pair of cyclic cubic points and therefore any line between points on $E(\mathbb{R})$ can be approximated arbitrarily closely by a rational line between such points. ■

We now have all we need to prove

Theorem 4.2.2 *Any elliptic curve $E/\mathbb{Q}$ with a point of infinite order in some cyclic cubic field increases its rank for an infinite number of cyclic cubic extensions.*

Proof. Suppose E has a point of infinite order over a cyclic cubic extension K. This point corresponds to a pair of rational points $(a, \pm d, b)$ on the discriminatal surface $D(a, d, b; A, B)$. Now that we have a density statement for (a, b) space and the means to construct at least one cyclic cubic extension with points of infinite order, the proof carries through in the same manner as the corresponding theorem for curves with positive rank over $\mathbb{Q}$. If the rational point on $D(a, d, b; A, B)$ is a torsion point it must lie in a Zariski closed set in (a, b) space because the order of rational torsion points are uniformly bounded by Mazur's theorem [21]. ■

As in the previous section we can state this theorem in terms of L-series, and combining both results we have proved

Theorem 4.2.3 *Any elliptic curve $E/\mathbb{Q}$ with a point of infinite order in some cyclic cubic field has vanishing L-function for an infinite number of distinct cyclic cubic twists.*

4.3 Detailed example for $E40$

A specific example will illustrate the methods described above.

The curve

$$E40 : y^2 = x^3 - 7x - 6$$

has no rational points and square discriminant 400. Assume we have a point $(x, a + bx)$ on $E40$. Then

$$f(x) = x^3 - 7x - 6 - (a + bx)^2 = 0$$

and the discriminantal curve takes the form

$$\begin{aligned} d^2 &= 400 - 216b^3a - 324a^2 - 756b^2 - 4b^3a^3 + 28b^5a - 27a^4 \\ &\quad +210a^2b^2 + 49b^4 - 24b^6 + 1176ab \end{aligned}$$

which is immediately seen to have rational points $(a = 0, d = \pm 20, b = 0)$ and so is equivalent to an elliptic curve in (a, d). This curve can be expressed in short Weierstrass form by sending the point $(0, 20, 0)$ to infinity. The minimal form is

$$\begin{aligned} y^2 &= x^3 + 513x - 185166 \\ &= (x - 54)\left(x^2 + 54x + 3429\right) \end{aligned}$$

which has conductor 2520. We note that the other point $(0, -20, 0)$ translates to $(54, 0)$ a torsion point of order two on the reduced curve. Using Cremona's MWrank program we see that this curve has rank 1 with generator

$$P_1 = (103, 980).$$

This point can then be used to produce an infinite set of rational values $(a_i, d_i, 0)$ on the discriminantal curve.

$$\begin{aligned} P_1 &\longrightarrow (-1, -7, 0) \\ 2P_1 &\longrightarrow (40/61, -59500/3721, 0) \\ 3P_1 &\longrightarrow (303/547, \ldots\ldots, 0) \\ 4P_1 &\longrightarrow (-2074000/2002663, \ldots\ldots, 0) \\ &\quad \text{etc.} \end{aligned}$$

These points lead to cyclic cubic extensions with characteristic polynomials

$$\begin{aligned} &x^3 - 7x - 7 \\ &x^3 - 26047x - 1459486 \\ &x^3 - 2094463x - 1032223461 \\ &x^3 - 28074613640983x - 56806398240381089482 \\ &\text{etc.} \end{aligned}$$

Or in reduced form

$$x^3 - x^2 - 2x + 1$$

$$x^3 - x^2 - 142x + 680$$
$$x^3 - x^2 - 182x + 81$$
$$x^3 - x^2 - 4672880x - 3862395200$$
etc.

We will now proceed to construct the high genus curve for the particular case $E40$. Let (x_1, a_1) be a point on $E40$ in a cyclic cubic field K_1. Suppose (x_2, a_2) is another point derived from (a_2, d_2) but that $x_2 \in K_1$ also. That is

$$g(x) = x_2^3 - 7x_2 - 6 - a_2^2 = 0.$$

Since x_1, x_2 are both in K_1 we can express x_2 in the power basis of x_1. Let

$$x_2 = p + qx_1 + rx_1^2.$$

We will use the above relations to establish a polynomial in a_1, a_2, r which will be shown to represent a curve of genus 3 when specialized to a curve in a_1, a_2. First we will establish some symmetric functions on the roots. We will drop subscripts since both f and g have the same structure. Let x, x', x'' be the three roots of f or g.

$$\begin{aligned}
x + x' + x'' &= 0 \\
x^2 + x'^2 + x''^2 &= (x + x' + x'')^2 - 2(xx' + x'x'' + x''x) \\
&= 14 \\
x^3 + x'^3 + x''^3 &= 7(x + x' + x'') + 3(6 + a^2) \\
&= 18 + 3a^2 \\
x^4 + x'^4 + x''^4 &= 7(x^2 + x'^2 + x''^2) + (6 + a^2)(x + x' + x'') \\
&= 98 \\
x^5 + x'^5 + x''^5 &= 7(x^3 + x'^3 + x''^3) + (6 + a^2)(x^2 + x'^2 + x''^2) \\
&= 7(18 + 3a^2) + 14(6 + a^2) \\
&= 210 + 35a^2
\end{aligned}$$

Hence, for the trace of g

$$\begin{aligned}
0 &= x_2 + x_2' + x_2'' = p + qx_1 + rx_1^2 + p + qx_1' + rx_1'^2 + p + qx_1'' + rx_1''^2 \\
&= 3p + 14r
\end{aligned}$$

then for the sum of squares

$$\begin{aligned} 14 &= x_2^2 + x_2'^2 + x_2''^2 = \sum_{conj} (p + qx_1 + rx_1^2)^2 \\ &= 3p^2 + 14q^2 + 98r^2 + 28pr + 6qr(6 + a_1^2). \end{aligned}$$

Developing the sum of cubes in a similar fashion we obtain

$$\begin{aligned} 18 + 3a_2^2 &= x_2^3 + x_2'^3 + x_2''^3 \\ &= 3pqr(6 + a_1^2) + p^3 + q^3(6 + a_1^2) - r^3(6 + a_1^2)^2 \\ &\quad +14((pq^2 + p^2q) + 98pr^2 + 98q^2r + 35qr^2(6 + a_1^2) \\ &= (6 + a_1^2)(3pqr + q^3 - r^3 + 35qr^2) + p^3 + 98pr^2 98q^2r. \end{aligned}$$

Using the first equation to eliminate p from the second equation we get

$$\begin{aligned} 42 &= 196r^2 + 42q^2 + 294r^2 - 392r^2 + 18qr(6 + a_1^2) \\ 21 &= 21q^2 + 49r^2 + 9qr(6 + a_1^2). \end{aligned}$$

Similarly we can eliminate p from the third equation to give the cubic expression

$$162 + 27a_2^2 = 27(6 + a_1^2)(q^3 + 49qr^2 - r^3(6 + a_1^2)) + 98r(9q^2 - 70r^2).$$

It is not practical to eliminate q across these last two equations by hand so we let Maple take the resultant of the two polynomials with respect to q. This give a single polynomial $h(a_1, a_2, r) = 0$ of degree 4 in a_2 and degree 6 in r. For generic values of a_1, h is a curve of genus three in the variables a_2, r. Using the algebraic curves package of Maple we find

$$\text{genus } h(a_2, r; a_1) \geq 3.$$

It is possible that for a number of values of a_1 the genus could fall below three. These combinations of values would correspond to ramification points of h and are identified by the vanishing of the discriminant. The appendix shows that this discriminant factors into five components, four of which are polynomials in a_1 or a_2 and one of which is a curve of genus three in (a_1, a_2). There are therefore only a finite set of combinations which could potentially reduce the genus. Since we have an infinite supply of a values given by points on the discriminantal curve, the rejection of a finite number of them

still leaves us with an infinite number of cyclic cubic extensions of the given elliptic curve which have infinite Mordell-Weil groups.

As we have seen, $b = 0$ is a good choice giving rise to an infinite family of cyclic cubic fields. If it had been a bad choice we could proceed as follows to generate a new value of b giving rational points on the discriminantal surface.

Set $a = -1, b = 0$ giving

$$\begin{aligned} f(x) &= x^3 - 7x - 6 - (-1 + 0x)^2 = 0 \\ &= x^3 - 7x - 7 = 0. \end{aligned}$$

The roots of this equation are

$$-1.692021472, -1.356895868, 3.048917340$$

corresponding to points

$$\begin{aligned} P &= (-1.692021472, -1) \\ P^\sigma &= (-1.356895868, -1) \\ P^{\sigma^2} &= (3.048917340, -1) \end{aligned}$$

and we can double two of these points on $E40$ giving

$$\begin{aligned} 2P &= (4.015122237, -5.533783453) \\ 2P^\sigma &= (3.258805396, 2.407543327). \end{aligned}$$

The line joining these two points is

$$y = 36.62500004 - 10.49999993x$$

which is a close approximation to the rational line

$$y = 293/8 - (21/2)x$$

substituting $a = 293/8, b = -21/2$ into the discriminantal surface gives the rational value $d = 7.13.29.181.2^{-6}$ and provides a new starting point for the generation of cyclic cubic extensions.

Chapter 5

Non-vanishing of Cyclic Twists

The constructions of the previous chapter have been largely geometric and have constructed twists for which the L-series *vanish*. In order to study *non-vanishing* of the L-function we will take a more algebraic approach. If we can show that the algebraic part of the twisted L-function is non-zero modulo some prime then it must be non-zero on $\mathbb{C}$. In order to define what we mean by the algebraic part of an L-function we introduce modular symbols following Mazur, Tate and Teitelbaum [22]. However, since we will only be considering weight two modular forms we will simplify the notation somewhat.

5.1 Modular Symbols

Let f be a weight two eigenform of level N. We define a modular symbol $\{\alpha, \beta\} \in S_2(N)^*$ as a functional

$$\{\alpha, \beta\} f = \frac{1}{2\pi i} \int_\alpha^\beta f(z) dz.$$

The properties of the modular symbol which are important for our purposes will now be summarized in a series of propositions. We shall assume that the Dirichlet character χ is of order k and has conductor m.

Proposition 5.1.1 (L-function relation) *The L-series of a modular cusp form at its critical point can be expressed as a modular symbol*

$$L(f, 1) = \{\infty, 0\}.$$

Proposition 5.1.2 (Birch's Theorem) *The value of an L-series twisted by a Dirichlet character can be expressed as a weighted sum of modular symbols*

$$L(f,1,\chi) = \frac{\tau(\chi)}{m} \sum_{a \bmod m} \bar{\chi}(a) \left\{\infty, \frac{a}{m}\right\}$$

where $\tau(\chi)$ is the Gauss sum.

Proposition 5.1.3 (Hecke action) *For an eigenform f the Hecke operator T_p with eigenvalue a_p acts on the modular symbol as follows*

$$a_p \left\{\infty, \frac{a}{m}\right\} = \left\{\infty, \frac{a}{m}\right\}^{T_p} = \sum_{u=0}^{p-1} \left\{\infty, \frac{a-um}{pm}\right\} + \varepsilon(p) \left\{\infty, \frac{ap}{m}\right\}$$

where $\varepsilon(p) = 0$ if $p|N$ else 1.

Proposition 5.1.4 (Integrality) *There are non-zero complex numbers $\Omega^{\pm}$ depending only upon f such that*

$$\Lambda^{\pm}(a,m) := \left(\left\{\infty, \frac{a}{m}\right\} \pm \left\{\infty, \frac{-a}{m}\right\} \right) / \Omega^{\pm} \text{ are integers.}$$

When f is the modular form associated to an elliptic curve the value $\Omega^{\pm}$ are rational multiples of the periods of the elliptic curve.

When dealing with even characters (i.e. characters χ such that $\chi(-1) = 1$) it is appropriate to take the positive sign. In what follows we shall use Λ to mean either Λ^+ or Λ^- depending on the parity of the character we are dealing with; and similarly for Ω.

This new symbol inherits by linearity all the above properties of the modular symbol. Using this symbol we can make precise the idea of the algebraic part of an L-function. Since

$$L(f,1,\chi) = \frac{\tau(\chi)}{m} \sum_{a \bmod m} \bar{\chi}(a) \left\{\infty, \frac{a}{m}\right\}.$$

We find easily

$$2L(f,1,\chi) = \frac{\tau(\chi)\Omega}{m} \sum_{a \bmod m} \bar{\chi}(a) \Lambda(a,m)$$

and so we define

$$L^*(f,1,\chi) := \frac{2mL(f,1,\chi)}{\Omega\tau(\chi)} = \sum_{a \bmod m} \bar{\chi}(a)\Lambda(a,m) \in \mathbb{Q}(\zeta_k)$$

to be the algebraic part of the twisted L-function.

5.2 Congruence relations

Let k be an odd prime. We wish to examine the residues modulo k of L-functions twisted by different Dirichlet characters of order k. We first observe that by Fermat's little theorem or otherwise,

$$\begin{aligned} 1 &= \chi(a)^k \equiv \chi(a) \bmod \mathfrak{k} \text{ when } (a,m) = 1 \\ 0 &= \chi(a) \text{ when } (a,m) \neq 1. \end{aligned}$$

Where $\mathfrak{k}$ is the unique prime above k in the cyclotomic field of k^{th} roots of unity.

So

$$\sum_{a \bmod m} \bar{\chi}(a)\Lambda(a,m) \equiv \sum_{\substack{a \bmod m \\ (a,m)=1}} \Lambda(a,m) \bmod \mathfrak{k}.$$

Suppose we further twist the L-series by a Dirichlet character ψ of prime conductor p coprime to m. Any primitive character of order k is the product of characters of order k of distinct prime conductors and, possibly, the character of conductor k^2. The subsequent analysis will be simplified by considering sums of modular symbols in a formal manner.

5.2.1 Sums of modular symbols

Let

$$S_m(t) := \sum_{\substack{a \bmod t \\ (a,m)=1}} \Lambda(a,t).$$

For a character of order k and conductor m we have

$$L^*(f,1,\chi) \equiv S_m(m) \bmod k.$$

We wish to study the effect on L^* of a further twist of the same order and prime conductor p and also the particular case of conductor p^2 when $p = k$.

That is, relations amongst $S_m(m)$, $S_{mp}(mp)$, and $S_{mp^2}(mp^2)$. We may do this using the Hecke action. We assume that f is an eigenform for all the Hecke operators and that $(m,p)=1$.

$$\begin{aligned} S_m(m)|\,T_p &= a_p S_m(m) = \sum_{\substack{a \bmod m \\ (a,m)=1}} \left[\sum_{u=0}^{p-1} \Lambda(a-um, pm) + \varepsilon(p)\Lambda(ap,m) \right] \\ &= \sum_{\substack{a \bmod m \\ (a,m)=1}} \sum_{u=0}^{p-1} \Lambda(a-um,pm) + \varepsilon(p) \sum_{\substack{a \bmod m \\ (a,m)=1}} \Lambda(ap,m) \\ &= S_m(pm) + \varepsilon(p) S_m(m). \end{aligned}$$

Now

$$\begin{aligned} S_m(pm) &= \sum_{\substack{a \bmod pm \\ (a,m)=1}} \Lambda(a,pm) \\ &= \sum_{\substack{a \bmod pm \\ (a,pm)=1}} \Lambda(a,pm) + \sum_{\substack{a \bmod pm \\ (a,pm)=p}} \Lambda(a,pm) \\ &= S_{pm}(pm) + \sum_{\substack{b \bmod m \\ (b,m)=1}} \Lambda(bp,pm) \\ &= S_{pm}(pm) + S_m(m). \end{aligned}$$

So

$$\begin{aligned} a_p S_m(m) &= S_{pm}(pm) + S_m(m) + \varepsilon(p) S_m(m) \\ S_{pm}(pm) &= (a_p - 1 - \varepsilon(p)) S_m(m). \end{aligned}$$

The derivation of a formula for $S_{mp^2}(mp^2)$ requires a second application of T_p.

$$\begin{aligned} (S_m(m)|\,T_p)|\,T_p &= a_p^2 S_m(m) = \sum_{\substack{a \bmod m \\ (a,m)=1}} \left[\sum_{u=0}^{p-1} \Lambda(a-um,pm)^{T_p} + \varepsilon(p)\Lambda(ap,m)^{T_p} \right] \\ &= \sum_{\substack{a \bmod m \\ (a,m)=1}} \sum_{v=0}^{p-1} \sum_{u=0}^{p-1} \Lambda(a-um-vmp, p^2 m) \end{aligned}$$

$$
\begin{aligned}
&+\varepsilon(p)\sum_{\substack{a \bmod m\\(a,m)=1}}\sum_{v=0}^{p-1}((a-um)p,pm)\\
&+\varepsilon(p)\sum_{\substack{a \bmod m\\(a,m)=1}}\sum_{v=0}^{p-1}\Lambda(ap-vm,pm)+\varepsilon^2(p)\sum_{\substack{a \bmod m\\(a,m)=1}}\Lambda(ap^2,m)\\
=\;& S_m(mp^2)+\varepsilon(p)pS_m(m)+\varepsilon(p)S_m(pm)+\varepsilon(p)S_m(m).
\end{aligned}
$$

Now

$$S_m(pm)=S_{pm}(pm)+S_m(m)$$

and

$$
\begin{aligned}
S_m(mp^2) &= \sum_{\substack{a \bmod p^2m\\(a,m)=1}}\Lambda(a,p^2m)\\
&\quad\sum_{\substack{a \bmod p^2m\\(a,mp^2)=1}}\Lambda(a,p^2m)+\sum_{\substack{a \bmod p^2m\\(a,mp^2)=p}}\Lambda(a,p^2m)+\sum_{\substack{a \bmod p^2m\\(a,mp^2)=p^2}}\Lambda(a,p^2m)\\
&= S_{mp^2}(mp^2)+\sum_{\substack{b \bmod pm\\(b,mp)=1}}\Lambda(bp,p^2m)+\sum_{\substack{c \bmod m\\(c,m)=1}}\Lambda(cp^2,p^2m)\\
&= S_{mp^2}(mp^2)+S_{mp}(mp)+S_m(m).
\end{aligned}
$$

So

$$
\begin{aligned}
a_p^2S_m(m) &= S_{mp^2}(mp^2)+S_{mp}(mp)+S_m(m)+\varepsilon(p)pS_m(m)+\varepsilon(p)S_m(m)\\
&\quad+\varepsilon(p)(S_{pm}(pm)+S_m(m))\\
&= S_{mp^2}(mp^2)+S_{mp}(mp)(1+\varepsilon(p))+S_m(m)(1+\varepsilon(p)p+2\varepsilon(p))\\
&= S_{mp^2}(mp^2)\\
&\quad+(a_p-1-\varepsilon(p))(1+\varepsilon(p))S_m(m)+S_m(m)(1+\varepsilon(p)p+2\varepsilon(p))\\
&= S_{mp^2}(mp^2)+S_m(m)(a_p+\varepsilon(p)a_p-\varepsilon(p)+\varepsilon(p)p).
\end{aligned}
$$

Simplifying

$$
\begin{aligned}
S_{mp^2}(mp^2) &= \left[a_p^2-a_p-\varepsilon(p)a_p-\varepsilon(p)p+\varepsilon(p)\right]S_m(m)\\
&= \left[(a_p-1)(a_p-\varepsilon(p))-\varepsilon(p)p\right]S_m(m).
\end{aligned}
$$

This is all we require for the next section but we will continue the analysis and establish a general recurrence relation for $S_{mp^t}(mp^t)$ for all $t > 2$. As before

$$\begin{aligned} a_p S_{mp^t}(mp^t) &= \sum_{\substack{a \bmod mp^t \\ (a,mp^t)=1}} \sum_{u=0}^{p-1} \Lambda(a - ump^t, mp^{t+1}) + \varepsilon(p) \sum_{\substack{a \bmod mp^t \\ (a,mp^t)=1}} \Lambda(ap, mp^t) \\ &= S_{mp^t}(mp^{t+1}) + \varepsilon(p) \sum_{\substack{a \bmod mp^{t-1} \\ (a,mp^{t-1})=1}} \Lambda(a, mp^{t-1}) \\ &= S_{mp^t}(mp^{t+1}) + \varepsilon(p) p S_{mp^{t-1}}(mp^{t-1}). \end{aligned}$$

Note that since $t > 2$, cancelling a p does not change the gcd. Now

$$\begin{aligned} S_{mp^t}(mp^{t+1}) &= \sum_{\substack{a \bmod mp^{t+1} \\ (a,mp^t)=1}} \Lambda(a, mp^{t+1}) \\ &= \sum_{\substack{a \bmod mp^{t+1} \\ (a,mp^{t+1})=1}} \Lambda(a, mp^{t+1}) + \sum_{\substack{a \bmod mp^{t+1} \\ (a,mp^{t+1})=p}} \Lambda(a, mp^{t+1}) \\ &= S_{mp^{t+1}}(mp^{t+1}) + S_{mp^t}(mp^t). \end{aligned}$$

Substituting this value above and rearranging terms we find

$$S_{mp^{t+1}}(mp^{t+1}) = a_p S_{mp^t}(mp^t) - \varepsilon(p) p S_{mp^{t-1}}(mp^{t-1})$$

which is the same recurrence satisfied by the original a_{p^t}.

5.2.2 Application to twisted L-series

Since the above formal sums are congruent modulo k to the algebraic part of the L-series, we have

Theorem 5.2.1 *Let χ be Dirichlet character of order k and conductor m, and let ψ be a Dirichlet character of order k and prime conductor p with $(m,p) = 1$. Let $\varepsilon(t) = 1$ if $(t,N) = 1$ and zero otherwise. Then for a modular form f of level N which is a simultaneous eigenform for the Hecke operators we have*

$$L^*(f, 1, \chi\psi) \equiv (a_p - \varepsilon(p) - 1) L^*(f, 1, \chi) \bmod k.$$

If φ is the Dirichlet character of order k and conductor k^2 prime to m we have

$$L^*(f,1,\chi\varphi) \equiv (a_k - 1)(a_k - \varepsilon(k))L^*(f,1,\chi) \bmod k.$$

Proof. We have previously established that $L^*(f,1,\chi) \equiv S_m(m) \bmod k$ and so we use the formulae derived in the previous section reduced modulo k.

$$\begin{aligned} S_{pm}(pm) &= (a_p - 1 - \varepsilon(p))S_m(m) \bmod k \\ S_{mp^2}(mk^2) &= (a_k - 1)(a_k - \varepsilon(k))S_m(m) \bmod k \end{aligned}$$

and the results follow immediately. ■

Consequently, a twist of conductor m can only vanish modulo k if either the L-function or one of the factors $(a_p - \varepsilon(p) - 1)$ vanishes modulo k for some $p|m$. In the special case that $k|m$ vanishing may occur if $a_k \equiv 1 \bmod k$ or $a_k \equiv \varepsilon(k) \bmod k$.

By Cebotarev's theorem (See [34] section 4.2) we know that the traces of Frobenius which can occur, do occur infinitely often and so, for any elliptic curve of zero rank, we can find a positive density of twists such that $a_p \equiv / \ 2 \bmod k$ for each p dividing the conductor of the twist. Consequently, we have

Proposition 5.2.2 *For any elliptic curve E with $L^*(E,1) \not\equiv 0 \bmod k$ we can find an infinity of cyclic twists χ of order k such that $L(E,1,\chi) \neq 0$.* ■

Proposition 5.2.3 *For any elliptic curve E with $L(E,1) \neq 0$ and for each prime order k (with a finite number of exceptions) there exists an infinity of cyclic characters χ of order k such that $L(E,1,\chi) \neq 0$.*

Proof. For all but a finite number of primes

$$L^*(E,1,\chi) \not\equiv 0 \bmod k \Longrightarrow L(E,1,\chi) \neq 0.$$

Hence, for all but this finite number of primes this proposition is implied by the previous one. ■

Chapter 6

Results for higher order twists

As we saw from the computational results, no convincing empirical case can be made for infinite vanishing for twists of order greater than 3. This chapter contains some fragmentary results for higher degree twists.

6.1 Construction of a curve with a point in a quintic extension

The special nature of cyclic quintic extensions permits us to construct a rational elliptic curve with a point in a cyclic quintic extension. While the construction is of interest in itself, it also provides a method of validating the computer programs used to compute the value of the L-function at the critical point.

Let α be the generator of the cyclic quintic extension which is a subfield of the cyclotomic extension $\mathbb{Q}(\zeta_p)$, and let its minimum polynomial be $g(x)$. Let $\beta \in \mathbb{Q}(\alpha)$. Since $(1, \alpha, \alpha^2, \alpha^3, \alpha^4)$ is a basis, we have

$$\beta = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4 \qquad a_i \in \mathbb{Z}$$

and, after reduction modulo g,

$$\beta^2 = b_0 + b_1\alpha + b_2\alpha^2 + b_3\alpha^3 + b_4\alpha^4 \qquad b_i \in \mathbb{Z}$$

where the b's are elementary functions of the a's. This is a genus one curve in quartic form and its jacobian is an elliptic curve

$$y^2 = 4x^3 - Ax - B$$

where

$$\begin{aligned} A &= b_0 b_4 - 4b_1 b_3 + 3b_2^2 \\ B &= b_0 b_2 b_4 + 2b_1 b_2 b_3 - b_0 b_3^2 - b_4 b_1^2 - b_2^3 \end{aligned}$$

This jacobian curve is isomorphic to the quartic and so also has a point in $\mathbb{Q}(\alpha)$. Consequently, its L-function should have a zero at the critical point. The challenge is to choose the a_i in such a way that the resulting jacobian is an elliptic curve of manageable conductor so that we may compute the sign of the functional equation and sum the series of the L-function to reasonable accuracy.

After some experimentation and with the help of Maple, the following example was discovered.

Let $\alpha = \zeta_{11} + \zeta_{11}^{-1} = 2\cos(2\pi/11)$. This has minimum polynomial

$$g(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1$$

A suitable choice is

$$\begin{aligned} \beta &= \alpha^2 + \alpha^3 \qquad \text{whence} \\ \beta^2 &= \alpha^4 + 2\alpha^5 + \alpha^6 \bmod g \\ &= 4\alpha^4 + 7\alpha^3 - 4\alpha - 1 \end{aligned}$$

This gives a jacobian

$$\begin{aligned} y^2 &= 4x^3 - 3 + \frac{15}{16} \qquad \text{or} \\ (4y)^2 &= (4x)^3 - 12(4x) + 15 \end{aligned}$$

with conductor $= 13392$.

Using Cremona's MWrank program we quickly establish that this curve has rank one and therefore the sign of the functional equation is -1. When the twisted L-function program was subsequently run for $10,000$ terms with a cyclic quintic character of conductor 11 it returned a critical value of zero to 19 decimal places.

6.2 Application of Waldspurger's theorem to sextic twists

Let $E/\mathbb{Q}$ be an elliptic curve and χ a cyclic cubic character. Let

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

be the L-function of E. Let $f(z) = \sum_{n=1}^{\infty} a(n)\exp(2\pi inz) \in S_2(N)$ be the weight two eigenform associated to E. It is the Mellin transform of $L(E,s)$. The corresponding twisted L-function $L(E,s,\chi) = \sum_{n=1}^{\infty} \frac{a(n)\chi(n)}{n^s}$ is similarly associated to a modular form with nebentype, $f_\chi \in S_2(N,\chi)$. From the Shimura correspondence stated above we see that there exists a weight $3/2$ form $g_{\chi^2} \in S_{3/2}(2N,\chi^2)$ corresponding to f_χ. Here we have switched the roles of χ and χ^2 in the original statement using the fact that, for cubic characters, $(\chi^2)^2 = \chi$.

We may now use Waldspurger's theorem to handle quadratic twists of these cubic twisted forms and get non-vanishing results as previously. In particular, for a specific cubic twist χ, there are an infinite number of elliptic curves E_D for which $L(E_D,s,\chi) \neq 0$. Assuming the Birch and Swinnerton-Dyer conjecture we can thus say that there exist an infinite number of sextic extensions having a specific cyclic cubic sub-extension for which the rank of E does not increase.

Bibliography

[1] A. Akbary. Non-vanishing of weight k modular L)-functions with large level., year = 1999, journal = J. Ramanujan Math. Soc., volume = 14, pages = 37-54, number = 1.

[2] C. Batut, D. Bernardi, H. Cohen, and M. Olivier. *User's Guide to PARI-GP.* FTP file, 1994.

[3] J. Buhler, B. H. Gross, and D. B. Zagier. On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. *Math. Comp.*, 44:473–481, 1985.

[4] D. Bump, S. Friedburg, and J. Hoffstein. On some applications of automorphic forms to number theory. *Bull. Amer. Math. Soc. (N.S.)*, 33:157–175, 1996.

[5] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[6] J. E. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, 1992.

[7] J. E. Cremona. Computing the degree of the modular parameterization of a modular elliptic curve. *Math. Comp.*, 64:1235–1250, 1995.

[8] J. E. Cremona. *Algorithms for Modular Elliptic Curves.* Cambridge University Press, second edition, 1997.

[9] W. Duke. The critical order of vanishing of automorphic L-functions with large level. *Invent. Math.*, 119(2):165–174, 1995.

[10] D. Goldfeld. Conjectures on elliptic curves over quadratic fields. In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, pages 108–118. Springer, Berlin, 1979.

[11] D. Goldfeld. On the computational complexity of modular symbols. *Math. Comp.*, 58(198), 1992.

[12] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers.* Oxford, at the Clarendon Press, 1954. 3rd ed.

[13] K. James. L-series with nonzero central critical value. *J. Amer. Math. Soc.*, 11(3):635–641, 1998.

[14] S. Kamienny. Torsion points on elliptic curves over fields of higher degree. *International Mathematics Research Notices*, 6, 1992.

[15] N. M. Katz and P. Sarnak. Zeroes of zeta functions and symmetry. *Bull. Amer. Math. Soc.(N.S.)*, 36(1):1–26, 1999.

[16] W. Kohnen. Fourier coefficients of modular forms of half-integral weight. *Math. Ann.*, 271(2):237–268, 1985.

[17] V. A. Kolyvagin and D. Y. Logachev. Finiteness of the group of rational points for some abelian modular varieties. *Leningrad Math J.*, 188:1229–1253, 1990.

[18] G. Kramarz and D. B. Zagier. Numerical investigations related to the L-series of certain elliptic curves. *J. Indian Math. Soc.*, 52:51–60, 1987.

[19] M. Kuwata. Points defined over cyclic cubic extensions on an elliptic curve and generalized Kummer surfaces. *preprint*, pages 1–13, 2000.

[20] S. Lang. *Number theory. III.* Springer-Verlag, Berlin, 1991. Diophantine geometry.

[21] B. Mazur. Modular curves and the Eisenstein ideal. *Pub. math de l'IHES*, 47:33–186, 1976.

[22] B. Mazur, J. Tate, and J. Teitelbaum. On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer. *Invent. Math.*, 84:1–48, 1986.

[23] H. Montgomery. The pair correlation of zeroes of the zeta function. *Proc. Sym. Pure Math.*, 24:181–193, 1973.

[24] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Philos. Soc.*, 21:179–192, 1922.

[25] M. R. Murty and V. K. Murty. Mean values of derivatives of modular L-series. *Ann. math*, 133:447–475, 1991.

[26] V. K. Murty. Modular elliptic curves. In V. K. Murty, editor, *Seminar on Fermat's last theorem*, volume 17, chapter 1. Canadian Mathematical Society, 1995.

[27] A. Odlyzko. The 10^{20}-th zero of the Riemann zeta function and 70 million of its neighbors. *(preprint) A.T.T*, 1989.

[28] K. Ono. Twists of elliptic curves. *Compositio Math.*, 106(3):349–360, 1997.

[29] K. Ono and C. Skinner. Non-vanishing of quadratic twists of modular L-functions. *Invent. Math.*, 134(3):651–660, 1998.

[30] D. E. Rohrlich. On L-functions of elliptic curves and cyclotomic towers. *Invent. Math.*, 75:409–423, 1984.

[31] D. E. Rohrlich. The vanishing of certain Rankin-Selberg convolutions. In *Automorphic Forms and Analytic Number Theory*, pages 123–133. Univ. Montréal, Montréal, PQ, 1989.

[32] K. Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103:25–68, 1991.

[33] K. Rubin. Euler systems and modular elliptic curves. In *Galois representations in arithmetic algebraic geometry (Durham 1996)*, pages 351–367. Cambridge Univ. Press, 1998.

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

[35] X. She. *On the non-vanishing of cubic twists of automorphic L-series.* PhD thesis, Brown University, 1995.

[36] G. Shimura. *Introduction to the arithmetic theory of automorphic forms.* Iwanami Shoten and Princeton University Press, 1971.

[37] G. Shimura. On modular forms of half integral weight. *Ann. of Math.*, 97(2):440–481, 1973.

[38] T. Stefanicki. Non-vanishing of L-functions attached to automorphic representations of $GL(2)$ over $\mathbf{Q}$. *J. Reine Angew. Math.*, 474:1–24, 1996.

[39] C. L. Stewart and J. Top. On ranks of twists of elliptic curves and power-free values of binary forms. *J. Amer. Math. Soc.*, 8(4):943–973, 1995.

[40] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Annals of Mathematics*, 141:553–572, 1995.

[41] V. Vatsal. Rank-one twists of a certain elliptic curve. *Math. Ann.*, 311(4):791–794, 1998.

[42] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl.(9)*, 60(4):375–484, 1981.

[43] A. Weil. Sur un théorème de Mordell. *Bull. Sci. Math.*, 54:497–508, 1930.

[44] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics*, 141:443–551, 1995.

Appendix A

Detailed table of vanishing twists

The following list tabulates the conductors below 1000 of cyclic characters χ of orders 3, 5 and 7 for which $L(E,1,\chi) = 0$. The elliptic curves are named as in Cremona's tables [8]. Repetitions are possible in the case of composite characters.

11A

```
Order 3 [151 157 307 571 643 721 873 997]
```

14A

```
Order 3 [31 117 171 247 283 333 337 499 547 559 657 673 691 711
         711 733 919 997]
Order 5 [251 641]
```

15A

```
Order 3 [103 163 193 259 577 679 679 703 727 973]
Order 5 [661]
```

17A

```
Order 3 [127 133 171 247 277 499 679 703 853 873]
Order 5 [251]
```

19A

Order 3 [43 63 67 73 117 279 373 387 403 439 469 481 487 523 547 559 643 657 721 819 873]

20A

Order 3 [9 63 73 91 117 133 171 229 259 277 307 559 613 703 711 711 727 763 819 819 829 871 889 889 919 973]
Order 5 [671]

21A

Order 3 [103 643 769 811 817 919]
Order 5 [41 451]

24A

Order 3 [31 67 133 133 151 193 247 469 547 589 613 679 691 703 739 817 853 871]
Order 5 [431]
Order 7 [491]

26A

Order 3 [127 133 181 301 457 511 643 657 691 711 997]

26B

Order 3 [73 157 193 307 313 439 511 643 657 711 711 997]

27A

Order 3 [19 37 109 127 181 217 397 427 553 721 739 793 811 871 883 949]

30A

Order 3 [61 67 127 133 259 367 427 439 553 607 643 733 763 871 949 973 997]

32A

Order 3 [349 397]

33A

Order 3 [67 103 151 499 547 553 613 619 643 853 871 889]

34A

Order 3 [9 63 73 133 163 217 283 439 549 559 703 711 769 819
873 981]

35A

Order 3 [43 67 171 279 333 409 433 457 657 711 711 811 873 949]
Order 5 [11]

36A

Order 3 [301 397 403 481 889]

37A

Order 3 [43 61 103 127 171 247 817 853]
Order 5 [41]

37B

Order 3 [7 13 63 117 133 157 181 217 279 283 301 337 387 387 403
427 657 721 757 793 819 819 823 871 871 981 981]

38A

Order 3 [13 43 61 63 63 79 117 211 217 279 387 403 427 439 469
511 553 657 763 763 819 877 883]
Order 5 [661]

38B

Order 3 [13 61 79 117 229 403 427 553 819 823]
Order 5 [41 781]
Order 7 [71]

39A

Order 3 [7 73 133 163 229 259 301 421 439 607 643 889 937 967]

40A

```
Order 3 [7 63 91 223 259 277 301 427 499 547 619 679 757 853
         883 919 973]
Order 5 [311]
```

42A

```
Order 3 [19 43 247 331 367 487 559 643 703 703 853 997]
Order 5 [241]
```

43A

```
Order 3 [91 109 259 271 427 439 469 481 657 721 739 871 949 967]
Order 5 [251]
```

44A

```
Order 3 [13 117 117 217 333 379 387 387 397 457 511 549 603 739
         819 949 973 997]
```

45A

```
Order 3 [103 163 193 481 577 679 763 973]
```

46A

```
Order 3 [139 223 307 481 613]
```

48A

```
Order 3 [43 127 223 397 457 661 679 733 853]
Order 5 [775]
```

49A

```
Order 3 [547]
```

50A

```
Order 3 [463 703 823]
Order 5 [31 341]
```

50B

```
Order 3 [19 31 61 133 241 379 439 553 589 711 751 811 817 829
         919]
Order 5 [341]
```

51A

```
Order 3 [217 403 577 721]
Order 5 [275]
```

52A

```
Order 3 [511 859]
```

53A

```
Order 3 [171 241 247 259 367 421 499 559]
```

54A

```
Order 3 [7 73 91 109 427 511 553 721 793 811 871 889]
Order 5 [11]
```

54B

```
Order 3 [7 13 67 73 91 133 217 241 247 259 313 337 367 427 427
         481 499 511 523 553 643 721 763 763 769 793 817 853 871]
Order 5 [431 761]
```

55A

```
Order 3 [13 19 61 67 91 117 133 171 181 313 349 403 469 511 511
         553 553 603 643 657 703 711 711 721 721 819 877 927 997]
Order 5 [31]
```

56A

```
Order 3 [19 31 43 109 117 117 171 337 487 499 559 703 927]
Order 5 [431 451]
```

56B

```
Order 3 [127 313 331 337 691]
```

57A

```
Order 3 [31 43 127 241 337 439 499 631 871]
Order 5 [25 151 251 911]
```

57B

```
Order 3 [67 109 163 181 217 217 259 259 301 313 367 403 421 481
         487 523 721 757 763 871]
Order 7 [29]
```

57C

```
Order 3 [31 43 259 727 871 919]
Order 5 [275]
```

58A

```
Order 3 [9 73 91 127 133 217 307 333 499 619 657 763 819]
Order 5 [41 431]
Order 7 [71]
```

58B

```
Order 3 [91 103 117 117 193 247 259 333 403 439 727 787 793 793
         823 927]
Order 5 [275]
```

61A

```
Order 3 [31 37 109 171 259 307 313 333 373 421 523 691 703 733
         829 889 967 973 997]
Order 5 [11 691 761]
```

62A

```
Order 3 [13 43 117 163 181 247 301 387 481 613 679 721 811 819
         853 871 873 919]
Order 7 [29]
```

63A

```
Order 3 [103 151 193 643 727 817]
```

64A

Order 3 [853]

65A

Order 3 [63 271 279 397 427 469 549 607 703 721]
Order 5 [41 71]

66A

Order 3 [13 43 91 91 133 229 247 457 469 589 661 679 703 709
721 733 817 973]

66B

Order 3 [7 91 259 271 421 511 763]

66C

Order 3 [109 127 181 307 523 571 643 883 997]
Order 5 [31 151]

67A

Order 3 [481 619 927]

69A

Order 3 [67 163 313 763]

70A

Order 3 [163 279 313 333 333 421 487 853]

72A

Order 3 [151 193 397 403 577 817]

73A

Order 3 [7 19 63 67 79 91 133 133 229 247 259 499 547 577 589
613 703 711 763 817 859]
Order 5 [311]

75A

```
Order 3 [139 823]
Order 5 [541]
```

75B

```
Order 3 [13 127 181 211 301 337 409 457 511 769 871 973]
```

75C

```
Order 3 [43 91 109 127 247 247 307 601 613]
```

76A

```
Order 3 [229 397 607 871]
```

77A

```
Order 3 [61 103 171 229 277 313 333 421 883]
Order 5 [25 181]
```

77B

```
Order 3 [37 61 117 223 229 421 559 559 657 673 703 711 769 811
         871 877 949]
```

77C

```
Order 3 [313 487 769 871]
```

78A

```
Order 3 [643 727]
```

79A

```
Order 3 [43 199 217 277 307 427 469 679 873 919]
Order 5 [31 191 641]
Order 7 [29]
```

80A

```
Order 3 [31 43 109 171 247 277 307 703 703 721 763]
Order 5 [241]
```

80B

Order 3 [13 91 117 181 229 259 313 337 349 763 769 819 871]

82A

Order 3 [31 63 63 67 73 163 193 259 367 457 601 643 727 793 817
967 973]
Order 5 [11 25 181]

83A

Order 3 [171 259 333 549 549 657 853 871]

84A

Order 3 [19 61 337 487 589 817]
Order 5 [41]

84B

Order 3 [19 103 223 247 589]

85A

Order 3 [13 37 181 247 259 313 547 631 679 691 703 763]

88A

Order 3 [13 19 31 63 217 247 367 387 439 457 549 657 733 853 919
973 973 997]
Order 5 [251 431 811]

89A

Order 3 [439 457 541 603 691 763 819 991]
Order 5 [25 131 341 451 491]

89B

Order 3 [7 13 43 63 117 133 133 199 217 247 259 313 337 373 469
487 553 763 817 823 829 859 871 919 949]
Order 5 [151]

90A

```
Order 3 [13 31 109 133 157 163 217 223 247 283 307 481 499 589
         589 601 679 703 727 793 817 919 973]
Order 7 [71]
```

90B

```
Order 3 [13 43 67 91 91 133 163 199 211 217 247 409 469 679 691
         703 763 817 871 973]
Order 5 [781]
```

90C

```
Order 3 [67 73 91 91 133 217 247 259 307 367 439 457 469 523 553
         559 589 613 679 691 757 763 853 949 973]
Order 5 [761]
```

91A

```
Order 3 [241 457 603 661 703 817]
```

91B

```
Order 3 [9 61 67 171 223 241 279 283 307 397 457 589 603 619 657
         657 711 711 817 853 873 981 991]
Order 5 [151 341 671]
```

92A

```
Order 3 [9 63 117 157 279 307 333 457 511 549 553 711 819 873 883
         981]
```

92B

```
Order 3 [7 63 67 91 193 217 247 259 271 301 523 549 709 721 973]
Order 5 [41 341]
```

94A

```
Order 3 [13 547 603 711 997]
```

96A

```
Order 3 [7 19 91 109 157 163 181 217 223 247 259 301 337 373 379
         421 427 469 487 661 673 703 811 817]
Order 7 [29 113]
```

96B

```
Order 3 [31 43 109 127 229 457 469]
Order 5 [41 251 451]
Order 7 [29 113]
```

98A

```
Order 3 [127 373 387 883]
```

99A

```
Order 3 [43 163 277 349 403 409 643]
Order 5 [191]
```

99B

```
Order 3 [103 619 709]
```

99C

```
Order 3 [103 271 307 499 553 643 679 709 937 997]
Order 5 [41]
```

99D

```
Order 3 [337 853]
```

Appendix B

Program listings

The following Pari-GP programs compute the twisted L-series used in this thesis. They use the 'local' command which was introduced in version 2.16.

Constants and global variables

```
default(parisize,40000000)
default(format,''g0.7'')
print(''Please call jinit to initialize
       ecurve,cond,eps,tol,sterms,an,kappa'')
e11=ellinit([0,-1,1,-10,-20]);
e37a=ellinit([0,0,1,-1,0]);
e37b=ellinit([0,1,1,-23,-50]);
e40=ellinit([0,0,0,-7,-6]);
e307a=ellinit([0,0,1,-8,-9]);
e307b=ellinit([1,1,0,0,-1]);
e307c=ellinit([0,0,1,1,-1]);
e307d=ellinit([0,-1,1,2,-1]);
e43=ellinit([0,1,1,0,0]);
\\global(ecurve=e11,cond=11,eps=1,digs=10,sterms=10000,an,lval);

\r crem200

\\ Jinit sets up global variables for the i th entry
\\ in etable (see table below)
 jinit(ii,kk=3,dd=10)=
```

```
{
local(c);
ecurve=ellinit(etable[ii]);
cond=ellglobalred(ecurve)[1];
sterms=terms(cond,5000,dd);
eps=1;if(etable[ii-1]<0,eps=-1);
an=ellan(ecurve,sterms);
lval=elllseries(ecurve,1.0);
cond
}

\\This function  computes the number of terms required for
\\at least dig digits accuracy in computing the L-function
terms(c,m,dig)=
{
local(q);
q=exp(-2*Pi/(m*sqrt(c)));
truncate(max(100,round((log(1.-q)-dig*log(10.))/log(q))));
}
```

Functions to evaluate twisted L-series using infinite sums

```
\\ lccrit computes the critical value of the twisted L-series
\\ of ecurve twisted by the primitive character (m,k,r)
lccrit(m,k,r=1,nn=sterms)=
{
local(n,qq,w,ppsi,cpsi,s);
qq=exp(-2*Pi/(m*cond^.5));
v=cchtab(m,k,r);
ppsi=v[cond%m+m];
w=gsum(m,v);
cpsi=ppsi*w*w/m;
s=sum(n=1,nn,an[n]*(v[n%m+m]+eps*cpsi*conj(v[n%m+m]))*qq^n/n);
rmdr=4*qq^nn/(1-qq);
s
}
\\ Computes the rth character table of a composite character
\\ where r is the base k representation of the powers of the
```

```
\\prime characters.
cchtab(m,k,r)=
{
local(v,x,vv,t,nn,d,nvec,basevec,charvec,rr);
if(isprime(m),return(chtab(m,k,r)));
v=vector(2*m,x,1);
\\ Starts by setting up a vector of 'prime' factors
\\ of m.  k^2 is treated like a prime.
if(!istwist(m,k),
   return([m,'' is not valid twist for order '',k,
             '' and ell curve conductor '',cond]));
nvec=omega(m);charvec=vector(nvec,x,0);
if(gcd(k^2,m)==k^2,charvec[1]=k^2;kk=2;nn=m\k^2, nn=m;kk=1);
fordiv(nn,d,if(isprime(d),charvec[kk]=d;kk++,));
\\print(nvec,charvec);
\\ We now express r in base k-1 format.
if(r>k^nvec,print([r,'' is too large for twist '',m,charvec]);
   return(0),);
basevec=vector(nvec,x,0);rr=r-1;kk=1;
while(rr!=0,basevec[kk]=rr%(k-1);rr=rr\(k-1);kk++);
for(kk=1,nvec,basevec[kk]++);
\\print(basevec);
\\ Now we compute the characters.
for(kk=1,nvec,vv=chtab(charvec[kk],k,basevec[kk]);
  for(t=1,2*m,v[t]*=vv[t%charvec[kk]+charvec[kk]]));
v
}

\\ Computes a vector of length 2*p representing the Dirichlet
\\ character of conductor p and degree k as complex roots of
\\ unity. The value of the character at the primitive root
\\ computed by Pari is exp(2*Pi*I*r/k).
chtab(p,k,r)=
{
local(g,n,v,zet);
if(k==1,return(vector(2*p,xx,1)));
g=znprimroot(p);
v=vector(2*p,xx,0);
```

```
zet=exp(2*Pi*I*r/k);
for(n=1,p,v[lift(g^n)]=zet^n);v[p]=0;
for(n=p+1,2*p,v[n]=v[n-p]);
v
}

\\ we assume k is prime and check if n is a sq free product
\\of primes ==1 mod k possibly multiplied by k^2
\\ and prime to cond.
istwist(m,k)=
{
if(gcd(m,cond)!=1,return(0));
if(k==1,return(1));
if(gcd(k^2,m)==k^2,m/=k^2);
if(gcd(m,k)!=1,return(0));
if(isprime(m) & m%k==1,return(1));
if(!issquarefree(m),return(0));
fordiv(m,d,if((isprime(d) & d%k!=1),return(0)));
1
}

\\Compute the Gauss sum
gsum(p,v)=
{
local(n,q,s,t);
q=exp(2*Pi*I/p);t=q;s=0;
for(n=1,p-1,s+=v[n]*t;t*=q);
s
}

\\Compute the derivative of the twisted L-series at the
\\critical point.
lcdcrit(eps,cond,m,k,r,nn)=
{
local(zz,w,n);
zz=2*Pi/(m*cond^.5);v=cchtab(m,k,r);
ppsi=v[cond%m+m];w=gsum(m,v);cpsi=ppsi*w*w/m;
s=sum(n=1,nn,an[n]*(v[n%m+m]-eps*cpsi*conj(v[n%m+m]))*eint1(n*zz)/n);
```

```
s
}

\\Remove unnecessary digits when viewing vectors of
\\complex numbers.
trim(v)=
{
local(n,nn,eps,w,xx,yy);
w=Vec(v);
nn=length(w);eps=10^-10;print(''nn= '',nn);
for(n=1,nn,xx=real(w[n]);yy=imag(w[n]);
    if(abs(xx)<eps,xx=0,);if(abs(yy)<eps,yy=0,);
    if(abs(abs(xx)-1)<eps,xx=sign(xx),);
    if(abs(abs(yy)-1)<eps,yy=sign(yy),);w[n]=xx+I*yy);
if(nn==1,return(w[1]),return(w));
}

\\Compute the critical value of the twisted L-series
\\for twists of prime conductor.
lcrit(eps,cond,p,k,r,nn)=
{
local(n,qq,w,v,ppsi,cpsi,s);
if(k==1 | p==1,return(lseries(eps,cond,nn)));
qq=exp(-2*Pi/(p*cond^.5));
v=chtab(p,k,r);
ppsi=v[cond%p+p]; w=gsum(p,v); cpsi=ppsi*w*w/p;
s=sum(n=1,nn,an[n]*(v[n%p+p]+eps*cpsi*conj(v[n%p+p]))*qq^n/n);
rmdr=4*qq^nn/(1-qq);
s
}
```

Functions to compute modular symbols

```
\\Set up the conductor matrix with the values of reduced M-symbols.
condinit(c=cond,k)=
{
local(t,u);
condmat=matrix(c,c,x,y,0);
```

```
accummat=matrix(c,c,x,y,0);
pccummat=matrix(c,c,x,y,vector(k,z,0));
for(t=1,c,for(u=1,c,
if([t,u]==msred([t,u]),condmat[t,u]=zsum(t,u),next);
))
}

\\ Compute the Manin symbol (t,u) for squarefree conductor
\\ using a method of Goldfeld.
zsum(t,u)=
{
local(avec,m1,m,t1,h,s,r,u1,s1,L,uu,sssum,q1,q2,c1,c2);
local(tt1,tt2,n,temp,gammaM,temp2,gammaN,gammaMMh);
nlim=10*cond; \\ Maybe this should be replaced with sterms!!
if(u==t | gcd(u,t)!=1,return(0.0));
  avec=bezout(u,t);                    \\print([1,t,u,avec]);
  r=avec[1];s=avec[2];                \\print([2,t,u,s,r]);
  m1=gcd(t,cond);m=cond/m1;t1=t/m1;\\print([3,t,u,m1,m,t1]);
  avec=bezout(t,m);h=avec[1]*u/avec[3];u1=avec[2]*u/avec[3];
  s1=s-r*h;mh=gcd(m,h);\\print([4,t,u,avec,h,u1,s1,mh]);
  if(gcd(h*cond/m,m/mh)!=1,
     print(''error in gcd'',t,u,r,s,m,h,mh]);return);
  if(m/mh==1,L=1,L=lift(Mod(1,m/mh)/Mod(h*cond/m,m/mh)));
  \\if( m/mh == 1 , L = 1 , L = m/(h*cond) % (m/mh) );
  \\P. Green's version
  \\print([t,u,r,s,m,h,mh,L]);
  uu=sqrt(m*mh);
  sssum=0.0+0.0*I;\\print([5,t,u,L,uu]);
  q1=exp(-(2*Pi/m)*(uu/sqrt(cond)-I*h));
  q2=exp(-2*Pi*mh*(1./(uu*sqrt(cond))+I*L/m));

/* compute the gammas. This is P. Green's correction. */
temp = factor(m); temp2 = matsize(temp);
gammaM = prod(i=1,temp2[1],(-an[temp[i,1]])^temp[i,2]);
temp = factor(cond); temp2 = matsize(temp);
gammaN = prod(i=1,temp2[1],(-an[temp[i,1]])^temp[i,2]);
temp = factor(m/mh); temp2 = matsize(temp);
gammaMMh = prod(i=1,temp2[1],(-an[temp[i,1]])^temp[i,2]);
```

```
  tt1=gammaM;tt2=-gammaN*gammaM*gammaMMh;
for(n=1,nlim,tt1*=q1;tt2*=q2;sssum+=(an[n]/n)*(tt1+tt2));
if(abs(sssum)<.00000000001,sssum=0);
if(abs(real(sssum))<.00000000001,sssum=imag(sssum)*I);
if(abs(imag(sssum))<.00000000001,sssum=real(sssum));
\\print([8,t,u,m,m1,mh,h,L,c1,c2,sssum]);
sssum
}

\\Returns the denominators of the convergents of
\\a rational number x
convers(x)=
{
local(cfr,n,mfr,vfr,nn);
cfr=contfrac(x);
n=length(cfr);mfr=contfracpnqn(cfr);
vfr=cfr;vfr[n]=mfr[2,1];vfr[n-1]=mfr[2,2];
if(n>2,forstep(nn=n-2,1,-1,vfr[nn]=vfr[nn+2]-cfr[nn+2]*vfr[nn+1]),);
vfr
}

\\Reduces the vector vfr to m-symbols for conductor, cond.
msymbol(vfr)=
{
local(n,nn,ms,mslist);
n=length(vfr);mslist=vector(n-1,x,[0,0]);
forstep(nn=n,2,-1,
ms=[(-1)^nn*vfr[nn],vfr[nn-1]];ms=msred(ms);mslist[nn-1]=ms);
mslist
}

\\ Reduces a modular symbol modulo the conductor, cond.
msred(ms)=
{
local(mms);
mms=ms%cond;
if(mms[2]==0,return([1,cond]));
if(mms[1]==0,return([cond,1]));
```

```
if(mms[2]==1,return(mms));
if(mms[1]==1 & gcd(mms[2],cond)>1,return(mms));
if(gcd(cond,mms[2])==1,
 mms[1]=lift(Mod(mms[1],cond)/Mod(mms[2],cond));
 mms[2]=1;return(mms));
if(gcd(cond,mms[1])==1,
 mms[2]=lift(Mod(mms[2],cond)/Mod(mms[1],cond));
 mms[1]=1;return(mms));
if(mms[1]==0,mms[1]=cond,);if(mms[2]==0,mms[2]=cond,);
if(gcd(gcd(mms[1],mms[2]),cond)==1,mms=mms/gcd(mms[1],mms[2]),);
mms=mms/gcd(mms[1],mms[2])
}

\\ evaluates {0,a/d}
valsym(a,d)=
{
local(n,vfr,mm,m,tsum,mfr,kk);
vfr=convers(a/d);mfr=msymbol(vfr);mm=length(mfr);
accummat*=0;for(m=1,mm,accummat[mfr[m][1],mfr[m][2]]+=1);
tsum=0;
for(m=1,cond,for(n=1,cond,kk=accummat[m,n];tsum+=kk*condmat[m,n]));
\\ om1=ecurve.omega[1]/2;om2=I*imag(ecurve.omega[2]);
\\ print([a,d,tsum,lindep([-tsum,om1,om2])]);
tsum
}

\\ Evaluates the rational modular symbol
\\ mazsym(a,d):=  ({0,a/d}+{0,(d-a)/d})/ecurve.omega[1].
mazsym(a,d)=
{
local(z);
z=(valsym(a,d)+valsym(d-a,d))/ecurve.omega[1];
if(abs(imag(z))<.0000001,z=real(z));
if(abs(real(z))<.0000001,z=imag(z));
z
}
```

Compute twisted L-series using modular symbols

```
\\ Compute the critical value of the L-series of ecurve
\\ twisted by (d,k,r) using finite sum of modular symbols.
lctwist(d,k,r)=
{
local(n,chi,vfr,mfr,mm,m,tsum,v);
if(k==1 | d==1,return(valsym(1,cond)));
v=cchtab(d,k,r);
accummat*=0;
for(n=1,d-1,chi=conj(v[n+d]);
    vfr=convers(n/d);mfr=msymbol(vfr);mm=length(mfr);
  for(m=1,mm,accummat[mfr[m][1],mfr[m][2]]+=chi));
tsum=0;for(m=1,cond,for(n=1,cond,tsum+=accummat[m,n]*condmat[m,n]));
tsum=tsum*gsum(d,v)/d;
if(real(v[d-1])<0,return(tsum),return(-tsum));
}

\\Mazsum computes the sum
\\S_m(mpk)=SUM{a mod mpk,(a,m)=1}mazsym(a,mpk).
\\Alternatively it may compute the above sum
\\twisted by (mpk,k,r).
mazsum(m,mpk,const=-1,k=0,r=0)=
{
local(s,n,v,a);
if(const==-1,cc=-2*lval/ecurve.omega[1],cc=const);
if(k==0,s=0;
   for(a=1,mpk,if(gcd(a,m)==1,s+=mazsym(a,mpk)+cc));return(s));
v=cchtab(mpk,k,r);
s=0;for(a=1,mpk-1,s+=conj(v[mpk+a])*mazsym(a,mpk));return(s);
}

hecke(a,m,p,const=-1)=
{
local(msz,mszz,cc);
if(const==-1,cc=-2*lval/ecurve.omega[1],cc=const);
msz=mazsym(a*p,m)+cc;
print([an[p]*(mazsym(a,m)+cc),''='',msz]);
```

```
for(u=0,p-1,mszz=mazsym(a-u*m,p*m)+cc;
  print(''+'',mszz]);msz+=mszz);
msz
}
```

Programs which print lists of twisted L-series of various kinds

```
\\Search lists twisted L-series of  |critical value|<.001
\\ for prime conductors between pp and ppp.
\\Characters are order k.
search(k,pp,ppp)=
{
local(qexp,p,w);
qexp=-2*Pi/sqrt(cond);
t=terms(cond,ppp,10);
if(t>sterms,an=ellan(ecurve,t);sterms=t);
forprime(p=pp,ppp,
  if(istwist(p,k),w=test(p,k,1,qexp),next);
  if(abs(w)<.001,print([cond,k,p,w,rmdr]))
  );
}

\\ Test is used by search to compute the critical value.
test(p,k,r,qexp)=
{
local(rho);
rho=exp(qexp/p);
nterms=terms(cond,p,10);
lccrit(p,k,r,nterms)
}

\\Search for zero twists when ell curve has sq free conductor,
\\using modular series
bigrun(crem1,crem2,mcond1,mcond2,korder1=3,korder2=7)=
{
local(lcrem,twistlim);
lcrem=min(length(etable),crem2);
forstep(ncrem=crem1,lcrem,2,jinit(ncrem);
```

```
        if(!issquarefree(cond),next);condinit(cond,korder2);
  for(m=mcond1,mcond2,
    forstep(k=korder1,korder2,2,if(!istwist(m,k),next);
      twistlim=(k-1)^(omega(m)-1);
      for(r=1,twistlim,lct=lctwist(m,k,r);
       if(abs(lct)<.000001,print([ncrem,cond,m,k,r,lct]))
       )
     )
    )
  );
}

\\Search for zero twists when ell curve has sq full conductor,
\\using infinite series.
 bigrunsq(crem1,crem2,mcond1,mcond2,korder1=3,korder2=7)=
{
local(lcrem,twistlim);
lcrem=min(length(etable),crem2);
forstep(ncrem=crem1,lcrem,2,jinit(ncrem);if(issquarefree(cond),next);
  for(m=mcond1,mcond2,\\print([cond,m]);
    forstep(k=korder1,korder2,2,if(!istwist(m,k),next);
      twistlim=(k-1)^(omega(m)-1); \\print([cond,m,k,twistlim]);
      for(r=1,twistlim,t=terms(cond,m,10);\\print([cond,m,k,r,t]);
        if(t>sterms,an=ellan(ecurve,t);sterms=t);lct=lccrit(m,k,r,t);
       if(abs(lct)<.0001,
       print([cond,m,k,r,lct,rmdr,t]))
       )
     )
    )
  );
}

\\Search for zero composite conductor twists for all ell curves
comprun(crem1,crem2,mcond1,mcond2,korder1=3,korder2=7)=
{
local(lcrem,twistlim,t);
lcrem=min(length(etable),crem2);rmdr=0;
forstep(ncrem=crem1,lcrem,2,jinit(ncrem);
```

```
   if(issquarefree(cond),condinit(cond,korder2));
   for(m=mcond1,mcond2, if(isprime(m),next);
     forstep(k=korder1,korder2,2,if(!istwist(m,k),next);
       twistlim=(k-1)^(omega(m)-1);
       for(r=1,twistlim,
         if(issquarefree(cond),lct=lctwist(m,k,r);rmdr=0;t=0);
         if(!issquarefree(cond),t=terms(cond,m,10);
           if(t>sterms,
              an=ellan(ecurve,t);sterms=t);lct=lccrit(m,k,r,t));
        if(abs(lct)<.0001,
        print([cond,m,k,r,lct,rmdr,t]))
        )
      )
     )
   );
}

\\Search for vanishing for twists and elliptic curves
\\ in the specified ranges.
onekrun(crem1,crem2,mcond1,mcond2,korder1=3,korder2=7)=
{
local(lcrem,twistlim,t);
lcrem=min(length(etable),crem2);rmdr=0;
forstep(ncrem=crem1,lcrem,2,jinit(ncrem);
  if(issquarefree(cond),condinit(cond,korder2));
  print('' \n''[ncrem,cond]);
  for(m=mcond1,mcond2,
    forstep(k=korder1,korder2,2,if(!istwist(m,k),next);
      twistlim=(k-1)^(omega(m)-1);
      for(r=1,twistlim,
        if(issquarefree(cond),lct=lctwist(m,k,r);rmdr=0;t=0);
        if(!issquarefree(cond),t=terms(cond,m,10);
          if(t>sterms,an=ellan(ecurve,t);sterms=t);
             lct=lccrit(m,k,r,t));
       if(abs(lct)<.0001,
          print1([m,k]'' ''))
       ))));
}
```

The table of elliptic curves used in this study

A number of the above routines refer to the vector 'etable'. This is a list of the elliptic curves of conductor below 100 which is used in all the computations. It is a list of the strong curves in Cremona's tables [8] organized for simple access by the Pari system. The format is $N, [a_1, a_2, a_3, a_4, a_6]$ where N is the conductor of the curve with a positive or negative sign depending on the root number and the a_i are the Weierstrass coefficients of the strong Weil curve. The content of the table is as follows:

```
etable=\
[11 ,[0,-1,1,-10,-20],\
14 ,[1,0,1,4,-6],\
15 ,[1,1,1,-10,-10],\
17 ,[1,-1,1,-1,-14],\
19 ,[0,1,1,-9,-15],\
20 ,[0,1,0,4,4],\
21 ,[1,0,0,-4,-1],\
24 ,[0,-1,0,-4,4],\
26 ,[1,0,1,-5,-8],\
26 ,[1,-1,1,-3,3],\
27 ,[0,0,1,0,-7],\
30 ,[1,0,1,1,2],\
32 ,[0,0,0,4,0],\
33 ,[1,1,0,-11,0],\
34 ,[1,0,0,-3,1],\
35 ,[0,1,1,9,1],\
36 ,[0,0,0,0,1],\
-37 ,[0,0,1,-1,0],\
37 ,[0,1,1,-23,-50],\
38 ,[1,0,1,9,90],\
38 ,[1,1,1,0,1],\
39 ,[1,1,0,-4,-5],\
40 ,[0,0,0,-7,-6],\
42 ,[1,1,1,-4,5],\
-43 ,[0,1,1,0,0],\
44 ,[0,1,0,3,-1],\
45 ,[1,-1,0,0,-5],\
46 ,[1,-1,0,-10,-12],\
```

```
48 ,[0,1,0,-4,-4],\
49 ,[1,-1,0,-2,-1],\
50 ,[1,0,1,-1,-2],\
50 ,[1,1,1,-3,1],\
51 ,[0,1,1,1,-1],\
52 ,[0,0,0,1,-10],\
-53 ,[1,-1,1,0,0],\
54 ,[1,-1,0,12,8],\
54 ,[1,-1,1,1,-1],\
55 ,[1,-1,0,-4,3],\
56 ,[0,0,0,1,2],\
56 ,[0,-1,0,0,-4],\
-57 ,[0,-1,1,-2,2],\
57 ,[1,0,1,-7,5],\
57 ,[0,1,1,20,-32],\
-58 ,[1,-1,0,-1,1],\
58 ,[1,1,1,5,9],\
-61 ,[1,0,0,-2,1],\
62 ,[1,-1,1,-1,1],\
63 ,[1,-1,0,9,0],\
64 ,[0,0,0,-4,0],\
-65 ,[1,0,0,-1,0],\
66 ,[1,0,1,-6,4],\
66 ,[1,1,1,-2,-1],\
66 ,[1,0,0,-45,81],\
67 ,[0,1,1,-12,-21],\
69 ,[1,0,1,-1,-1],\
70 ,[1,-1,1,2,-3],\
72 ,[0,0,0,6,-7],\
73 ,[1,-1,0,4,-3],\
75 ,[0,-1,1,-8,-7],\
75 ,[1,0,1,-1,23],\
75 ,[0,1,1,2,4],\
76 ,[0,-1,0,-21,-31],\
-77 ,[0,0,1,2,0],\
77 ,[0,1,1,-49,600],\
77 ,[1,1,0,4,11],\
78 ,[1,1,0,-19,685],\
```

```
-79 ,[1,1,1,-2,0],\
80 ,[0,0,0,-7,6],\
80 ,[0,-1,0,4,-4],\
-82 ,[1,0,1,-2,0],\
-83 ,[1,1,1,1,0],\
84 ,[0,1,0,7,0],\
84 ,[0,-1,0,-1,-2],\
85 ,[1,1,0,-8,-13],\
-88 ,[0,0,0,-4,4],\
-89 ,[1,1,1,-1,0],\
89 ,[1,1,0,4,5],\
90 ,[1,-1,0,6,0],\
90 ,[1,-1,1,-8,11],\
90 ,[1,-1,1,13,-61],\
-91 ,[0,0,1,1,0],\
-91 ,[0,1,1,-7,5],\
92 ,[0,1,0,2,1],\
-92 ,[0,0,0,-1,1],\
94 ,[1,-1,1,0,-1],\
96 ,[0,1,0,-2,0],\
96 ,[0,-1,0,-2,0],\
98 ,[1,1,0,-25,-111],\
-99 ,[1,-1,1,-2,0],\
99 ,[1,-1,0,-15,8],\
99 ,[1,-1,1,-59,186],\
99 ,[0,0,1,-3,-5]];
```

Appendix C

Maple calculations for E40

The following two pages show a Maple session which expands on the analysis of the example in chapter four. The creation of the high genus curve is shown in full generality and the specialization to $E40$ is made to illustrate the factors of the discriminant.

Maple text to show that only a finite number of values a1, a2... can belong to the same cyclic cubic extension.
The strategy is to show that the hypothesis that two such values a1,a2 generate the same extension give rise to an algebraic variety whose specialization results in a high genus curve which can have only a finite number of points by Faltings' theorem.

```
> restart;
```

Suppose that the elliptic curve E:y^2=x^3+Ax+B has a point (x1,a1+bx) in a cyclic cubic extension K/Q generated by x1.

```
> f:=x^3+A*x+B-a1^2;
```

$$f := x^3 + A\,x + B - a1^2$$

We will compute the sums of the first three powers of the roots of f(x;a1,b).

```
> sum(k,'k'=RootOf(f,x));
```

$$0$$

```
> sum(k^2,'k'=RootOf(f,x));
```

$$-2\,A$$

```
> sum(k^3,'k'=RootOf(f,x));
```

$$-3\,B + 3\,a1^2$$

Suppose further that the (x2,a2+bx2) is also a point on E/K. Then x2=p+qx1+rx1^2 for some p,q,r in Q.
Developing the same sums of powers for the roots of f(x;a2,b) gives polynomial relations g1=0, g2=0,g3=0 as follows:

```
> g1:=sum(p+q*k+r*k^2,'k'=RootOf(f,x));
```

$$g1 := 3\,p - 2\,r\,A$$

```
> g2:=sum((p+q*k+r*k^2)^2,'k'=RootOf(f,x))+2*A;
```

$$g2 := 3\,p^2 - 4\,A\,p\,r - 2\,A\,q^2 - 6\,q\,r\,B + 6\,q\,r\,a1^2 + 2\,r^2\,A^2 + 2\,A$$

```
> g3:=sum((p+q*k+r*k^2)^3,'k'=RootOf(f,x))+3*B-3*a2^2;
```

$$g3 := 3\,p^3 - 6\,A\,p^2\,r - 6\,A\,p\,q^2 - 18\,p\,q\,r\,B + 18\,p\,q\,r\,a1^2 - 3\,q^3\,B + 3\,q^3\,a1^2 + 6\,A^2\,p\,r^2$$
$$+ 6\,A^2\,q^2\,r + 15\,q\,r^2\,A\,B - 15\,q\,r^2\,A\,a1^2 - 2\,r^3\,A^3 + 3\,r^3\,B^2 - 6\,r^3\,B\,a1^2 + 3\,r^3\,a1^4 + 3\,B - 3\,a2^2$$

g1 is linear in p,q,r so we use it to eliminate p from g2 and g3 giving h2 and h3.

```
> h2:=resultant(g1,g2,p);
```

$$h2 := -18\,A\,q^2 - 54\,q\,r\,B + 54\,q\,r\,a1^2 + 6\,r^2\,A^2 + 18\,A$$

```
> h3:=resultant(g1,g3,p);
```

$$h3 := -81\,q^3\,B + 81\,q^3\,a1^2 + 54\,A^2\,q^2\,r + 81\,q\,r^2\,A\,B - 81\,q\,r^2\,A\,a1^2 + 6\,r^3\,A^3 + 81\,r^3\,B^2$$
$$- 162\,r^3\,B\,a1^2 + 81\,r^3\,a1^4 + 81\,B - 81\,a2^2$$

A further elimination between h2 and h3 eliminates q leaving h(a2, r; a1 ,b)=0 as a curve in a2, r. This curve has degree 4 in a2 and degree 6 in r.

```
> h:=resultant(h2,h3,q):
> degree(h,a2);
```

$$4$$

```
> degree(h,r);
```

6

We will use the algebraic curves package of Maple to compute the genus of specializations of this curve.

```
> with(algcurves):
> genus(h,a2,r);
```

3

The curve E40 with A=-7, B=-6 has been analysed in detail in chapter four.

```
> genus(subs(A=-7,B=-6,h),a2,r);
```

3

```
> hd:=factors(discrim(h,r));
```

$$hd := \left[1385202198822188619124601248237855267264234094271631636425142945381737124\backslash \right.$$

$$\left. 295530964714520576, \left[\left[\frac{4}{27} A^3 + a2^4 + a1^4 - 2\,a1^2 B + 2\,B^2 - 2\,a2^2 B, 2 \right], \left[\frac{4}{27} A^3 + a1^4 - 2\,a1^2 B + B^2, 15 \right], [A, 6], [a1^2 - B, 6], \left[B^2 - 2\,a2^2 B + \frac{4}{27} A^3 + a2^4, 3 \right] \right] \right]$$

```
> ifactor(1385202198822188619124601248237855267264234094271631636425
  142945381737124295530964714520576);
```

$$(2)^{30}\ (3)^{170}$$

```
> hd1:=27*hd[2,1,1];
```

$$hd1 := 4\,A^3 + 27\,a2^4 + 27\,a1^4 - 54\,a1^2 B + 54\,B^2 - 54\,a2^2 B$$

```
> hd2:=27*hd[2,2,1];
```

$$hd2 := 4\,A^3 + 27\,a1^4 - 54\,a1^2 B + 27\,B^2$$

```
> hd3:=hd[2,3,1];
```

$$hd3 := A$$

```
> hd4:=hd[2,4,1];
```

$$hd4 := a1^2 - B$$

```
> hd5:=27*hd[2,5,1];
```

$$hd5 := 27\,B^2 - 54\,a2^2 B + 4\,A^3 + 27\,a2^4$$

```
> genus(hd1,a1,a2);
```

3

```
>
```