Modular symbols and the (equivariant) conjecture of Birch and Swinnerton-Dyer

chris wuthrich

8th July 2011

1 Introduction

These is the draft for my lecture notes for the Birch and Swinnerton-Dyer summer school in Alghero 2011. A part of this was presented in a slightly different order in Sardinia. I intend to add a bit more at a later stage, hopefully.

The main aim of the lectures is to understand the correct statement of an equivariant version of the Birch and Swinnerton-Dyer conjecture in the setting where $E/\mathbb{Q}$ is an elliptic curve and $K/\mathbb{Q}$ is an abelian extension. This equivariant conjecture should say something about the $\mathrm{Gal}(K/\mathbb{Q})$-structure of various arithmetic objects like the Tate-Shafarevich group. On the analytic side, we are considering the twisted L-functions $L(E,\chi,s)$ at $s=1$.

First, we will look at modular symbols and Stickelberger elements. Analytic in nature, they link well to twisted L-function and can be used to prove an important result for the Birch and Swinnerton-Dyer conjecture, namely that the quotient of probably transcendental numbers $L(E/\mathbb{Q},1)/\Omega_+$ is always a rational number. We prove then the generalisation of this to abelian fields.

I am grateful to Masato Kurihara and Werner Bley for discussions about the recent results of them presented partly in these notes. I have to thank Gianluigi Sechi and Alma Cardi for the organisation of this wonderful summer school, Tim and Vlad Dokchitser for their nice lectures and the students for improving the lectures a lot by asking interesting questions and pointing out errors. Of course, I am still interested in hearing about further improvements to these notes.

2 Setting

Throughout this notes E will be an elliptic curve over $\mathbb{Q}$. We can find a global minimal Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

with $a_i \in \mathbb{Z}$ and a_1, a_2, and a_3 in $\{-1,0,1\}$. In examples we will just give the label of the curve in Cremona's tables [12].

We will be interested in an abelian extension $K/\mathbb{Q}$ of degree d, discriminant Δ_K and Galois group G. By the theorem of Kronecker-Weber, K is contained in a cyclotomic field $\mathbb{Q}(\zeta_m)$, where ζ_m denotes a primitive m-th root of unity. The minimal m is called the

conductor of K. Given an integer a coprime to m, we write $\sigma_a \in G$ for the image of a under the composition

$$\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \xrightarrow{\cong} \mathrm{Gal}\big(\mathbb{Q}(\zeta_m)/\mathbb{Q}\big) \twoheadrightarrow G$$

Any character $\chi\colon G \to \mathbb{C}^\times$ can be viewed as a Dirichlet character $\chi\colon \mathbb{Z} \to \mathbb{C}$ of conductor dividing m by letting $\chi(a) = \chi(\sigma_a)$ when a and m are coprime and $\chi(a) = 0$ otherwise.

We write d_- for the number of complex places in K, which is either 0 or $\frac{d}{2}$, and write $d_+ = d - d_-$.

Where needed, and we will state whenever we use them, we will assume the hypotheses

(Hyp 1). No place of additive reduction ramifies in K.

(Hyp 2). The abelian field K is totally real.

(Hyp 3). The degree d is coprime to m.

The most important hypothesis will be the first. Without it things could become more complicated. See later the example in section 12.4.

The other two are mainly there because I am lazy. If K has a complex place, we have to consider $+$ and $-$ modular symbols, but it should not make any difference. When d has a common factor with m, the formulae change slightly and sometimes they are asked as exercises.

The last hypothesis (Hyp 3) implies that m is square-free: Indeed, if ℓ^2 divides m, then K is a subextension of $\mathbb{Q}(\zeta_{\ell^2 m'})$ but not of $\mathbb{Q}(\zeta_{\ell m'})$, so the degree of K must be divisible by ℓ. Conversely, if d is odd and m is square-free, then d is coprime to m. Because if ℓ is a prime dividing both m and d, then it also divides $\varphi(m)$, which could only happen if ℓ is 2.

So the last hypothesis says that we are not doing Iwasawa theory, where one wants the conductor of the field to be a power of a prime and the degree to be a power of the same prime.

3 Periods

We define first the periods in general and specialise afterwards to our situation. Let E be an elliptic curve over a number field F. Let ω be an invariant differential on E. For a complex place v of F, we define the period to be

$$\Omega_v = \Big|2\int_{E(F_v)} \bar{\omega} \wedge \omega\Big|$$

If we choose a group homomorphism $\pi\colon \mathbb{C} \to E(F_v)$ such $\pi^*(\omega) = dz$ then this period is equal to 4 times the area of a fundamental parallelogram in the kernel of π. If v instead is a real period, then we define the period to be

$$\Omega_v = \Big|\int_{E(F_v)} \omega\Big|.$$

We now pass to our situation. So E is defined over $\mathbb{Q}$ and we have chosen a fixed global minimal Weierstrass equation (2). Write

$$\omega = \frac{dx}{2y + a_1 x + a_3}$$

for the Néron differential[1].

Consider the homology $H_1(E(\mathbb{C}), \mathbb{Z})$ defined to be the free group generated by loops in $E(\mathbb{C})$ based at O modulo contractible loops. Since $E(\mathbb{C})$ is a torus, this is a free $\mathbb{Z}$-module of rank 2. Complex conjugation acts on the homology group non-trivially, but with exactly one fixed loop, namely the connected component $E^0(\mathbb{R})$ of $E(\mathbb{R})$ containing O. Hence the eigenvalues of this action must be $+1$ and -1. Let γ_+ and γ_- be generators of the corresponding eigenspaces. We define the canonical periods by

$$\Omega_+ = \int_{\gamma_+} \omega \qquad \text{and} \qquad \Omega_- = \int_{\gamma_-} \omega.$$

Furthermore, we can fix the generators $\gamma_\pm$ in such a way as to assure that Ω_+ is a positive real and Ω_- is a positive real multiple of i. The period map

$$\begin{aligned} H_1(E(\mathbb{C}), \mathbb{Z}) &\longrightarrow \mathbb{C} \\ \gamma &\longmapsto \textstyle\int_\gamma \omega \end{aligned}$$

maps the homology to a lattice in $\mathbb{C}$, which we will call it the Néron lattice Λ of E. Of course $E(\mathbb{C})$ con now be identified with $\mathbb{C}/\Lambda$ and ω with dz. By construction $\mathbb{Z}\Omega_+ \oplus \mathbb{Z}\Omega_-$ is contained in Λ, but it does not need to be equal to it.

Exercise 1. Prove that $\mathbb{Z}\Omega_+ \oplus \mathbb{Z}\Omega_-$ has index 1 or 2 depending on the number of connected components of $E(\mathbb{R})$.

We will write c_∞ for the number of components of $E(\mathbb{R})$, which is 1 if the discriminant of the elliptic curve is negative and 2 otherwise.

Exercise 2. Express the real or complex period for an infinite place v in an number field K in terms of the canonical periods and c_∞.

4 Modularity

Nothing is known so far about the Birch and Swinnerton-Dyer conjecture without modularity. Rather than describing the full power of modularity, we will only gather here the results that we will need in the sequel.

Let N be the conductor of E. The modular curve $X_0(N)$ is an projective smooth curve defined over $\mathbb{Q}$. See [35] and [16] for good explanations of modular curves. Its complex points can be described using the completed upper half plane $\mathcal{H}^*$, which is the set $\{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\} \cup \mathbb{P}^1(\mathbb{Q})$, as the quotient space

$$X_0(N)(\mathbb{C}) = \Gamma_0(N) \backslash \mathcal{H}$$

[1]The name comes from the fact that it is a generator of the $\mathbb{Z}$-module $H^1(\mathcal{E}, \Omega_{\mathcal{E}/\mathbb{Z}})$ where $\mathcal{E}$ is the Néron model of E.

with $\Gamma_0(N)$ being the congruence subgroup of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ having c divisible by N. As usual we note $q = e^{2\pi i \tau}$.

The image of $\mathbb{P}^1(\mathbb{Q})$ in $X_0(N)(\mathbb{C})$ is the finite set of cusps.

Theorem 1 (...-Taylor-Wiles [38, 40, 6]). • *There exists a non-constant morphism $\varphi\colon X_0(N) \to E$ of algebraic curves defined over $\mathbb{Q}$ sending ∞ to O.*

- *There is a constant $c \in \mathbb{Z}$, called the Manin constant, such that $\varphi^*(\omega) = c \cdot \omega_X$ for the differential form on $X_0(N)$*

$$\omega_X = \sum_{n \geqslant 1} a_n q^n \frac{dq}{q} = 2\pi i \sum_{n \geqslant 1} a_n e^{2\pi i \tau n} d\tau \tag{1}$$

  where a_n are the coefficients of the L-series.

- *For all characters $\chi \in \hat{G}$ the twisted L-function $L(E, \chi, s) = \sum_{n \geqslant 1} \frac{\chi(n) a_n}{n^s}$ admits an analytic continuation on the whole of the complex plane.*

Among all the possible modular parametrisation φ, we will always choose one of minimal degree. It is then defined up to sign. By imposing that $c > 0$, we can even fix it uniquely. The Manin constant is conjectured to be 1 for at least one curve in each isogeny class. For the strong Weil curve, it is known that the odd prime divisors of its Manin constant are all primes of additive reduction. This is not always the case[2]: The curve 11a3 has Manin constant $c = 5$. For more on the Manin constant, please see [1].

The map φ can be understood explicitly on the complex points as the following diagram commutes:

$$\begin{array}{ccc} \mathcal{H} & \twoheadrightarrow & X_0(N)(\mathbb{C}) \\ & \searrow & \downarrow \varphi \\ & & \mathbb{C}/\Lambda \cong E(\mathbb{C}) \end{array}$$

where the slanted arrow on the left is the map obtained by choosing any path from ∞ to τ and to integrate $c \cdot \omega_X$ against it, which yields a complex number only well-defined up to elements in Λ.

5 Modular symbols

The main reference for this section is [31, Sections I.1-I.8]. For any rational number r, we put

$$\lambda(r) = \int_\infty^r \omega_X \in \mathbb{C}. \tag{2}$$

More precisely, let $\{\infty, r\}$ be the path on $X_0(N)$ which is the image of the ray $\{r + it \,|\, t \geqslant 0\}$. Then $\lambda(r) = \int_{\{\infty, r\}} \omega_X$. If for instance r is $\Gamma_0(N)$-equivalent to ∞, then $\{\infty, r\}$ is a loop on $X_0(N)$ based at ∞. In general, we view $\{\infty, r\}$ as an element in $H_1(X_0(N)(\mathbb{C}), \mathbb{Z}; \{\text{cusps}\})$, the group of homotopy classes of paths between cusps on $X_0(N)(\mathbb{C})$. [3] [[3]]

[2] But it should only happen when the X_1-optimal curve is different from the strong Weil curve.

[3] [[Todo: include picture]]

The integral evaluates formally to

$$\lambda(r) = 2\pi i \sum_{n\geqslant 1} a_n \int_\infty^r e^{2\pi i \tau n} d\tau = \sum_{n\geqslant 1} \frac{a_n}{n} e^{2\pi i\, nr}$$

though we should seriously worry about the convergence of this last sum; it certainly does not converge absolutely, but it has good chances of converging conditionally. Of course, this is not the way to compute it numerically. See instead [12], [23] for this.

Proposition 2. *Let p be a prime of good reduction. Then*

$$a_p \cdot \lambda(r) = \lambda(pr) + \sum_{a=0}^{p-1} \lambda\Big(\frac{a+r}{p}\Big) \tag{3}$$

for all $r \in \mathbb{Q}$.

Exercise 3.

- Show that $a_{pn} = a_p \cdot a_n$ if n and p are coprime and $a_{pn} = a_p \cdot a_n - p a_{n/p}$ otherwise.
- Use this and the above formula to prove the proposition 2 (disregarding all questions about convergence).
- What happens if p is a prime of bad reduction with the above formula ?

Theorem 3 (Manin [28], Drinfel'd [19])**.** *There is an integer $t \geqslant 1$ such that $t \cdot \lambda(r) \in \Lambda$ for all $r \in \mathbb{Q}$.*

Here is a little lemma which is helpful to know when two rational numbers give the same cusp on $X_0(N)$.

Lemma 4 (Proposition 2.2.3 in [12])**.** *Let $r = \frac{u}{v}$ and $r' = \frac{u'}{v'}$ be two reduced fractions. Then r is $\Gamma_0(N)$-equivalent to r' if and only if $sv' \equiv s'v \pmod{\gcd(vv', N)}$ where s is an inverse of u modulo v and s' is an inverse of u' modulo v'.*

Proof. We use the Bezout identity to write $su - tv = 1$ and $s'u' - t'v' = 1$ for integers s, s', t, and t'. Then the element $\gamma = \left(\begin{smallmatrix} u & t \\ v & s \end{smallmatrix}\right)$ and $\gamma' = \left(\begin{smallmatrix} u' & t' \\ v' & s' \end{smallmatrix}\right)$ are elements of $\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma(\infty) = r$ and $\gamma'(\infty) = r'$. The stabiliser of ∞ in $\mathrm{SL}_2(\mathbb{Z})$ is given by all matrices of the form $\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right)$. Hence the general element in $\mathrm{SL}_2(\mathbb{Z})$ sending r to r' is $\gamma' \cdot \left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \cdot \gamma^{-1}$ for some x in $\mathbb{Z}$. So r is equivalent to r' if and only if we can find an x such that the lower left entry is divisible by N. This is equivalent to finding an x such that $sv' - s'v - vv'x \equiv 0 \pmod{N}$. □

Proof of theorem 3. Let $r = \frac{u}{v}$ be a rational number written as a reduced fraction. By Dirichlet, there exists a prime[4] $p \equiv 1 \pmod{N}$. With the above lemma, we can check that pr and r are $\Gamma_0(N)$-equivalent. Also for all a, the cusps r and $\frac{a+r}{p}$ are equal in $X_0(N)$. Now equation (3), gives

$$\big(p + 1 - a_p\big)\lambda(r) = \Big[\lambda(r) - \lambda(pr)\Big] + \sum_{a=0}^{p-1} \Big[\lambda(r) - \lambda\big(\frac{a+r}{p}\big)\Big]$$

[4] Often one could take a smaller modulus than N.

and the expressions in [ ] can be written as integrals of ω_X along closed paths $\{r, r'\}$. Since

$$\int_{\{r,r'\}} \omega_X = \frac{1}{c} \int_{\varphi\{r,r'\}} \omega,$$

these values lies in $\frac{1}{c}\Lambda$. So we can take $t = c(p+1-a_p)$. By definition of a_p, we have that $p+1-a_p$ is the number of points on the reduction of E at p. Since $p \equiv 1 \pmod N$ this reduction is good and hence $t > 0$. □

Exercise 4. Fill in the verification of the $\Gamma_0(N)$-equivalence of the said cusps.

Corollary 5. *For any cusp r, the image $\varphi(r) \in E(\mathbb{C})$ is always a torsion point.*

Later we will mainly be interested in the modular symbols

$$[r] = \frac{\mathrm{Re}(\lambda(r))}{\Omega_+},$$

which by the above is a rational number for all $r \in \mathbb{Q}$. In fact theorem 3 shows that the denominator of this rational number $[r]$ is small. More precisely it will be a divisor of $2t$, the 2 coming in only in the case that the lattice is not rectangular.

Example. As a first example, we present here a few modular symbols for the curve

$$y^2 + y = x^3 - x^2 + 79\,x - 1123$$

labelled 435b1 in Cremona's tables. For instance, we have $[0] = 1$. The $[\frac{a}{m}]$ for small denominators are listed in the table 1. For instance $[\frac{3}{7}] = -\frac{5}{2}$. The only reason why the modular symbols for this curve are not integral is because the lattice is not rectangular. In particular $[r] \in \frac{1}{2}\mathbb{Z}$ for all r.

The integer t given in the proof of the theorem is nowhere near being as small as possible. To obtain better results one should take the Galois action on the cusp on $X_0(N)$ into account. For instance the cusp 0 is always defined over $\mathbb{Q}$, hence $\varphi(0)$ is a torsion point in $E(\mathbb{Q})$.

Proposition 6. *To each elliptic curve, there exists an isogenous curve such that $t \in \mathbb{Z}$ can be take coprime to any odd prime of semistable reduction.*

The proof is unpublished work. Typically these curves will not have p-torsion points defined over K, except maybe for $p = 2$ or primes of additive reduction.

Exercise (*) 5. What is the exact power of 2 and of additive primes that can appear at worst in the denominators of $[r]$?

Example. Let E be the curve 324a1 whose Manin constant is 1. Then $[\frac{1}{9}] = \frac{1}{6}$. Despite $E(\mathbb{Q}) = {}^{\mathbb{Z}}/_{3\mathbb{Z}}$ and E having a rectangular Néron lattice.

Table 1: The modular symbols $\left[\frac{a}{m}\right]$ for 435b1

m	$a=1$	2	3	4	5	6	7	8	9	10	11	12	13	14
2	-2													
3	-1	-1												
4	$-\frac{1}{2}$		$-\frac{1}{2}$											
5	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$	$-\frac{1}{2}$										
6	2				2									
7	3	$-\frac{5}{2}$	$-\frac{5}{2}$	$-\frac{5}{2}$	$-\frac{5}{2}$	3								
8	1		1		1		1							
9	3	-1		-1	-1		-1	3						
10	1		1				1		1					
11	3	3	$-\frac{7}{2}$	$-\frac{3}{2}$	$-\frac{3}{2}$	$-\frac{3}{2}$	$-\frac{3}{2}$	$-\frac{7}{2}$	3	3				
12	4				-3		-3				4			
13	3	3	$-\frac{1}{2}$	$-\frac{3}{2}$	$-\frac{1}{2}$	$-\frac{3}{2}$	$-\frac{3}{2}$	$-\frac{1}{2}$	$-\frac{3}{2}$	$-\frac{1}{2}$	3	3		
14	5		$-\frac{1}{2}$		$-\frac{1}{2}$				$-\frac{1}{2}$		$-\frac{1}{2}$		5	
15	3	$\frac{1}{2}$		-2			$\frac{1}{2}$	$\frac{1}{2}$			-2		$\frac{1}{2}$	3

6 Stickelberger elements

Let now K be an abelian extension of $\mathbb{Q}$. The Galois group will be denoted by G, the conductor by m. In this section, we do not need to assume (Hyp 2) that d is odd, but one should be aware that the Stickelberger elements as defined below only really see the elliptic curve over the maximal real subextension of K.

As a short hand, we will write $\sum_{a \bmod m^\times}$ for the sum over all invertible residue classes modulo m. Following Mazur-Tate [30], we define the Stickelberger elements

$$\Theta = \Theta_{E/K} = \sum_{a \bmod m^\times} \left[\frac{a}{m}\right] \sigma_a \in \mathbb{Q}[G] \tag{4}$$

where σ_a is the image of a under $\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \to G$.

Lemma 7. *Let L/K be an extension such that $L/\mathbb{Q}$ is an abelian extension of conductor $m\cdot\ell$. Suppose that ℓ and m are coprime. Write $N_{L/K}$ for the natural map $\mathbb{Q}[\mathrm{Gal}(L/\mathbb{Q})] \to \mathbb{Q}[\mathrm{Gal}(K/\mathbb{Q})]$. Then*

$$N_{L/K}(\Theta_{E/L}) = -\sigma_\ell\left(1 - a_\ell \sigma_\ell^{-1} + \delta_N(\ell)\cdot\sigma_\ell^{-2}\right)\cdot\Theta_{E/K}, \tag{5}$$

where $\delta_N(\ell)$ is equal to 0 if ℓ is coprime to N and equal to 1 otherwise.

Proof. By the Chinese remainder theorem, each invertible a modulo $m\ell$ can be written uniquely as $a = bm + c\ell$ where b runs through invertibles modulo ℓ and c runs through invertibles modulo m. We get

$$\begin{aligned} N_{L/K}(\Theta_{E/L}) &= \sum_{a \bmod (m\ell)^\times} \left[\frac{a}{m\ell}\right]\sigma_a = \sum_{c \bmod m^\times}\ \sum_{b \bmod \ell^\times} \left[\frac{b + \frac{c\ell}{m}}{\ell}\right]\sigma_{c\ell} \\ &= \sum_{c \bmod m^\times} \left(a_\ell\left[\frac{c\ell}{m}\right] - \delta_N(\ell)\left[\frac{c\ell^2}{m}\right] - \left[\frac{c}{m}\right]\right)\cdot\sigma_c\cdot\sigma_\ell \end{aligned}$$

where we used the relation (3) with $r = \frac{c\ell}{m}$. Now as c runs through invertibles modulo m, so do $e = c\ell$ and $e = c\ell^2$, hence

$$\begin{aligned} N_{L/K}(\Theta_{E/L}) &= a_\ell \sum_{e \bmod m^\times} \left[\frac{e}{m}\right] \sigma_e \sigma_\ell^{-1} \sigma_\ell - \delta_N(\ell) \sum_{e \bmod m^\times} \left[\frac{e}{m}\right] \sigma_e \sigma_\ell^{-2} \sigma_\ell - \sum_{c \bmod m^\times} \left[\frac{c}{m}\right] \sigma_c \sigma_\ell \\ &= a_\ell \Theta_{E/K} - \delta_N(\ell) \sigma_\ell^{-1} \Theta_{E/K} - \sigma_\ell \Theta_{E/K}. \end{aligned}$$

□

Corollary 8. *Let K be an abelian field of conductor m satisfying (Hyp 3). Then*

$$N_{K/\mathbb{Q}}(\Theta_{E/K}) = \mu(m) \cdot [0] \cdot \prod_{\ell \mid m} \big(1 - a_\ell + \delta_N(\ell)\big).$$

Proof. Use the previous lemma inductively on the prime factors of the squarefree integer m. Finally, we have $\Theta_{E/\mathbb{Q}} = [0]$ and all σ_a are trivial in $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}/\mathbb{Q})] = \mathbb{Q}$. □

Exercise 6. What happens if ℓ divides m in the previous lemma 7 ?

Example. If we return to the example at the end of the last section, namely the curve 435b1. Now we choose $m = 7$ and $d = 3$. So the abelian field is $\mathbb{Q}(\mu_7)^+$, the cubic cyclic extension unramified outside 7. It can also be given by the roots of the polynomial $x^3 + x^2 - 2\,x - 1$. From the list of modular symbols in table 1, we get

$$\Theta = 3\sigma_1 - \tfrac{5}{2}\sigma_2 - \tfrac{5}{2}\sigma_3 - \tfrac{5}{2}\sigma_4 - \tfrac{5}{2}\sigma_5 + 3\sigma_6 = 6 - 5 \cdot g - 5 \cdot g^2$$

where we chose $g = \sigma_3$ as a generator for $G = \mathrm{Gal}(K/\mathbb{Q})$ since 3 is a primitive element modulo 7. The norm of Θ is $N(\Theta) = 6 - 5 - 5 = -4$ and $[0] = 1$, while $a_7 = -2$.

Exercise 7. Do a similar computation for $m = 11$ and $d = 5$. Check if a_{11} is indeed 1.

7 Winding number

For each finite place v in $\mathbb{Q}$, we write c_v for the Tamagawa number of E at v. The Tate-Shafarevich group is denoted by $Ш(E/\mathbb{Q})$. Both are defined in Vlad's lecture [18]. Over $\mathbb{Q}$, we have the theorem originally due to Kolyvagin [26], but later reproved using modular symbols.

Theorem 9 (..., Kato [24], Urban-Skinner).

- *If $L(E/\mathbb{Q}, 1) \neq 0$, then both $E(\mathbb{Q})$ and $Ш(E/\mathbb{Q})$ are finite.*
- *If $L(E/\mathbb{Q}, 1) = 0$ then either $E(\mathbb{Q})$ or $Ш(E/\mathbb{Q})$ is infinite.*[5]

Set

$$b_{\mathbb{Q}} = \frac{\prod_v c_v \cdot \#Ш(E/\mathbb{Q})}{\big(\#E(\mathbb{Q})_{\mathrm{tors}}\big)^2}$$

whenever $Ш(E/\mathbb{Q})$ is finite. The product runs over all places including the infinite place. Here is the rank 0 part of the Birch and Swinnerton-Dyer conjecture over $\mathbb{Q}$:

[5] More precisely, the p-primary Selmer group is infinite for all primes p of good reduction.

Conjecture 1. If $L(E/\mathbb{Q},1)\neq 0$, then $\frac{L(E/\mathbb{Q},1)}{\Omega_+}=b_{\mathbb{Q}}$.

In fact, the method of Kolyvagin and the results of Kato allow one to prove quite a bit about the exact formula involving $b_{\mathbb{Q}}$. See [37, Section 8] or [32] for instance. The conjecture would imply the surprising fact that the left hand side, a fraction of two real numbers, is in fact a rational number. We proceed now to prove this.

Theorem 10. $\lambda(0)=L(E/\mathbb{Q},1)$.

Proof. (Again, we give a proof in which we neglect the convergence question. For a correct proof, see [31].) On the one hand, we have

$$L(E/\mathbb{Q},1)=\sum_{n\geqslant 1}\frac{a_n}{n^s}\Big|_{s=1}=\sum_{n\geqslant 1}\frac{a_n}{n}$$

and on the other hand we had computed

$$\lambda(0)=\sum_{n\geqslant 1}\frac{a_n}{n}e^{2\pi i n 0}.$$ □

The definition of $L(E/\mathbb{Q},s)$ shows that $L(E,1)$ and $[0]$ are real numbers. By theorem 3, we have that $t\cdot\lambda(0)\in\Lambda\cap\mathbb{R}=\mathbb{Z}\cdot\Omega_+$.

Corollary 11. *The value of* $[0]=\frac{L(E/\mathbb{Q},1)}{\Omega_+}$ *is a rational number.*

If $t=1$, then the the image of $\{\infty,0\}$ is a loop on $E^0(\mathbb{R})\cong\mathbb{S}^1$. Therefore $\lambda(0)/\Omega_+\in\mathbb{Z}$ is just the number of windings that this loop makes. Hence it is called the winding number. See [29].[6] [[6]]

Example. In our example 435b1, we have $[0]=1$. Since the Tamagawa numbers and the torsion order are trivial, the BSD conjecture is equivalent to $Ш(E/\mathbb{Q})$ being trivial. This can be verified without much difficulty.

The discussion of the denominator of $[0]$ before shows that if the Birch and Swinnerton-Dyer conjecture holds and the Manin constant is 1 then at least one of the two factors $\#E(\mathbb{Q})$ in $b_{\mathbb{Q}}$ must cancel with the numerator.

Example. For the curve 11a1, we have $[0]=\frac{1}{5}$. The order of the torsion subgroup $E(\mathbb{Q})_{\text{tors}}=\mathbb{Z}/5\mathbb{Z}$ cancels once with the Tamagawa number $c_{11}=5$. Instead for the curve 11a3, we have $[0]=\frac{1}{25}$ because the Manin constant is 5 and there is no cancellation as $\prod c_v=1$ in this case.

The curve 66b3 has $\prod_v c_v=c_\infty=2$ and $E(\mathbb{Q})=\mathbb{Z}/2\mathbb{Z}$. But the winding number is $[0]=2$; so this time the cancellation in the formula also involves the Tate-Shafarevich group. And indeed $Ш(E/\mathbb{Q})=\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}$.

[6] [[Todo: add a picture]]

8 Twists

Let χ be a character of G, so it is a Dirichlet character modulo m. Its conductor, denoted by f_χ, is a divisor of m. The character χ takes values in $\mathbb{Q}(\zeta_d)$ where ζ_d is a primitive d-th root of unity. Let

$$G(\chi) = \sum_{a \bmod m} \chi(a) \cdot e^{\frac{2\pi i a}{m}} \tag{6}$$

be the Gauss sum of χ. We use the same definition whether or not χ is primitive. Recall that, if χ is primitive, then the twisted[7] L-function is defined by

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

for s with sufficiently[8] large real part. Otherwise if χ is not primitive, we still denote by $L(E, \chi, s)$ the L-function of the corresponding primitive character. The following is a natural generalisation of theorem 10, see again [31].

Theorem 12 (Birch)**.** *Suppose χ is primitive, i.e. $f_\chi = m$. Then we have*

$$G(\chi) \cdot L(E, \bar{\chi}, 1) = \sum_{a \bmod m} \chi(a) \cdot \lambda\Big(\frac{a}{m}\Big).$$

Proof. We compute

$$\begin{aligned} \sum_{a \bmod m} \chi(a) \cdot \lambda\Big(\frac{a}{m}\Big) &= \sum_{a \bmod m} \chi(a) \sum_{n \geqslant 1} \frac{a_n}{n} \cdot e^{2\pi i a n/m} \\ &= \sum_{n \geqslant 1} \frac{a_n}{n} \cdot \sum_{a \bmod m} \chi(a) \cdot e^{2\pi i a n/m} \end{aligned}$$

If n is coprime to m, then the second sum is equal to

$$\sum_{a \bmod m} \chi(a) \cdot e^{2\pi i a n/m} = \bar{\chi}(n) \sum_{a \bmod m} \chi(an) \cdot e^{2\pi i a n/m}$$

as $\bar{\chi}(n) \cdot \chi(an) = \chi(n)^{-1} \cdot \chi(a) \cdot \chi(n) = \chi(a)$. Now an will equally well run over all classes modulo m and so the above sum is equal to $\bar{\chi}(n) \cdot G(\chi)$. If instead n is not coprime to m, then this second sum above is zero as shown in the following exercise. □

Exercise 8. Let χ be a primitive character and let n have a common divisor with m. Show that

$$\sum_{a \bmod m} \chi(a) \cdot e^{2\pi i a n/m} = 0$$

and hence it is still equal to $\bar{\chi}(n) \cdot G(\chi)$.

[7] This is slightly off the more motivic definition of the twisted L-function. First of all, one might argue that this is the definition for $L(E, \bar{\chi}, s)$ instead. But note there is also a small difference: If there is a place v of additive reduction that ramifies, i.e. when (Hyp 1) is not satisfied, and if the reduction type changes in this extension, then the local factor at v is trivial with our definition, while the characteristic polynomial of Frobenius on $(V_p E^* \otimes \bar{\chi})^{I_v}$ might be non-trivial.

[8] for absolute convergence we want $\mathrm{Re}(s) > \frac{3}{2}$.

From now on we suppose (Hyp 2) that K is totally real. We see now that $\chi(-a) = \chi(-1)\cdot\chi(a) = \chi(a)$. From the way the complex conjugation[9] acts on $X_0(N)$, we have that $\lambda(-r) = \overline{\lambda(r)}$.

We deduce

$$\begin{aligned}\sum_{a \bmod m} \chi(a)\cdot\lambda\Big(\frac{a}{m}\Big) &= \frac{1}{2}\Big(\sum_{a \bmod m} \chi(a)\cdot\lambda\Big(\frac{a}{m}\Big) + \sum_{a \bmod m} \chi(-a)\cdot\lambda\Big(-\frac{a}{m}\Big)\Big)\\ &= \frac{1}{2}\sum_{a \bmod m}\Big(\chi(a)\cdot\lambda\Big(\frac{a}{m}\Big) + \chi(a)\cdot\overline{\lambda\Big(\frac{a}{m}\Big)}\Big)\\ &= \sum_{a \bmod m}\chi(a)\cdot\mathrm{Re}\Big(\lambda\Big(\frac{a}{m}\Big)\Big)\end{aligned}$$

Note that this sum belongs to $\mathbb{Q}(\zeta_d)\otimes\big(\Lambda\cap\mathbb{R}\big) = \mathbb{Q}(\zeta)\cdot\Omega_+$. By our definition of $[r]$ and Θ, we conclude the following.

Corollary 13. *Assuming (Hyp 2), a primitive character χ of G sends Θ to*

$$\chi(\Theta) = \sum_{a \bmod m}\chi(a)\cdot\Big[\frac{a}{m}\Big] = \frac{G(\chi)L(E,\bar\chi,1)}{\Omega_+}, \tag{7}$$

which is an algebraic number in $\mathbb{Q}(\zeta_d)$.

If the character is not primitive, we can still compute these values.[10]

Proposition 14. *Assume (Hyp 3). Let $\tilde\chi$ be a Dirichlet character modulo m of conductor f_χ. Write χ for the corresponding primitive character modulo f_χ. Let Θ_f be the Stickelberger element for the subextension of K which is fixed by the kernel of $\tilde\chi$. Then*

$$\tilde\chi(\Theta) = \chi(\Theta_f)\cdot\prod_{\ell\mid\frac{m}{f}}(-\chi(\ell))\Big(1 - a_\ell\cdot\bar\chi(\ell) + \delta_N(\ell)\cdot\bar\chi(\ell)^2\Big)$$

$$G(\tilde\chi) = G(\chi)\cdot\prod_{\ell\mid\frac{m}{f}}(-\chi(\ell)) = G(\chi)\cdot\chi\Big(\frac{m}{f}\Big)\cdot\mu\Big(\frac{m}{f}\Big)$$

---

[9] This follows from the description of the modular parametrisation as a map $\phi\colon\mathcal{H}\to\mathbb{C}/\Lambda$:

$$\phi(\tau) = c\int_\infty^\tau\omega_X = c\sum_{n\geqslant1}\frac{a_n}{n}e^{2\pi i n\tau}.$$

Now $\overline{\phi(\tau)} = \phi(-\bar\tau)$ because $\overline{e^z} = e^{-\bar z}$.

[10] Provided m is square-free, Darmon in [13] uses instead the slightly modified modular symbols

$$\Big[\frac{a}{m}\Big]^* = \sum_{d\mid m}\mu\Big(\frac{m}{d}\Big)\cdot\Big[\frac{ak}{m}\Big],$$

where k is the inverse of m/d modulo d. With these, the formulae become less sensitive to the conductor. For instance,

$$\chi(\Theta^*) = \frac{m\cdot G(\chi)\cdot L(E,\bar\chi,1)}{f\cdot\Omega_+}$$

holds for all characters. This comes from the better compatibility relation (5) in which the correct Euler-system factor appears: $N(\Theta^*_{E/L}) = -\sigma_\ell(\ell - a_\ell\sigma_\ell^{-1} + \sigma_\ell^{-2})\Theta^*_{E/K}$ when $\ell\nmid N$.

Proof. The formula for $\tilde{\chi}(\Theta)$ follows from lemma 7 and the fact that $\tilde{\chi}(\Theta) = \chi(N(\Theta))$ where N is the norm down to the field which is fixed by the kernel of $\tilde{\chi}$. The formula for the Gauss sum can be computed easily. Say ℓ divides m and $f_\chi = m/\ell$. Then, using $a = b\ell + cf$ as in the proof of lemma 7, we find

$$\begin{aligned} G(\tilde{\chi}) &= \sum_{a \bmod m^\times} \tilde{\chi}(a) e^{2\pi i a/m} = \sum_{b \bmod f^\times} \sum_{c \bmod \ell^\times} e^{2\pi i (b\ell + cf)/m} \chi(b\ell) \\ &= \chi(\ell) \cdot \sum_{b \bmod f^\times} \chi(b) e^{2\pi i b/f} \cdot \sum_{c \bmod \ell^\times} e^{2\pi i c/\ell}. \end{aligned}$$

and the last sum is -1 as ℓ is a prime. Then an induction proves the formula in the proposition. □

Exercise 9. Extend this proposition to the case when (Hyp 3) does not hold.

In particular, it shows that

$$\frac{L(E, \bar{\chi}, 1) \cdot G(\chi)}{\Omega_+} \tag{8}$$

is the product of $\chi(\Theta)$ and an algebraic number in $\mathbb{Q}(\zeta_d)$ even when χ is not primitive. So this expression itself is in $\mathbb{Q}(\zeta_d)$.

Example. In our example 435b1 with the character χ sending g to ζ_3, we find

$$\frac{L(E, \bar{\chi}, 1) \cdot G(\chi)}{\Omega_+} = 6 - 5\zeta_3 - 5\zeta_3^2 = 6 - 5\zeta_3 - 5\big(-1 - \zeta_3\big) = 11.$$

Exercise 10. Find the value of $\chi(\Theta) \in \mathbb{Z}[\zeta_5]$ for χ a Dirichlet character of conductor $m = 11$ and order $d = 5$. What is its norm ?

9 Birch and Swinnerton-Dyer over K

Now let K be an abelian extension of $\mathbb{Q}$. The Birch and Swinnerton-Dyer conjecture over K links the L-series $L(E/K, s)$ to the arithmetic side. By the Artin formalism (see Tim's lectures [17]), we have the following[11]

Lemma 15 (Artin formalism)**.** *Suppose (Hyp 1), then*

$$L(E/K, s) = \prod_{\chi \in \hat{G}} L(E, \chi, s) \tag{9}$$

where χ runs over all characters of G.

We will try to split it up to make a conjecture for $L(E, \chi, 1)$. On the arithmetic side, we can split up the Mordell-Weil group as follows:

$$E(K) \otimes \mathbb{C} = \bigoplus_{\chi \in \hat{G}} \Big(E(K) \otimes \mathbb{C} \Big)^\chi$$

as $E(K) \otimes \mathbb{C}$ is a finite dimensional $\mathbb{C}$-vector space with a linear action by G on it. The following theorem was shown by Kato [24, Corollary 14.3].

[11] The condition (Hyp 1) is necessary. If a place $\ell \mid m$ is of additive reduction, then the type of reduction might change, say from additive to good reduction. In this case the local factors do not multiply together as they should as in footnote 7.

Theorem 16. *If $L(E,\chi,1)\neq 0$ then $\big(E(K)\otimes\mathbb{C}\big)^{\chi}=0$. If $L(E/K,1)\neq 0$, then $E(K)$ and $Ш(E/K)$ are finite.*

Now to the precise formula for the leading term. For each finite place w in K, we define C_w to be the product of the Tamagawa number $c_w(E/K)$ and the correction factor[12] h as follows. If the Weierstrass equation (2) is still minimal at w, then $h=1$. If instead we have to change the Weierstrass equation to a minimal equation at w in x', y' using a transformation $x'=u^3\,x$, then $h=q^{-w(u)}$ where q is the number of elements of the residue field of w. For each real place, we set $C_v=c_v$ equal to the number of connected components c_∞ of $E(\mathbb{R})$. For each complex place $C_v=c_v$ is set to $2c_\infty$.

Lemma 17. *Under the assumption of (Hyp 1), the equation is still minimal at all places of K. In particular $C_w=c_w$ for all places of K.*

Proof. Let w be a finite place of K. If w is unramified, then the equation is still minimal. Otherwise w is ramified and so by (Hyp 1), the reduction is semi-stable at w. It is clear that the equation stays minimal if the reduction is good at w. If the reduction is multiplicative, then the reduction will still be multiplicative and the equation will still be minimal, see the proof of Proposition VII.5.4.b) in [36]. □

However, the Néron model and hence the Tamagawa number might change. If d is odd, then we simply have $c_w=e_{w|v}\cdot c_v$ for all split multiplicative places that ramify, where $e_{w|v}$ is the ramification index of $w\mid v$, and $c_w=c_v$ for all other places.

Set

$$b_K=\frac{\prod_w C_w\cdot \#Ш(E/K)}{\big(\#E(K)_{\mathrm{tors}}\big)^2}$$

provided that $Ш(E/K)$ is finite. We can announce the analogous rank 0 version of the Birch and Swinnerton-Dyer conjecture.

Conjecture 2. If $L(E/K,1)\neq 0$, then

$$\frac{L(E/K,1)\cdot\sqrt{|\Delta_K|}}{\Omega_+^{d_+}\cdot|2\Omega_-|^{d_-}}=b_K.$$

Theorem 18. *Assume (Hyp 2) and (Hyp 1). The expression*

$$\frac{L(E/K,1)\cdot\sqrt{\Delta_K}}{\Omega_+^{d}}$$

is a rational number.

[12] This can also be expressed as the normalised absolute value of the quotient of the fixed Néron differential ω over $\mathbb{Q}$ and a Néron differential over K_w.

Proof. From equation (8), we know that

$$\prod_{\chi\in\hat{G}} \frac{L(E,\bar{\chi},1)\cdot G(\chi)}{\Omega_+} = \frac{L(E/K,1)}{\Omega_+^d}\prod_{\chi\in\hat{G}} G(\chi)$$

is an element of $\mathbb{Q}(\zeta_d)$. The Führerdiskriminantenproduktformel says that the product overall conductors f_χ of characters $\chi\in\hat{G}$ is equal to the discriminant of K. So

$$\Big(\prod_{\chi\in\hat{G}} G(\chi)\Big)^2 = \prod_{\chi\in\hat{G}} G(\chi)\cdot G(\bar{\chi}) = \prod_{\chi\in\hat{G}} f_\chi = \Delta_K$$

Hence $\prod_\chi G(\chi) = \pm\sqrt{\Delta_K}$. This shows that the formula in our statement is in $\mathbb{Q}(\zeta_d)$, too. Moreover the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ acts on the expression. One can check that it fixes the product: The precise formula from proposition 14 is

$$\frac{L(E/K,1)\cdot\sqrt{\Delta}}{\Omega_+^d} = \pm\prod_{\chi\in\hat{G}}\chi(\Theta)\cdot\prod_{\ell|m}\prod_{\substack{\chi\in\hat{G}\\ \ell\nmid f_\chi}}\big(1-a_\ell\bar{\chi}(\ell)+\delta_N(\ell)\bar{\chi}(\ell)^2\big)^{-1}$$

and we see that both products will run over all conjugate characters for the Galois group of $\mathbb{Q}(\zeta_d)/\mathbb{Q}$. So the right hand side is in $\mathbb{Q}$. □

Of course, this theorem holds with any of the hypotheses as long as K is abelian and E is defined over $\mathbb{Q}$. If the degree d is prime, the formula reads a bit simpler as

$$\frac{L(E/K,1)\cdot\sqrt{\Delta}}{\Omega_+^d} = [0]\cdot\prod_{\text{primitive }\chi}\chi(\Theta) = [0]\cdot N_{\mathbb{Q}(\zeta_d)/\mathbb{Q}}(\chi(\Theta))$$

where on the right hand side χ is any primitive character.

Example. Back to our example 435b1. For the L-values of E/K, we get

$$\frac{L(E/K,1)\cdot\sqrt{7^2}}{\Omega_+^3} = [0]\cdot\chi(\Theta)\cdot\overline{\chi(\Theta)} = 11^2.$$

Given that the Tamagawa numbers are still trivial (no bad place is ramified) and that there are still no torsion points defined over K (because all p-adic representations are surjectve), the Birch and Swinnerton-Dyer conjecture over K asserts that $\#Ш(E/K) = 11^2$.

Exercise 11. Compute what BSD predicts for E =435b1 over the quintic field of conductor 11.

10 Symmetry

These elements also satisfy a relation that resembles the functional equation, see [30, Section 1.6]. Let Q' be the greatest common divisor of N and m and write $N = Q\cdot Q'$. By assumption (Hyp 1), m is coprime to Q. Using the Atkin-Lehner operator w_Q one can show that $[\frac{a}{m}] = \tilde{w}_Q\cdot[\frac{a'}{m}]$ where a' is the inverse of $-aQ$ modulo m and $-\tilde{w}_Q$ is a root

number. More precisely $\tilde{w}_N$ is the global root number $w(E/\mathbb{Q})$ as defined by Vlad in [18]. Instead $\tilde{w}_Q = \tilde{w}_N \cdot \prod_{\ell | Q'} w_\ell$ where w_ℓ is the local root number, which equals -1 for split multiplicative ℓ and $+1$ for the non-split multiplicative places. As a consequence, we get

$$\Theta = \sum_{a \bmod m^\times} \left[\frac{-a}{m}\right] \sigma_a = \tilde{w}_Q \cdot \sum_{a \bmod m^\times} \left[\frac{b}{m}\right] \sigma_b$$

where b is the inverse of aQ modulo m. Thus we have $\sigma_a = \sigma_b^{-1} \cdot \sigma_Q^{-1}$, hence we get

$$= \tilde{w}_Q \cdot \sigma_Q^{-1} \sum_{b \bmod m^\times} \left[\frac{b}{m}\right] \sigma_b^{-1} = \tilde{w}_Q \cdot \sigma_Q^{-1} \cdot \Theta^*$$

where * denotes the involution on $\mathbb{Q}[G]$ induced by replacing g by g^{-1} for all g in G. We have prove the following.

Proposition 19 (Functional equation)**.** *Let χ be a character modulo m. Let $Q = \frac{N}{\gcd(N,m)}$. If (Hyp 3) holds, then*

$$\chi(\Theta) = \tilde{w}_Q \cdot \bar{\chi}(Q) \cdot \overline{\chi(\Theta)}.$$

Moreover,

$$\chi(\Theta) \in \begin{cases} \mathbb{Q}(\zeta_d)^+ \cdot \chi(Q)^{\frac{d-1}{2}} & \text{if } \tilde{w}_Q = 1 \text{ and} \\ \mathbb{Q}(\zeta_d)^+ \cdot (\zeta_d - \bar{\zeta_d}) \cdot \chi(Q)^{\frac{d-1}{2}} & \text{if } \tilde{w}_Q = -1. \end{cases}$$

Proof. We only have the justify the last statement. Note that the set of solutions in $z \in \mathbb{C}$ to $z = \tilde{w}_Q \cdot \bar{\chi}(Q) = \bar{z}$ forms a ray $\mathbb{R}_{>0} \cdot z_0$ for any chosen solution z_0. If $\tilde{w}_Q = 1$, then it is easy to check that $z_0 = \chi(Q)^k$ with $k = \frac{d-1}{2}$ is a solution; similarly for $\tilde{w}_Q = -1$, we can take $z_0 = \chi(Q)^k \cdot (\zeta_d - \bar{\zeta_d})$. □

This last consequence was noted in [15, Theorem 2.1].

Corollary 20. *If K is a cyclic cubic extension satisfying (Hyp 3), i.e. $3 \nmid m$. Let χ be one of the two non-trivial characters. Then $\chi(\Theta)$ belongs to $\chi(Q) \cdot \mathbb{Q}$ if $\tilde{w}_Q = 1$ and to $\chi(Q) \cdot \sqrt{-3} \cdot \mathbb{Q}$ otherwise.*

Example. In the example 435b1, we have $Q' = 1$, so $Q = N$ and $\tilde{w}_N = +1$ is the global root number. Since $N \equiv 1 \pmod 7$, we have $\sigma_N = 1$ and so $\Theta = \Theta^*$, which is clear as $\Theta = 6 - 5g - 5g^2$.

Exercise 12. Here is the list of some modular symbols for 11a2. Verify that the above functional equation holds for the Stickelberger element for $m = 7$, $d = 3$ and for $m = 11$ and $d = 5$.

a	0	1	2	3	4	5	6	7	8	9	10
$\left[\frac{a}{7}\right]$	1	$\frac{7}{2}$	$\frac{7}{2}$	-9	-9	$\frac{7}{2}$	$\frac{7}{2}$				
$\left[\frac{a}{11}\right]$	1	0	5	$\frac{5}{2}$	$-\frac{5}{2}$	-5	-5	$-\frac{5}{2}$	$\frac{5}{2}$	5	0

Let I be the augmentation ideal of $\mathbb{Q}[G]$, i.e. the kernel of the ring homomorphism $\mathbb{1}\colon \mathbb{Q}[G] \to \mathbb{Q}$. Then $\mathbb{1}(\Theta)$ is a multiple of $[0]$, so it should vanish if $L(E/\mathbb{Q},1)=0$. The "order of vanishing" of an element in $\mathbb{Q}[G]$ could be defined to be the highest power of I to which it belongs. In view of the change in the root number above when m is divisible by split multiplicative primes, we can not expect that the order of vanishing is equal to the rank of $E(\mathbb{Q})$. Instead we have a phenomenon of "trivial zeroes".

Conjecture 3 (Mazur-Tate [30])**.** Θ belongs to is the r'-th power of I with

$$r' = \operatorname{rank} E(\mathbb{Q}) + \#\{\ell \text{ primes of split multiplicative reduction with } \ell \mid m\}.$$

The "leading" term in $I^{r'}/I^{r'+1} \cong \mathbb{Q}$ has a Birch and Swinnerton-Dyer formula involving the p-adic heights. However, it is to note that Θ might belong to an even higher power of I. For instance, if $m=\ell$ is coprime to N and $a_\ell = 2$, then Θ will belong to I even when the rank over $\mathbb{Q}$ is zero. This is because $\mathbb{1}(\Theta) = (a_\ell - 2)\cdot[0] = 0$.

On the arithmetic side, we also have a symmetry. Let

$$Ш(E/K) \times Ш(E/K) \to \mathbb{Q}/\mathbb{Z}$$

be the Cassels-Tate pairing. It is non-degenerate if and only if $Ш(E/K)$ is finite. By construction, this is naturally G-equivariant. This implies that the "χ-part" and the "$\bar\chi$-part" of $Ш(E/K)$ are dual to each other.

Proposition 21. *If K is a cyclic cubic extension and $p \neq 3$ a prime. Assume that $Ш(E/K)[p^\infty]$ is finite. Then the $\mathbb{F}_p[G]$-module $Ш(E/K)[p]/Ш(E/\mathbb{Q})[p]$ is a direct sum of $\mathbb{F}_p[G]/\mathbb{F}_p$.*

This is obvious when $\mathbb{F}_p$ does not contain a primitive 3-rd root of unity; however, when $p \equiv 1 \pmod 3$, there are two characters $\chi, \bar\chi\colon G \to \mathbb{F}_p^\times$ and the proposition says that they appear with equal multiplicity in $Ш(E/K)[p]$.

11 The equivariant conjecture

We consider the $\mathbb{Z}[G]$-module structure of the following three groups. First of all the Tate-Shafarevich group $Ш(E/K)$. Then there is the torsion subgroup $T = E(K)_{\text{tors}}$ and its dual $T^\vee$. Finally the Tamagawa numbers C, which can be defined as follows.

Assume (Hyp 1) holds. For each finite place w, consider the finite group $\Phi_w = E(K_w)/E^0(K_w)$ where $E^0(K_w)$ is the subgroup of points with good reduction in our fixed minimal model.[13] Now for a finite place v in $\mathbb{Q}$, the group $\oplus_{w|v}\Phi_w$ has a G-action on it as Φ_w has an action by the decomposition group on it. If (Hyp 2) holds, then set $\Phi_\infty = \mathbb{Z}/2\mathbb{Z}[G]$ if $E(\mathbb{R})$ has two connected components and $\Phi_\infty = 0$ otherwise. Finally $C = \Phi_\infty \oplus \bigoplus_w \Phi_w$ is a $\mathbb{Z}[G]$-module where w runs over all finite places of K.

Let p be a prime. Rather than working with $\mathbb{Z}[G]$-modules, we will split up the task to individual p-primary parts. We will suppose that

[13] The group Φ_w is nothing but the group of connected k_w-rational components of the Néron model at w. Under our hypothesis (Hyp 1), the Néron model did not change, see lemma 17 so it has a natural G-action on it.

(Hyp 4). p is a prime which does not divide d.

Fix a *primitive* character $\chi\colon \mathbb{Z}[G] \to \mathbb{Z}[\zeta_d]$. Let $\mathfrak{p}$ be a maximal ideal of $\mathbb{Z}[\zeta_d]$ above p. Through χ, we can view $\mathfrak{p}$ also as a maximal ideal of $\mathbb{Z}[G]$.

For any finite $\mathbb{Z}[G]$-module M, we define $\mathrm{len}_{\mathfrak{p}}(M)$ to be the length of the $\mathbb{Z}[G]_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$. So $q^{\mathrm{len}_{\mathfrak{p}}(M)} = \#M_{\mathfrak{p}}$ where q is the number of elements in the residue field of $\mathbb{Z}[G]_{\mathfrak{p}}$. Of course, we have $\mathrm{len}_{\mathfrak{p}}(M) = \mathrm{len}_{\mathfrak{p}}(M[p^\infty])$.

Conjecture 4. Assume hypotheses (Hyp 1), (Hyp 2), and (Hyp 4) hold. If $L(E,\chi,1) \neq 0$, then $\mathrm{ord}_{\mathfrak{p}}(\Theta) = \mathrm{len}_{\mathfrak{p}}(Ш(E/K)) + \mathrm{len}_{\mathfrak{p}}(C) - \mathrm{len}_{\mathfrak{p}}(T) - \mathrm{len}_{\mathfrak{p}}(T^\vee)$.

Of course $L(E,\chi,1)$ vanishes exactly when $L(E,\bar{\chi},1)$ does.

Denote by $F_{\mathfrak{p}}$ the completion of $\mathbb{Z}[\zeta_d]$ at $\mathfrak{p}$ and by $\mathcal{O}_{\mathfrak{p}}$ its ring of integers. So $\mathcal{O}_{\mathfrak{p}} = \mathbb{Z}[G]_{\mathfrak{p}}$ is a unramified extension of $\mathbb{Z}_p$ by assumption (Hyp 4). Then $\mathrm{ord}_{\mathfrak{p}}(\Theta) = \mathrm{ord}_{\mathfrak{p}}(\chi(\Theta))$ where we view $\chi(\Theta) \in F_{\mathfrak{p}}^\times$.

One can reformulate this conjecture using fashionable K-groups. For references on K-theory, see chapter 2 of [2] and references in there. Let $\mathfrak{M}_{\mathfrak{p}}$ be the category of finitely generated torsion $\mathcal{O}_{\mathfrak{p}}$-modules and let $\delta\colon K_1(F_{\mathfrak{p}}) \to K_0(\mathfrak{M}_{\mathfrak{p}})$ be the connecting homomorphism in the localisation sequence for K-theory. Then we can reformulate it as follows.

Conjecture 4′. Assume hypotheses (Hyp 1), (Hyp 2) and (Hyp 4) hold. If $L(E,\chi,1) \neq 0$, then the image of $\chi(\Theta) \in F_{\mathfrak{p}}^\times \cong K_1(F_{\mathfrak{p}})$ under the map δ is the formal sum $[Ш(E/K)] + [C] - [T] - [T^\vee]$.

Lemma 22. *These two conjectures are equivalent.*

Proof. We have the long exact sequence in which the middle term is $K_0(\mathfrak{M}_{\mathfrak{p}})$, which can be viewed as a relative K-group $K_0(\mathcal{O}_{\mathfrak{p}}, F_{\mathfrak{p}})$.

$$\begin{array}{ccccccccc} K_1(\mathcal{O}_{\mathfrak{p}}) & \longrightarrow & K_1(F_{\mathfrak{p}}) & \xrightarrow{\delta} & K_0(\mathfrak{M}_{\mathfrak{p}}) & \longrightarrow & K_0(\mathcal{O}_{\mathfrak{p}}) & \xrightarrow{\cong} & K_0(F_{\mathfrak{p}}) \\ \| & & \| & & & & \| & & \| \\ \mathcal{O}_{\mathfrak{p}}^\times & & F_{\mathfrak{p}}^\times & & & & \mathbb{Z} & & \mathbb{Z} \end{array}$$

So $K_0(\mathfrak{M}_{\mathfrak{p}})$ is also isomorphic to $\mathbb{Z}$. A finitely generated torsion $\mathcal{O}_{\mathfrak{p}}$-module M is the direct sum of cyclic modules, say $M = \oplus_i \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{k_i}$. Then its class in $K_0(\mathfrak{M}_{\mathfrak{p}})$ is equal to the class $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^k$, where $k = \sum_i k_i$. This k gives the isomorphism with $\mathbb{Z}$ and of course it is nothing but the function $\mathrm{len}_{\mathfrak{p}}\colon K_0(\mathfrak{M}_{\mathfrak{p}}) \to \mathbb{Z}$ described earlier.

On the other side, the connecting homomorphism $F_{\mathfrak{p}}^\times \to K_0(\mathfrak{M}_{\mathfrak{p}})$ sends α to the class of the module $\mathcal{O}_{\mathfrak{p}}/(\alpha)$ if α belongs to $\mathcal{O}_{\mathfrak{p}}$. So under the map $\mathrm{len}_{\mathfrak{p}}$ it is sent to $\mathrm{ord}_{\mathfrak{p}}(\alpha)$. This shows the equivalence of the two conjectures. □

Not only we used heavily that G is abelian, but also that p does not divide d. The general Equivariant Tamagawa Number Conjecture formulates a conjecture even when G is not abelian and when p does divide $\#G$.

The conjecture above is formulated only for a primitive character χ and links $L(E,\bar{\chi},1)$ when it is not zero to the arithmetic side. Equivalently, we only looked at primes $\mathfrak{p}$ of

$\mathbb{Z}[G]$ that come from primes in $\mathbb{Z}[\zeta_d]$. If the character is not primitive, then we get a fudge factor as in lemma 7. Instead we would have to use modified Stickelberger elements if we wish the conjecture to hold in general.

Exercise 13. Work out in details what the conjecture says when E is 435b1 and $(m,d) = (11,5)$ and $(m,d) = (7,3)$. Can you determine the eigenvalues of the action of a generator of G on $Ш(E/K)$?

Exercise 14. Let d be prime. Suppose $L(E/K,1) \neq 0$. Show that the BSD conjecture 1 over $\mathbb{Q}$ and the equivariant conjecture 4 imply the BSD conjecture 2 over K, at least up to units in $\mathbb{Z}[\frac{1}{d}]$.

Exercise (*) 15. Prove the conjecture using the Euler system given by Kato's zeta elements.

Exercise (*) 16. What is the correct conjecture when some of the hypotheses are not satisfied ? Say an additive place ramifies in $K/\mathbb{Q}$ and it becomes multiplicative or good ? Or if p divides d ?

What does the conjecture say more explicitely for small degree. Let $d = 3$, first. The primes p fall into two cases.

Suppose $d = 3$ and $p \equiv 1 \pmod 3$. In this case $\mathbb{F}_p$ contains the 3-rd roots of unity and hence $\mathbb{F}_p[G]$ splits as $\mathbb{F}_p \oplus \mathbb{F}_p\chi \oplus \mathbb{F}_p\bar{\chi}$. So for all the p-torsion parts of our finite $\mathbb{Z}[G]$-modules, such as $Ш(E/K)[p]$, we can split them into one-dimensional representation. This equivariant conjecture now says what irreducible part appear in these $\mathbb{F}_p[G]$-modules.

Suppose $d = 3$ and $p \equiv 2 \pmod 3$. Now, $\mathbb{F}_p[G]$ only splits into two factors, a trivial $\mathbb{F}_p$ and a 2-dimensional $\mathbb{F}_p$-vector space V with a non-trivial G-action. This V will split only over $\mathbb{F}_{p^2}$, i.e. $V \otimes \mathbb{F}_{p^2}$ is no longer irreducible. So the equivariant conjecture only says with what frequency

12 Numerical Examples

12.1 First example

Let E be the elliptic curve 67a1 with global minimal equation

$$y^2 + y = x^3 + x^2 - 12\,x - 21.$$

It is easy to show that $E(\mathbb{R})$ is connected and that Φ_v is trivial for the unique place 67 of bad reduction. All the Galois representations $\rho_p\colon \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p)$ are surjective and so E does not admit a non-trivial torsion point over any abelian extension of $\mathbb{Q}$. The full BSD is known over $\mathbb{Q}$ and the Tate-Shafarevich group $Ш(E/\mathbb{Q})$ is trivial.

As our abelian field, we take a septic field of conductor $m = 71$. It is generated by a root of

$$x^7 + x^6 - 30\,x^5 + 3\,x^4 + 254\,x^3 - 246\,x^2 - 245\,x + 137$$

and has discriminant 71^6. We compute that

$$\frac{L(E/K,1)\cdot\sqrt{\Delta_K}}{\Omega_+^7} = 6355441.0000\ldots \approx 2521^2.$$

Hence $E(K)$ is finite and, given that the Tamagawa factors are still trivial (as 67 does not ramify) and that there are no torsion points over K, we have $E(K) = 0$ and we expect

$\#Ш(E/K)$ to have order 2521^2. There is no hope that we could verify this other than by proving the Birch and Swinnerton-Dyer conjecture 2.

Choose 7 as a primitive root modulo m and write g for the generator σ_7 of G. Then the Stickelberger elements is

$$\Theta = -12 - 12\,g - 12\,g^2 + 2\,g^3 + 15\,g^4 + 15\,g^5 + 2\,g^6$$

in $\mathbb{Q}[G] = \mathbb{Q}[g]/(g^7 - 1)$. Its image under the Dirichlet character $\chi(g) = \zeta_7$ factors as

$$\chi(\Theta) = (-\zeta_7^3 - 2\,\zeta_7^2 - 2\,\zeta_7 - 1) \cdot (\zeta_7^5 + 2\,\zeta_7^4 + 4\,\zeta_7^3 + 2\,\zeta_7 + 1) \cdot (\zeta_7^5 + 2\,\zeta_7^4 + \zeta_7^3 + 2\,\zeta_7 - 2)$$

where the first factor is a unit while the two other factors are elements of norm 2521. So the equivariant BSD for E/K and $p = 2521$ simply claims that $Ш(E/K) = \mathbb{Z}[\frac{1}{7}][\zeta_7]/\chi(\Theta)$ as a $\mathbb{Z}[\frac{1}{7}][G]$-module. This is is equivalent to $Ш(E/K)[p] = \mathbb{F}_p\,\xi_1 \oplus \mathbb{F}_p\,\xi_2$ with the action of G given by $g(\xi_1) = 1312 \cdot \xi_1$ and $g(\xi_2) = 1028 \cdot \xi_2$. For all other primes $p \neq 67$, is claims that $Ш(E/K)[p]$ is trivial, just as BSD over K does.

12.2 Second example

The curve 204a1 has trivial Mordell-Weil group over $\mathbb{Q}$, in fact all ρ_p are surjective. The Tamagawa numbers are $c_\infty = 1$, $c_2 = 3$, $c_3 = 1$ and $c_{17} = 1$. Since the Winding number is $[0] = 3$, the Tate-Shafarevich group is trivial over $\mathbb{Q}$.

Now choose the conductor to be the prime $m = 181$ and the degree to be 5. The field K is actually given by the polynomial

$$x^5 + x^4 - 72\,x^3 - 123\,x^2 + 223\,x - 49\,.$$

The Stickelberger element is equal to

$$\zeta_5 \cdot (121\,\zeta_5^3 + 121\,\zeta_5^2 + 74)$$

where the second factor is a prime element of norm $328298161 = 18119^2$. Note that 18119 splits into two primes $\mathfrak{p}_1 \cdot \mathfrak{p}_2 = (121\,\zeta_5^3 + 121\,\zeta_5^2 + 47) \cdot (121\,\zeta_5^3 + 121\,\zeta_5^2 + 74)$ in $\mathbb{Q}(\zeta_5)$. We conclude that the non-5-primary part of $Ш(E/K)$ should be isomorphic to $\mathbb{Z}[\zeta_5]/\mathfrak{p}_2 \cong \mathbb{F}_{25}$.

12.3 Third example

As a third example, we take E to be 1738c1. Again, we have $E(\mathbb{Q}) = 0$ and $E(K)$ is torsion-free for all abelian fields. But $E(\mathbb{R})$ has two connected components and the reduction at $v = 2$ is non-split multiplicative of type I_{22}, at $v = 11$ it is split multiplicative of type I_4, and at $v = 79$ it is non-split multiplicative of type I_1. The Tamagawa numbers are $c_\infty = c_2 = 2$, $c_{11} = 4$ and $c_{79} = 1$. Since $[0] = 16$, BSD over $\mathbb{Q}$ asserts $Ш(E/\mathbb{Q}) = 0$, which can easily be shown to be true.

Now, we look at E over the field $K = \mathbb{Q}(\mu_{11})^+$, so $d = 5$ and $m = 11$. The $\mathbb{Z}[G]$-module C is now fairly complicated. First at ∞ we get $C_\infty = \mathbb{Z}/2\mathbb{Z}[G]$. The Néron model does not change for the places above 2 and 79 and since both are inert, we get $C_2 = \mathbb{Z}/2\mathbb{Z}$ and $C_{79} = 0$. Finally, there is a unique place w above $v = 11$ and the reduction is still split multiplicative. So $C_w = c_w = e_{w|11} \cdot c_{11} = 4 \cdot 5 = 20$. It is easy to see that the action of G

on this $C_{11} = {}^{\mathbb{Z}}/_{20\mathbb{Z}}$ is trivial. In particular, we do not have that Φ_w^G is equal to Φ_{11}. The BSD conjecture over K asserts that

$$\frac{L(E/K,1)\sqrt{\Delta_K}}{\Omega_+^5} \approx 1280 =^? \#C \cdot \#Ш(E/K)$$

which predicts that $Ш(E/K)$ is trivial. The Stickelberger element is $\Theta = 2 \cdot g \cdot (1-g)$. For the unique prime $\mathfrak{p}$ of $\mathbb{Q}(\zeta_5)$ above 2, we have $\mathrm{ord}_{\mathfrak{p}}(\Theta) = 1$ and this equals $\mathrm{ord}_{\mathfrak{p}}(C)$ if and only if $Ш(E/K)[2] = 0$. Note on the other hand, for the unique prime $\mathfrak{p}$ above 5, we would get $\mathrm{ord}_{\mathfrak{p}}(\Theta) = 1$, however $\mathrm{ord}_{\mathfrak{p}}(C) = 0$. So the conjecture for prime p dividing d can not be as simple as stated for $p \nmid d$.

12.4 Fourth example

Here we take the curve 147b1, which admits a 13-isogeny over $\mathbb{Q}$. When passing to the cubic extension of conductor $m = 7$, the curve acquires a K-rational torsion point of order 13. In fact $E(K) = {}^{\mathbb{Z}}/_{13\mathbb{Z}}$.

The place $v = 3$ is of split multiplicative reduction of type I_1 and this remains so for the unique place w above 3. The additive place $v = 7$ of type IV^* achieves good reduction over the unique place w above 7. This example does not satisfy (Hyp 1). We find that $C_w = 7^2$, so BSD over K is equivalent to $Ш(E/K)$ being trivial as $L(E/K,1)\sqrt{\Delta_K}/\Omega_+^2 \approx \frac{49}{13^2}$.

The Stickelberger element is equal to

$$\Theta = \frac{2}{13} - \frac{7}{13}\,g - \frac{8}{13}\,g^2$$

where $g = \sigma_3$. In particular, we find for $\chi(g) = \zeta_3$ that

$$\chi(\Theta) = \frac{1}{13} \cdot (10 + \zeta_3) = \frac{\zeta_3 - 2}{\zeta_3 - 3}$$

is a fraction of an element of norm 7 be an element of norm 13. Now we consider $p = 13$ and $\mathfrak{p} = \zeta_3 - 3$, one of the two primes above p in $\mathbb{Q}(\zeta_3)$. We find $\mathrm{ord}_{\mathfrak{p}}(\Theta) = -1$ and for the other prime $\bar{\mathfrak{p}}$, we have $\mathrm{ord}_{\bar{\mathfrak{p}}}(\Theta) = 0$.

It is important to note that Artin formalism does not hold in this situation as explained in footnote 7. Instead, we have

$$L(E/K,s) = \left(1 - 5 \cdot 7^{-s} + 7 \cdot 7^{-2s}\right)^{-1} \cdot L(E/\mathbb{Q},s) \cdot L(E,\chi,s) \cdot L(E,\bar{\chi},s)$$

and evaluated at $s = 1$, it is

$$\frac{L(E/K,1) \cdot \sqrt{7^2}}{\Omega_+^3} = \frac{7}{13} \cdot [0] \cdot \chi(\Theta) \cdot \overline{\chi(\Theta)}$$

which gives on both sides $\frac{49}{169}$ as $[0] = 1$. This makes it clear that our conjecture can not hold as such in this case, because of this additional Euler factor.

12.5 Fifth example

Let E be the curve 17a1 over $\mathbb{Q}(\zeta_1 1)^+$, which is a quintic field. The Stickelberger element evaluates to $\chi(\Theta) = 4 \cdot (\zeta_5^3 + \zeta_5 + 1)$, where the second factor is a unit. From the facts that $\prod_w c_w = 4$ and $E(K) = \mathbb{Z}/4\mathbb{Z}$, one sees that BSD over K states that $Ш(E/K)$ has 2^8 elements. It is easy to compute the 2-Selmer group $\mathrm{Sel}_2(E/K) = \left(\mathbb{Z}/2\mathbb{Z}\right)^5$. So we have $Ш(E/K)[2] = \left(\mathbb{Z}/2\mathbb{Z}\right)^4$ and we should believe that $Ш(E/K) = \left(\mathbb{Z}/4\mathbb{Z}\right)^4$.

12.6 Some tables

We include a few tables 2, 3, 4, 5with orders of Tate-Shafarevich groups over abelian fields. The latter ones were computed by John Bergall at Sage-days 22 at MSRI.

13 Reformulation using Fitting ideals

Let R be a noetherian ring and let M be a finitely generated torsion R-module. Take a free resolution $R^b \xrightarrow{\alpha} R^a \longrightarrow M \longrightarrow 0$ of M and write the map α as a matrix with entries in R. Then the i-th Fitting ideal $\mathrm{Fitt}^i(M)$ of M is defined to be the ideal in R generated by all $a - i$ times $a - i$ minors of the matrix of α. It is always true that the initial Fitting ideal $\mathrm{Fitt}^0(M)$ is contained in the annihilator.

If R is a Dedekind ring, then $\mathrm{Fitt}^0(M)$ is the product of $\mathfrak{p}^{\mathrm{len}_\mathfrak{p}(M)}$ as $\mathfrak{p}$ runs over all maximal ideals of R. If R is a principal ideal domain, then the sequence $\{\mathrm{Fitt}^i(M)\}_i$ determines M up to isomorphism.

The equivariant Birch and Swinnerton-Dyer conjecture 4 can yet be reformulated.

Conjecture 4″. Assume hypotheses (Hyp 1), (Hyp 2), and (Hyp 4) hold. If $L(E, \chi, 1) \neq 0$, then $\chi(\Theta) \in F_\mathfrak{p}$ generates the fractional $\mathcal{O}_\mathfrak{p}$-ideal

$$\mathrm{Fitt}^0_{\mathcal{O}_\mathfrak{p}}(Ш(E/K)) \cdot \mathrm{Fitt}^0_{\mathcal{O}_\mathfrak{p}}(C) \cdot \left(\mathrm{Fitt}^0_{\mathcal{O}_\mathfrak{p}}(T)\right)^{-2}.$$

This is a refinement of an old conjecture by Mazur and Tate [30]:

Conjecture 5. If R is a subring of $\mathbb{Q}$ containing all modular symbols $[\frac{a}{m}]$, then Θ belongs to the initial Fitting ideal in $R[G]$ of the integral Selmer group.

Under the assumption that $L(E/K, 1)$ does not vanish, the integral Selmer group is just the Tate-Shafarevich group. Moreover by assuming that the denominators of all modular symbols are invertible in R, it seems very plausible that T will be trivial, too. So for a prime $\mathfrak{p}$ "belonging" to a primitive character the above conjecture implies the $\mathfrak{p}$-part of the conjecture below. For any other primes $\mathfrak{p}$, there is a fudge factor appearing, which results in Θ not being the generator of the initial Fitting ideal anymore, but it will still lie in it, because the fudge factor is integral. So our conjecture should imply the conjecture of Mazur Tate at least for R replaced by $R[\frac{1}{d}]$.

These formulations are analogous to the classical theorem of Stickelberger which proves that his elements are annihilators of the class groups of abelian fields.

Curve	$m=7$	13	19	31	37	43	61	67	73	79	91	97
11a1	5^2	$2^2 \cdot 5^2$	2^2	5^2	2^4	1	2^2	$3^2 \cdot 5^2$	5^2	$3^2 \cdot 5^2$	2^2	$2^2 \cdot 3^2 \cdot 5^2$
14a1	1	3^2	2^2	0	3^2	3^2	3^2	3^2	2^2	$3^2 \cdot 7^2$	$2^2 \cdot 3^2$	3^4
15a1	2^2	1	2^2	2^2	$2^2 \cdot 3^2$	2^2	2^2	1	2^4	$2^2 \cdot 7^2$	2^4	$2^2 \cdot 3^4$
17a1	2^4	2^4	$2^4 \cdot 3^2$	2^4	2^8	2^4	$2^4 \cdot 3^2$	2^6	7^2	2^4	2^8	$2^6 \cdot 3^2$
19a1	3^2	3^4	3^2	$2^2 \cdot 3^2$	$3^2 \cdot 5^2$	0	3^4	0	0	3^4	$2^2 \cdot 3^2$	5^2
20a1	2^2	1	2^4	2^2	$2^2 \cdot 3^2$	2^2	2^2	1	0	$2^2 \cdot 3^2$	0	2^4
21a1	1	1	2^2	1	7^2	3^2	2^4	2^2	1	3^2	1	11^2
24a1	1	1	3^2	0	5^2	1	1	0	2^2	5^2	2^2	3^2
26a1	1	1	$2^2 \cdot 3^2$	3^2	$2^4 \cdot 3^2$	3^4	3^2	3^2	$2^2 \cdot 3^2$	3^2	0	$3^2 \cdot 5^2$
26b1	1	1	2^2	1	2^2	1	1	1	0	3^2	2^2	3^4
27a1	3^2	3^2	0	3^2	0	3^2	2^4	2^4	3^2	$2^2 \cdot 3^2$	3^2	$3^2 \cdot 5^2$
30a1	1	2^2	1	1	3^2	1	0	0	2^2	3^4	0	5^2
32a1	2^2	2^2	2^2	1	2^2	1	$2^2 \cdot 3^2$	2^2	2^2	$2^2 \cdot 5^2$	2^6	$2^2 \cdot 5^2$
33a1	1	1	2^2	5^2	2^2	2^2	1	0	2^2	3^2	1	3^2
34a1	1	1	1	1	5^2	2^2	1	1	0	$2^2 \cdot 3^2$	0	1
35a1	1	3^2	1	3^2	3^2	0	3^2	0	1	3^2	3^2	3^2
36a1	1	1	1	1	1	1	1	1	1	5^2	0	5^2

Table 2: Conjectural order of $Ш(E/K)$ for various curves of small conductor over cubic extensions. A 0 indicates that the analytic rank of $E(K)$ is positive.

Curve	$d=5$					$d=7$			$d=11$		
	$m=11$	31	41	61	71	29	43	71	23	67	89
11a1	5^2	5^6	5^4	19^2	5^4	5^6	5^6	5^6	5^{10}	$5^{10}\cdot 23^2$	$5^{10}\cdot 43^2$
14a1	3^4	3^4	3^4	3^4	3^4	$2^6\cdot 3^6$	2^6	$3^6\cdot 29^2$	3^{10}	$3^{10}\cdot 23^2$	3^{10}
15a1	2^4	1	2^4	2^4	$2^4\cdot 5^2$	2^{12}	2^6	1	2^{10}	2^{10}	$2^{10}\cdot 23^2$
17a1	2^8	2^8	2^8	2^8	2^8	1	$2^{12}\cdot 43^2$	1	2^{20}	$2^{20}\cdot 43^2$	$2^{20}\cdot 23^2$
19a1	3^4	$3^4\cdot 19^2$	3^4	3^8	$2^4\cdot 3^4$	3^6	3^6	$3^6\cdot 97^2$	3^{10}	$3^{10}\cdot 1013^2$	3^{10}
20a1	2^4	1	2^4	$2^4\cdot 5^2$	$2^4\cdot 19^2$	2^6	$2^6\cdot 13^2$	7^2	2^{10}	$2^{10}\cdot 11^2$	$2^{10}\cdot 23^2$
21a1	1	1	0	11^2	29^2	2^6	1	1	43^2	263^2	967^2
24a1	1	1	1	1	1	2^6	1	13^2	1	$23^2\cdot 43^2$	23^2
26a1	3^4	3^4	3^8	41^2	$3^4\cdot 5^2$	3^6	3^6	3^6	3^{10}	$3^{10}\cdot 23^2$	3^{10}
26b1	1	1	1	5^2	11^2	1	7^2	1	23^2	89^2	67^2
27a1	3^4	3^4	2^4	3^4	$3^4\cdot 11^2$	3^6	$3^6\cdot 13^2$	$2^6\cdot 3^6$	3^{10}	$3^{10}\cdot 23^2$	$3^{10}\cdot 199^2$
30a1	1	2^4	2^4	1	19^2	2^6	13^2	$2^6\cdot 13^2$	23^2	43^2	1297^2
32a1	2^4	2^4	2^4	$2^4\cdot 3^4$	$2^4\cdot 11^2$	2^{12}	2^6	2^6	2^{10}	2^{10}	$2^{10}\cdot 23^2$
33a1	1	5^2	1	2^4	71^2	2^6	181^2	1	1	991^2	1187^2
34a1	1	1	1	19^2	19^2	2^6	1	2^6	1	89^2	881^2
35a1	0	3^4	3^4	$3^4\cdot 11^2$	3^4	3^6	2^6	3^6	3^{10}	$3^{10}\cdot 23^2$	$3^{10}\cdot 67^2$
36a1	1	1	1	3^4	11^2	2^6	1	1	1	109^2	109^2

Table 3: Conjectural order of Ш(E/K) for various curves of small conductor over abelian extensions of degree $d=5$, 7 and 11. A 0 indicates that the analytic rank of $E(K)$ is positive.

m	7	13	19	31	37	43	61	67	73	79	97	103	109	127	139
$\sqrt{Ш(E/K)}$	2	3	1	3^3	3	2^2	1	3	3	2^3	17	3	$2 \cdot 3^2 \cdot 5$	$2 \cdot 37$	23
151	157	163	181	193	199	211	223	229	241	271	277	283			
2	2^4	43	7	2	$2 \cdot 5$	2^3	$3 \cdot 5$	2^2	$2^2 \cdot 3$	3^2	$2^3 \cdot 11$	$5 \cdot 23$			
307	313	331	337	349	367	373	379	397	409	421	433	439			
$2^3 \cdot 3$	$2 \cdot 3^2$	11	$2 \cdot 5$	7	7	7^2	73	3^4	$2^3 \cdot 3$	5^2	$2 \cdot 37$	3			
457	463	487	499	523	541	547	571	577	601	607	613	619			
$2^4 \cdot 3$	19	3^3	31	3	$2^2 \cdot 3$	3	$5 \cdot 7$	7	$7 \cdot 17$	$3 \cdot 7$	13	0			
631	643	661	673	691	709	727	733	739	751	757	769	787			
41	31	2^2	37	283	$2 \cdot 23$	53	97	$2^2 \cdot 7^2$	3^2	1	$2^3 \cdot 5$	2			
811	823	829	853	859	877	883	907	919	937	967	991	997			
$2^2 \cdot 3 \cdot 7$	43	3	3	$2 \cdot 13$	3^2	2^4	$2^2 \cdot 3 \cdot 7$	$2 \cdot 29$	73	2	$2 \cdot 3^2$	$2 \cdot 23$			

Table 4: The square root of the analytic orders of Sha for the curve 67a1 and various **cubic** extensions of prime conductor. This curve has trivial Tamagawa numbers c_v and no non-zero points over $\mathbb{Q}$.

11	31	41	61	71	101	131	151	181	191	211	241	251
11	31	11	11	71	$5 \cdot 29$	11	$41 \cdot 199$	$5 \cdot 71$	11	19	521	$11 \cdot 311$
271	281	311	331	401	421	431	461	491	521	541	571	601
$31 \cdot 41$	$5 \cdot 31$	2^2	179	$2^2 \cdot 71$	$2^2 \cdot 149$	131	$5 \cdot 569$	$11 \cdot 29$	$3^2 \cdot 11$	$2^2 \cdot 29$	$5 \cdot 7^2$	$29 \cdot 151$
631	641	661	691	701	751	761	811	821	881	911	941	971
491	199	$2^2 \cdot 5$	$41 \cdot 61$	$2^4 \cdot 251$	101	$5 \cdot 181$	719	$3^2 \cdot 71$	$2^2 \cdot 19$	$19 \cdot 59$	509	8761

Table 5: The square root of the analytic orders of Sha for the curve 67a1 and various **quintic** extensions of prime conductor. This curve has trivial Tamagawa numbers c_v and no non-zero points over $\mathbb{Q}$.

14 The equivariant Tamagawa number conjecture

There are existing conjectures about equivariant L-values in great generality. They are formulated for any motive with possibly non-commutative coefficient rings. See [7, 39, 22, 25] for details. The case of elliptic curves has been looked at a bit closer. It is "standard" that the conjecture for the motive $h^1(E)(1)$ and the ring $\mathbb{Z}$ is equivalent to the Birch and Swinnerton-Dyer conjecture over $\mathbb{Q}$ – at least up to the sign. A very good explanation of this can be found in [25].

Our equivariant setting has also been considered in [33, 8, 4, 5, 3]. Mostly these articles are concerned with the harder and more interesting cases when either the Galois group G is non-abelian or if the prime p divides the order of the group G.

[14] [[14]]

15 Kurihara's recent work

That the higher Fitting ideals can be useful to analyse further the structure of the Selmer group. We present here unpublished work of Kurihara, which deals with the trivial character rather than with general characters χ. Moreover, in this section (Hyp 4) is not satisfied, in fact, we are exactly interested in d being a power of p.

We suppose that E has good reduction at p. We impose that $a_p \not\equiv 1 \pmod{p}$ (not anomalous) and that $a_p = 0$ if it is divisible by p. We assume that the p-adic representation

[14] [[Todo:]]

is surjective, i.e. $\mathrm{Gal}(\mathbb{Q}(E[p^n])/\mathbb{Q})$ is isomorphic to $\mathrm{GL}_2\left(\mathbb{Z}/p^n\mathbb{Z}\right)$ for all n. We also assume that the Iwasawa μ-invariant vanishes for this curve (conjecturally this happens for at least one curve in each isogeny class).

As conductor m we will choose a product of r primes ℓ_j all of which are congruent to 1 modulo p. Then as K we take the maximal p-extension in $\mathbb{Q}(\zeta_m)$, which is of degree $p^{\sum n_j}$ where $n_j = \mathrm{ord}_p(\ell_j - 1)$. The Galois group G is a direct sum $\oplus G_{\ell_j}$ for Galois group of the subextension of conductor ℓ_j. Write N_j for the norm element $\sum \sigma$ where σ runs over all elements in G_{ℓ_j}.

Now I is the augmentation ideal in $\mathbb{Z}_p[G]$. For any $i \geqslant 0$, the following function is related to the i-th Fitting ideal. For any $\alpha \in \mathbb{Z}_p[G]$, set

$$\mathrm{ord}^i(\alpha) = \max\left\{ c \;\middle|\; \alpha \in p^c \cdot \mathbb{Z}_p[G] + I^{i+1} + \sum_j N_j\, \mathbb{Z}_p[G] \right\}$$

Example. Suppose $m = \ell$ is a prime. Choose a generator g of G and set $S = g - 1$. Then I is generated by S and $N = \sum_{i=0}^{d-1} g^i$ expands as $N = d + \frac{1}{2}d(d-1)\cdot S + \cdots$. So we can make $\mathrm{ord}^0(\alpha)$ more explicit. Write $\alpha = \alpha_0 + \alpha_1 \cdot S + \cdots$ in the variable S. Then, if $\mathrm{ord}_p(\alpha) < \mathrm{ord}_p(d)$, then $\mathrm{ord}^0(\alpha) = \mathrm{ord}_p(\alpha_0)$, otherwise $\mathrm{ord}^0(\alpha) = \infty$. In general $\mathrm{ord}^i(\alpha)$ is linked to the minimum of the valuations of the i-th first coefficients of α.

Recall that the p-primary Selmer group fits into an exact sequence

$$0 \longrightarrow E(K) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow \mathrm{Sel}_{p^\infty}(E/K) \longrightarrow Ш(E/K)[p^\infty] \longrightarrow 0$$

Theorem 23 (Kurihara). *Decompose the dual $X = \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}), \mathbb{Q}_p/\mathbb{Z}_p)$ of the p-primary Selmer group as $\bigoplus_{i=1}^{s} \mathbb{Z}_p/\!/_{\mathbb{Z}_p p^{k_i}}$ for $k_1 \leqslant k_2 \leqslant \ldots \leqslant k_s \leqslant \infty$. Then, for all $i \geqslant 0$*

$$k_1 + k_2 + \cdots + k_{s-i} \leqslant \mathrm{ord}^i(\Theta).$$

This needs not always to be a sharp bound, but we will get one if we vary over different conductors m. Set

$$\vartheta_i = \max\left\{ \mathrm{ord}^i(\Theta_{E/K}) \;\middle|\; K \text{ of conductor } m = \prod \ell_i \text{ as above} \right\}$$

Theorem 24 (Kurihara). *Assume that p does not divide the Tamagawa numbers, assume that p is good ordinary for E, that the p-adic height is non-degenerate and the main conjecture holds.*[15] *Write s for the integer such that*

$$\infty = \vartheta_0 = \vartheta_1 = \cdots = \vartheta_{s-1} > \vartheta_s \geqslant \vartheta_{s+1} \geqslant \cdots.$$

Firstly, this implies that $\vartheta_s = \vartheta_{s+1}$, $\vartheta_{s+2} = \vartheta_{s+3}$ ..., and that the consecutive differences between these pairs are always even. If we write $t_j = \frac{1}{2}(\vartheta_{s+2j} - \vartheta_{s+2j+2})$, then the structure of the Selmer group is given by

$$X \cong \mathbb{Z}_p^s \oplus \bigoplus_{j \geqslant 0} \left(\mathbb{Z}/p^{t_j}\mathbb{Z} \right)^{\oplus 2}.$$

Example. [16] As an example we take the curve [[16]]

$$E\colon\ y^2+y=x^3-x^2-8216\,x+683553$$

which is the quadratic twist of 11a3 by 157. We find $[0]=9$. Since the Tamagawa numbers and the torsion order are trivial, the predicted order of $Ш(E/\mathbb{Q})$ is 9. We are going to choose three different prime values m and for each we pick a primitive element g modulo m. We write S for the variable $g-1$ in $\mathbb{Q}[G]$. We get the following Stickelberger elements.

m	d	a_m	g	Θ	$\mathrm{ord}^0(\Theta)$	$\mathrm{ord}^1(\Theta)$	$\mathrm{ord}^2(\Theta)$
19	9	0	σ_2	$-18-99\,S-237\,S^2+\cdots$	∞	∞	1
37	9	3	σ_2	$9+36\,S+119\,S^2+\cdots$	∞	∞	0
109	27	10	σ_6	$72+12875\,S+12841\,S^2+\cdots$	2	2	0

For $\mathrm{ord}^0(\alpha)$ we find that it is equal to ∞ is the 3-adic valuation of the leading term of Θ is larger or equal to $\mathrm{ord}_3(m-1)=\mathrm{ord}_3(d)$. This happens in the first two cases, but not in the last as 72 is not divisible by 27. And so forth. The first two choices of m would not have given the correct bounds on $Ш(E/\mathbb{Q})[3^\infty]$. The last choice instead proves that $Ш(E/\mathbb{Q})[3^\infty]=\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, which we could have deduces from the non-degeneracy of the Cassels-Tate pairing, too.

16 A congruence

We prove the following congruence that appears in several places, e.g. [21] and [3].

Theorem 25. *Let χ be a Dirichlet character modulo m of order d. If $(d,m)=1$, i.e. (Hyp 3) holds, then*

$$\chi(\Theta)\equiv[0]\cdot\prod_{\ell\mid m}\bigl(-1+a_\ell-\delta_N(\ell)\bigr)\pmod{(\zeta_d-1)}$$

where $\delta_N(\ell)$ is equal to 0 if ℓ is coprime to N and equal to 1 otherwise.

Proof. Since for any invertible a modulo m, the value of $\chi(a)$ is a d-th root of unity, it is congruent to 1 modulo ζ_d-1. Hence

$$\chi(\Theta)\equiv\sum_{a\bmod m^\times}\left[\frac{a}{m}\right]=\mathbb{1}_m(\Theta)\pmod{(\zeta_d-1)},$$

where $\mathbb{1}_m$ stands for the trivial representation modulo m. Now, corollary 8 yields

$$\mathbb{1}_m(\Theta)=[0]\cdot\prod_{\ell\mid m}\Bigl(-1+a_\ell-\delta_N(\ell)\Bigr).$$

□

[15] All of these conditions can be checked easily in a given example.

[16] [[Todo: These values do not coincide with the ones Kurihara presented in Montréal, but the result is the same.]]

Suppose d is a prime. The equivariant Tamagawa number conjecture at the prime $p = d$ can be shown to be equivalent to this congruence under certain conditions, see [3]. Note that this is strictly stronger than the sort of conjecture one would make by analogy from the case of primes p not dividing d as explained in the example in 12.3.

Note that if d is prime and (Hyp 3) holds, then all prime divisors ℓ of m are congruent to 1 modulo d. So the congruence can also be written as

$$\chi(\Theta) \equiv \frac{L(E/\mathbb{Q},1)}{\Omega_+} \cdot \prod_{\ell|m}(-1)(1-a_\ell\ell^{-1}-\delta_N\ell^{-1}) = \mu(m)\cdot\frac{L_m(E/\mathbb{Q},1)}{\Omega_+} \pmod{(\zeta_d-1)}$$

where $L_m(E/\mathbb{Q},s)$ is the L-function $L(E/\mathbb{Q},s)$ with all the local factors at places $\ell \mid m$ removed.

17 Vanishing

In a series of articles [15, 14, 20, 21, 27], David, Fearnley, Kisilevsky, and Kuwata studied the frequency with which the twisted L-value vanishes in odd cyclic extensions. Through the conjecture of Birch and Swinnerton-Dyer this should tell us how often we expect the rank of the Mordell-Weil group to grow in such extensions.

We measure the frequency of vanishing by the following function:

$$N_{E,d}(X) = \left\{\chi \text{ Dirichlet character of order } d \,\middle|\, f_\chi \leqslant X \text{ and } L(E,\chi,1)=0\right\}$$

Conjecture 6. [17] The function $N_{E,d}(X)$ for d an odd prime behaves as follows:

$N_{E,3}(X) \sim C\cdot\sqrt{X}\cdot\log^c(X)$ for some constants C and c.
$N_{E,5}(X) \ll X^\varepsilon$ for any $\varepsilon > 0$, but $N_{E,5}(X)$ is not bounded.
$N_{E,d}(X)$ is bounded for all odd primes $d > 5$.

The growth for $d = 3$ should be compared to the number of all cubic characters of conductor less than X. It is known that this grows like $0.317\ldots\cdot X$.

This conjecture can be deduced from certain conjectures in random matrix theory. Apart from vast numerical evidence supporting the conjectures, they also have some results. It is shown that there are infinitely many cubic twists that vanish granted that there is at last one cubic extension in which the rank grows. This uses elliptic surfaces. Instead using modular symbols, one can show

Theorem 26. *Let d be an odd prime and suppose $[0] \not\equiv 0 \pmod{d}$. Then there is a set S of positive density among the characters of order d and prime conductors such that $L(E,\chi,1) \neq 0$ for all characters χ of order d and conductor f_χ belongs to S.*

Proof. By Chebotarev, there exists an positive density of primes ℓ of good reduction such that $a_\ell - 2 \not\equiv 0 \pmod{d}$ and $\ell \equiv 1 \pmod{d}$. So by theorem 25, we have that $\chi(\Theta) \not\equiv 0 \pmod{(\zeta_d - 1)}$ for any character χ of order d and conductor ℓ. □

[17] For $d = 3$, this is not stated as a conjecture in the paper only as a possibility; they conjecture instead that $\log N_{E,3}(X) \sim \frac{1}{2}\log(X)$.

In an other direction, when considering towers of cyclic fields, we have analytic results by Rohrlich [34] and Chinta [9]. The interest of Iwasawa theory is in the case when $m = p^k$ is a power of a prime p.

Theorem 27 (Rohrlich). *Let p be a prime. Then $L(E, \chi, 1) \neq 0$ for all but finitely many characters χ of conductor a power of p.*

This theorem is used in the proof that the rank of the Mordell-Weil group of E is bounded in the tower $E(\mathbb{Q}(\zeta_{p^k}))$; as the theorem suggests indeed.

Let η_p be the smallest k such that $L(E, \chi, 1) \neq 0$ for all χ of conductor a larger power of p than p^k.

Theorem 28 (Chinta). *There is a constant C depending on E, such that $\eta_p < C$ for all p.*

Varying the conductor through primes p, one gets results like

Theorem 29 (Chinta). *Then for all $\varepsilon > 0$,*

$$\#\Big\{\chi \;\Big|\; f_\chi = p \text{ and } L(E, \chi, 1) = 0\Big\} \leqslant p^{\frac{7}{8}+\varepsilon}$$

for all large enough primes p.

We also have a wild speculation by Coates [10].

Conjecture 7. Let K_∞ be the composite of all cyclotomic $\mathbb{Z}_p$-extensions of $\mathbb{Q}$ as p runs through all primes. Then there are only finitely many characters χ of $\mathrm{Gal}(K_\infty/K)$ of finite order such that $L(E, \chi, 1) = 0$.

In particular, $\eta_p = 0$ for all but finitely many p. It is easy to find examples where we expect $\eta_p = 0$ for all primes p; and the main conjecture of Iwasawa theory would imply this. Yet it is not clear what happens in the composite extensions.

Example. Let E be the curve 11a3. It is known that the rank of E over any $\mathbb{Z}_p$-extension is still 0, see [11]. Now let p and q be two distinct primes. The conjecture above also says that $L(E, \chi, 1)$ vanishes only finitely many times as χ runs through all characters of order $p \cdot q$ and conductor $p^2 \cdot q^2$.

A short numerical experiment shows that $L(E, \chi, 1)$ does not vanish for any pair (p, q) with $2 < p < 11$ and $p < q < 100$. By the way the Tate-Shafarevich group of the last example $p \cdot q = 7 \cdot 97$ is supposed to have the order equal a square of an integer that has more than 500 digits and whose factorisation I was not able to determine.

References

[1] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, part 2, 617–636, probably the first hit in a internet search on "Manin constant".

[2] Konstantin Ardakov and Simon Wadsley, *Characteristic elements for p-torsion Iwasawa modules*, J. Algebraic Geom. **15** (2006), no. 2, 339–377.

[3] Werner Bley, *ETNC and modular symbols*, 2010.

[4] ———, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture*, to be published in Experimental Mathematics, 2010.

[5] ———, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (Part II)*, 2010.

[6] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[7] D. Burns and M. Flach, *Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001), 501–570.

[8] Masataka Chida, *On the equivariant Tamagawa number conjecture for CM elliptic curves*, Proceedings of the Symposium on Algebraic Number Theory and Related Topics, RIMS Kôkyûroku Bessatsu, B4, Res. Inst. Math. Sci. (RIMS), Kyoto, 2007, pp. 197–221.

[9] Gautam Chinta, *Analytic ranks of elliptic curves over cyclotomic fields*, J. Reine Angew. Math. **544** (2002), 13–24.

[10] John Coates, *The enigmatic Tate-Shafarevich group*, 2011.

[11] John Coates and Ramdorai Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, vol. 88, Narosa Publishing House, 2000.

[12] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[13] Henri Darmon, *Euler systems and refined conjectures of Birch Swinnerton-Dyer type*, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), Contemp. Math., vol. 165, Amer. Math. Soc., Providence, RI, 1994, pp. 265–276.

[14] Chantal David, Jack Fearnley, and Hershy Kisilevsky, *Vanishing of L-functions of elliptic curves over number fields*, Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Note Ser., vol. 341, pp. 247–259.

[15] ———, *On the vanishing of twisted L-functions of elliptic curves*, Experiment. Math. **13** (2004), no. 2, 185–198.

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

[17] Tim Dokchitser, *L-functions and root numbers*, Excellent lectures at the same Sardinia conference on Birch and Swinnerton-Dyer conference, 2011.

[18] Vladimir Dokchitser, *Birch and swinnerton-dyer and parity*, Marvellous lectures at the same Sardinia conference on Birch and Swinnerton-Dyer conference, 2011.

[19] V. G. Drinfel′d, *Two theorems on modular curves*, Funkcional. Anal. i Priložen. **7** (1973), no. 2, 83–84.

[20] Jack Fearnley and Hershy Kisilevsky, *Critical values of derivatives of twisted elliptic L-functions*, Experiment. Math. **19** (2010), no. 2, 149–160.

[21] Jack Fearnley, Masato Kuwata, and Hershy Kisilevsky, *Vanishing and non-vanishing Dirichlet twists of L-functinos of elliptic curves*, unpublished, 200?

[22] Matthias Flach, *The equivariant Tamagawa number conjecture: a survey*, Stark's conjectures: recent work and new directions, Contemp. Math., vol. 358, Amer. Math. Soc., Providence, RI, 2004, With an appendix by C. Greither, pp. 79–125.

[23] Dorian Goldfeld, *On the computational complexity of modular symbols*, Math. Comp. **58** (1992), no. 198, 807–814.

[24] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque (2004), no. 295, ix, 117–290, Cohomologies p-adiques et applications arithmétiques. III.

[25] Guido Kings, *An introduction to the equivariant Tamagawa number conjecture: the relation to the Birch-Swinnerton-Dyer conjecture*, available at `http://www.uni-regensburg.de/Fakultaeten/nat_Fak_I/preprints/Kings.htm`, 2009.

[26] V. A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $SH(E, \mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671.

[27] Masato Kuwata, *Points defined over cyclic quartic extensions on an elliptic curve and generalized Kummer surfaces*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 65–76.

[28] Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[29] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[30] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*, Duke Math. J. **54** (1987), no. 2, 711–750.

[31] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.

[32] Robert Miller, *Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one*, To appear, preprint available at `http://arxiv.org/abs/1010.2431`, 2011.

[33] Tejaswi Navilarekallu, *Equivariant Birch-Swinnerton-Dyer conjecture for the base change of elliptic curves: an example*, Int. Math. Res. Not. IMRN (2008), no. 6.

[34] David E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423.

[35] ———, *Modular curves, Hecke correspondence, and L-functions*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 41–100.

[36] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[37] William Stein and Christian Wuthrich, *Computations About Tate-Shafarevich Groups Using Iwasawa Theory*, `http://modular.math.washington.edu/papers/shark/`, 2011.

[38] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[39] Otmar Venjakob, *From the Birch and Swinnerton-Dyer conjecture to non-commutative Iwasawa theory via the equivariant Tamagawa number conjecture—a survey*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 333–380.

[40] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.