Denominators of BSD quotients

Young Researchers in Algebraic Number Theory

David Kurniadi Angdinata

London School of Geometry and Number Theory

Wednesday, 31 July 2024

Mordell's theorem

Let E be an elliptic curve over $\mathbb{Q}$ given by a Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbb{Q}.$$

Its rational points forms a group $E(\mathbb{Q})$ under a geometric addition law.

Theorem (Mordell)

$$E(\mathbb{Q}) \cong \mathrm{tor}(E) \oplus \mathbb{Z}^{\mathrm{rk}(E)}.$$

The **torsion subgroup** $\mathrm{tor}(E)$ is well understood.

Theorem (Mazur)

$$\mathrm{tor}(E) \cong \begin{cases} C_n & \text{for } n = 1,2,3,4,5,6,7,8,9,10,12, \\ C_2 \oplus C_{2n} & \text{for } n = 1,2,3,4. \end{cases}$$

The **rank** $\mathrm{rk}(E)$ is somewhat mysterious.

The Birch–Swinnerton-Dyer conjecture

Assume E has conductor N. The L-function of E is the infinite product

$$L(E,s) := \prod_p \frac{1}{L_p(E,p^{-s})}.$$

Here,

$$L_p(E,T) := \begin{cases} 1 \pm \epsilon T & \text{if } p \mid N, \\ 1 - a_p(E)T + pT^2 & \text{if } p \nmid N, \end{cases}$$

where $a_p(E) := 1 + p - \#E(\mathbb{F}_p)$ and $\epsilon \in \{-1, 0, 1\}$.

Conjecture (weak Birch–Swinnerton-Dyer)

$$\operatorname{ord}_{s=1} L(E,s) = \operatorname{rk}(E).$$

This is known for $\operatorname{ord}_{s=1} L(E,s) \leq 1$. Assume that $\operatorname{ord}_{s=1} L(E,s) = 0$.

The Birch–Swinnerton-Dyer quotient

Conjecture (strong Birch–Swinnerton-Dyer)

$$\frac{L(E,1)}{\Omega(E)} = \frac{\mathrm{Tam}(E) \cdot \#Ш(E)}{\#\,\mathrm{tor}(E)^2}.$$

The LHS is the **algebraic L-value** and the RHS is the **BSD quotient**.

- The **Tamagawa product** is the finite product

$$\mathrm{Tam}(E) := \prod_{p \mid N} [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)],$$

  where $E_0(\mathbb{Q}_p)$ is the subgroup of points of $E(\mathbb{Q}_p)$ whose reduction is *nonsingular*. It can be computed by *Tate's algorithm*.
- The **Tate–Shafarevich group** is the finite group

$$Ш(E) := \ker\left(H^2(\mathbb{Q}, E) \to H^2(\mathbb{R}, E) \times \prod_p H^2(\mathbb{Q}_p, E) \right).$$

The Birch–Swinnerton-Dyer quotient

Conjecture (strong Birch–Swinnerton-Dyer)

$$\frac{L(E,1)}{\Omega(E)} = \frac{\mathrm{Tam}(E)\cdot \#\text{Ш}(E)}{\#\,\mathrm{tor}(E)^2}.$$

The LHS is the **algebraic L-value** and the RHS is the **BSD quotient**.

- The **real period** is the integral

$$\Omega(E) := \int_{E(\mathbb{R})} \omega_E,$$

where ω_E is the **Néron differential**. If E is given by a *minimal* Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$,

$$\omega_E = \frac{\mathrm{d}x}{2y + a_1x + a_3}.$$

It is the least positive element of the *real period lattice* of E.

Elliptic curve with Cremona label 90c3 (LMFDB label 90.c7)

Introduction

Overview Random
Universe Knowledge

L-functions

Rational All

Modular forms

Classical Maass
Hilbert Bianchi

Varieties

Elliptic curves over $\mathbb{Q}$
Elliptic curves over $\mathbb{Q}(\alpha)$
Genus 2 curves over $\mathbb{Q}$
Higher genus families
Abelian varieties over $\mathbb{F}_q$

Fields

Number fields
p-adic fields

Representations

Dirichlet characters
Artin representations

Groups

Galois groups
Sato-Tate groups

Database

Minimal Weierstrass equation

Show commands: Magma / Oscar / PariGP / SageMath

$y^2+xy+y=x^3-x^2-122x+1721$ (homogenize, simplify)

Mordell-Weil group structure

$\mathbb{Z}/12\mathbb{Z}$

Torsion generators

$(-9, 49)$

Integral points

$(-15,7)$, $(-9,49)$, $(-9,-41)$, $(1,39)$, $(1,-41)$, $(9,31)$, $(9,-41)$, $(21,79)$, $(21,-101)$, $(81,679)$, $(81,-761)$

Invariants

Conductor:	90	=	$2 \cdot 3^{2} \cdot 5$
Discriminant:	-1119744000	=	$-1 \cdot 2^{12} \cdot 3^{7} \cdot 5^{3}$
j-invariant:	$-\frac{273359449}{1536000}$	=	$-1 \cdot 2^{-12} \cdot 3^{-1} \cdot 5^{-3} \cdot 11^{3} \cdot 59^{3}$
Endomorphism ring:	$\mathbb{Z}$		
Geometric endomorphism ring:	$\mathbb{Z}$		(no potential complex multiplication)
Sato-Tate group:	$\mathrm{SU}(2)$		
Faltings height:	$0.42032494899046121656963281857\dots$		
Stable Faltings height:	$-0.12898119534359362912798979989\dots$		
abc quality:	$1.0491971880149842\dots$		
Szpiro ratio:	$6.308958268204\dots$		

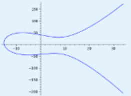
BSD invariants

Analytic rank:	0
Regulator:	1
Real period:	$1.3375959945886485057653424429\dots$
Tamagawa product:	$144 = (2^2 \cdot 3) \cdot 2^2 \cdot 3$
Torsion order:	12
Analytic order of Ш:	1 (exact)
Special value:	$L(E,1) \approx 1.3375959945886485057653424429$

$$\frac{L(E,1)}{\Omega(E)} = \frac{\mathrm{Tam}(E)\cdot \#Ш(E)}{\#\,\mathrm{tor}(E)^2}$$

Properties

Label	90c3



Conductor	90
Discriminant	-1119744000
j-invariant	$-\frac{273359449}{1536000}$
CM	no
Rank	0
Torsion structure	$\mathbb{Z}/12\mathbb{Z}$

Related objects

Isogeny class 90c
Minimal quadratic twist 30a3
All twists
L-function
Symmetric square L-function
Modular form 90.2.a.c

Downloads

q-expansion to text
All stored data to text
Code to Magma
Code to Oscar
Code to PariGP
Code to SageMath
Underlying data

Learn more

Source and acknowledgments
Completeness of the data
Reliability of the data
Elliptic curve labels
Congruent number curves
Picture description

Denominator bounds

Observe that BSD quotients have bounded denominators.

Theorem (Mazur)

$$\mathrm{tor}(E) \cong \begin{cases} C_n & \text{for } n = 1,2,3,4,5,6,7,8,9,10,12, \\ C_2 \oplus C_{2n} & \text{for } n = 1,2,3,4. \end{cases}$$

Corollary

$$\mathrm{ord}_p\left(\frac{\mathrm{Tam}(E) \cdot \#Ш(E)}{\#\,\mathrm{tor}(E)^2}\right) \geq \begin{cases} -8 & \text{if } p = 2, \\ -4 & \text{if } p = 3, \\ -2 & \text{if } p = 5,7, \\ 0 & \text{if } p \geq 11. \end{cases}$$

There are typically cancellations between tor(E) and Tam(E).

Torsion cancellations

Theorem (Lorenzini, 2010)

Assume that $\mathrm{tor}(E)$ *has a point of order* $n \geq 4$.

- *If* $n = 4$, *then* $2 \mid \mathrm{Tam}(E)$, *except for 15a7, 15a8, 17a4.*
- *If* $n \geq 5$, *then* $n \mid \mathrm{Tam}(E)$, *except for 11a3, 14a4, 14a6, 20a2.*
- *If* $n = 9$, *then* $27 \mid \mathrm{Tam}(E)$.

Corollary

With seven exceptions,

$$\mathrm{ord}_p\left(\frac{\mathrm{Tam}(E)\cdot \#\text{Ш}(E)}{\#\,\mathrm{tor}(E)^2}\right) \geq \begin{cases} -5 & \text{if } p = 2 \text{ and } \mathrm{tor}(E) \cong C_2 \oplus C_{2n}, \\ -3 & \text{if } p = 2 \text{ and } \mathrm{tor}(E) \ncong C_2 \oplus C_{2n}, \\ -2 & \text{if } p = 3 \text{ and } \mathrm{tor}(E) \cong C_3, \\ -1 & \text{if } p = 3 \text{ and } \mathrm{tor}(E) \ncong C_3, \\ -1 & \text{if } p = 5, 7, \\ 0 & \text{if } p \geq 11. \end{cases}$$

The seven exceptions

Let BSD(E) denote the BSD quotient.

E	$11a3$	$14a4$	$14a6$	$15a7$	$15a8$	$17a4$	$20a2$
tor(E)	C_5	C_6	C_6	C_4	C_4	C_4	C_6
Tam(E)	1	2	2	1	1	1	3
Ш(E)	1	1	1	1	1	1	1
BSD(E)	$\frac{1}{5^2}$	$\frac{1}{2\cdot 3^2}$	$\frac{1}{2\cdot 3^2}$	$\frac{1}{2^4}$	$\frac{1}{2^4}$	$\frac{1}{2^4}$	$\frac{1}{2^2\cdot 3}$
$c_0(E)$	5	3	3	2	4	4	2
$c_0(E)\,\mathrm{BSD}(E)$	$\frac{1}{5}$	$\frac{1}{2\cdot 3}$	$\frac{1}{2\cdot 3}$	$\frac{1}{2^3}$	$\frac{1}{2^2}$	$\frac{1}{2^2}$	$\frac{1}{2\cdot 3}$

Here, $c_0(E)$ is the **Manin constant** in the LMFDB.

Elliptic curve with Cremona label 11a3 (LMFDB label 11.a3)

BSD invariants

Show commands: Magma / Oscar / PariGP / SageMath

Analytic rank:	0
Regulator:	1
Real period:	$6.3460465213977671084439730838\ldots$
Tamagawa product:	1
Torsion order:	5
Analytic order of Ш:	1 (exact)
Special value:	$L(E,1) \approx 0.25384186085591068433775892335$

BSD formula

$$0.253841861 \approx L(E,1) = \frac{\#Ш(E/\mathbb{Q}) \cdot \Omega_E \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p}{\#E(\mathbb{Q})_{\mathrm{tor}}^2} \approx \frac{1 \cdot 6.346047 \cdot 1.000000 \cdot 1}{5^2} \approx 0.253841861$$

Modular invariants

Modular form 11.2.a.a

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + O(q^{20})$$

For more coefficients, see the Downloads section to the right.

Modular degree:	5
$\Gamma_0(N)$-optimal:	no
Manin constant:	5

Local data

This elliptic curve is semistable. There is only one prime of bad reduction:

prime	Tamagawa number	Kodaira symbol	Reduction type	Root number	ord(N)	ord(Δ)	ord(j)_
11	1	I_1	Split multiplicative	-1	1	1	1

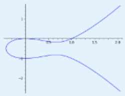
Galois representations

The ℓ-adic Galois representation has maximal image for all primes ℓ except those listed in the table below.

prime ℓ	mod-ℓ image	ℓ-adic image
5	5B.1.1	25.120.0.1

Properties

Label	11a3



Conductor	11
Discriminant	-11
j-invariant	$-\frac{4096}{11}$
CM	no
Rank	0
Torsion structure	$\mathbb{Z}/5\mathbb{Z}$

Related objects

Isogeny class 11a
Minimal quadratic twist 11a3
All twists
L-function
Symmetric square L-function
Symmetric cube L-function
Modular form 11.2.a.a

Downloads

q-expansion to text
All stored data to text
Code to Magma
Code to Oscar
Code to PariGP
Code to SageMath
Underlying data

Learn more

Source and acknowledgments
Completeness of the data
Reliability of the data
Elliptic curve labels
Congruent number curves
Picture description

The Manin constant

Theorem (Modularity, version L)

There is an eigenform $f_E \in S_2(\Gamma_0(N))$ with eigenvalues $a_p(E)$ such that

$$L(f_E, s) = L(E, s).$$

In particular, this defines a differential $f_E(q)\mathrm{d}q$ on $X_0(N)$.

Theorem (Modularity, version $X_{\mathbb{Q}}$)

There is a finite morphism $\phi_E : X_0(N) \twoheadrightarrow E$ defined over $\mathbb{Q}$ such that

$$\phi_E^* \omega_E = c_0(E) \cdot f_E(q)\mathrm{d}q,$$

for some positive integer $c_0(E)$.

Conjecturally $c_0(E) = 1$ for all $\Gamma_0(N)$-*optimal* elliptic curves (known in the semistable case!), but the seven exceptions are not $\Gamma_0(N)$-optimal.

A refined conjecture

Conjecture

With no exceptions,

$$\operatorname{ord}_p\left(\frac{c_0(E)\cdot \mathrm{Tam}(E)\cdot \#\text{Ш}(E)}{\#\operatorname{tor}(E)^2}\right) \geq \begin{cases} -3 & \text{if } p = 2, \\ -1 & \text{if } p = 3, 5, 7, \\ 0 & \text{if } p \geq 11. \end{cases}$$

This follows from Lorenzini's theorem, but the bound for $p = 2$ holds for $\operatorname{tor}(E) \cong C_2 \oplus C_{2n}$, and the bound for $p = 3$ holds for $\operatorname{tor}(E) \cong C_3$.

Conjecture

Assume that $\operatorname{tor}(E) \cong C_3$. *Then* $3 \mid c_0(E)\cdot \mathrm{Tam}(E)\cdot \#\text{Ш}(E)$.

I can prove this under the strong Birch–Swinnerton-Dyer conjecture.

Modular symbols

If $f \in S_2(\Gamma_0(N))$ and $p \nmid N$, the Hecke operator T_p acts on periods by

$$(1 + p - T_p) \cdot \int_0^{\infty} f(q)\mathrm{d}q = \sum_{a=1}^{p-1} \int_0^{\frac{a}{p}} f(q)\mathrm{d}q.$$

If $f = f_E$ and p is odd, this says that

$$(1 + p - a_p(E)) \cdot (-L(E,1)) = \frac{\Omega(E)}{c_0(E)} \cdot n, \quad n \in \mathbb{Z}.$$

If the strong Birch–Swinnerton-Dyer conjecture holds,

$$(1 + p - a_p(E)) \cdot \frac{c_0(E) \cdot \mathrm{Tam}(E) \cdot \# Ш(E)}{\# \,\mathrm{tor}(E)^2} \in \mathbb{Z}.$$

If $\mathrm{tor}(E) \cong C_3$, it suffices to find an odd prime $p \nmid N$ such that

$$1 + p - a_p(E) \equiv 3 \mod 9.$$

3-adic Galois images

In terms of $\rho_{E,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_3)$,

$$p = \det(\rho_{E,3}(\mathrm{Fr}_p)), \qquad a_p(E) = \mathrm{tr}(\rho_{E,3}(\mathrm{Fr}_p)).$$

Chebotarev's density theorem says that Fr_p is uniformly distributed in $\mathrm{im}(\rho_{E,3})$, so it suffices to find a matrix $M \in \mathrm{im}(\rho_{E,3})$ such that

$$3 = 1 + \det(M) - \mathrm{tr}(M).$$

Theorem (Rouse–Sutherland–Zureick-Brown, 2022)

Assume that $\mathrm{tor}(E) \cong C_3$. *Then* $\mathrm{im}(\rho_{E,3})$ *is one of the explicit matrix subgroups 3.8.0.1, 3.24.0.1, 9.24.0.1/2, 9.72.0.1/2/3/4/6/7/8/9/10, 27.72.0.1, 27.648.13.25, 27.648.18.1, or 27.1944.55.31/37/43/44.*

Each $\mathrm{im}(\rho_{E,3})$ contains a matrix M such that $3 = 1 + \det(M) - \mathrm{tr}(M)$, except for 9.72.0.1, but Tate's algorithm shows $3 \mid \mathrm{Tam}(E)$ in this case.

Concluding remarks

Theorem (A., 2023)

Assume the 3-part of the strong Birch–Swinnerton-Dyer conjecture. Then

$$\operatorname{ord}_p\left(\frac{c_0(E)\cdot \operatorname{Tam}(E)\cdot \#\text{Ш}(E)}{\#\operatorname{tor}(E)^2}\right) \geq \begin{cases} -3 & \text{if } p = 2, \\ -1 & \text{if } p = 3,5,7, \\ 0 & \text{if } p \geq 11. \end{cases}$$

Note the similarity to a conjecture by Agashe–Stein (2005) that

$$\frac{2\cdot c_0(E)\cdot \operatorname{Tam}(E)\cdot \#\text{Ш}(E)}{\#\operatorname{tor}(E)} \in \mathbb{Z}.$$

This is known for semistable optimal elliptic curves by Melistas (2023), building upon Česnavičius (2018) and Byeon–Kim–Yhee (2020).

Does this generalise to $\mathbb{F}_q(C)$ or $\operatorname{ord}_{s=1} L(E,s) \geq 1$?