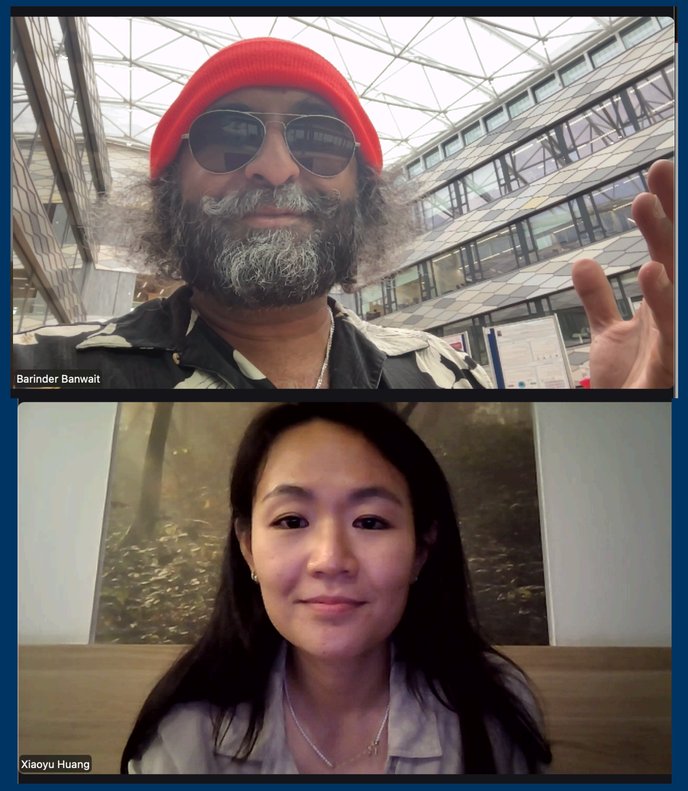
On the identification of elliptic curves that admit infinitely many twists satisfying the Birch--Swinnerton-Dyer conjecture

© Clay Mathematical Institute



XVII ANTS taking over Rijksuniversiteit Groningen

8th July 2026

Peter Swinnerton-Dyer with Bryan Birch, July 2nd 1973, Solihull UK

Barinder S. Banwait, Coco Xiaoyu Huang (Temple)

1958: Computer laboratory at Cambridge gets EDSAC-2

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

They start computing, for various elliptic curves E/Q

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

They start computing, for various elliptic curves E/Q

4. In this section we describe our results. We have applied the methods described in §§ 2, 3 to the curves

(30) $$\Gamma : y^2 = x^3 - Ax - B$$

for all integers A, B with $0 < |A| \leqq 20$, $0 < |B| \leqq 30$; to the curve

(31) $$y^2 = x^3 - D$$

for all integers D with $|D| \leqq 400$; and to the curve

(32) $$y^2 = x^3 - Dx$$

for all integers D with $|D| \leqq 200$. We have also dealt with a few higher ranges of A, B and a few larger values of D. The calculations needed for each curve take very little time; as we had to put a great deal of effort into producing a working program, it would have been uneconomical not to do a lot of cases.

From *Notes on elliptic curves I*, 1963

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

$N_p := \#\tilde{E}(\mathbb{F}_p)$

They start computing, for various elliptic curves E/Q

4. In this section we describe our results. We have applied the methods described in §§ 2, 3 to the curves

(30) $$\Gamma : y^2 = x^3 - Ax - B$$

for all integers A, B with $0 < |A| \leqq 20$, $0 < |B| \leqq 30$; to the curve

(31) $$y^2 = x^3 - D$$

for all integers D with $|D| \leqq 400$; and to the curve

(32) $$y^2 = x^3 - Dx$$

for all integers D with $|D| \leqq 200$. We have also dealt with a few higher ranges of A, B and a few larger values of D. The calculations needed for each curve take very little time; as we had to put a great deal of effort into producing a working program, it would have been uneconomical not to do a lot of cases.

From *Notes on elliptic curves I*, 1963

$$\prod_{p<x} \frac{N_p}{p}$$

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

$N_p := \#\tilde{E}(\mathbb{F}_p)$

They start computing, for various elliptic curves E/Q

4. In this section we describe our results. We have applied the methods described in §§ 2, 3 to the curves

(30) $$\Gamma : y^2 = x^3 - Ax - B$$

for all integers A, B with $0 < |A| \leqq 20$, $0 < |B| \leqq 30$; to the curve

(31) $$y^2 = x^3 - D$$

for all integers D with $|D| \leqq 400$; and to the curve

(32) $$y^2 = x^3 - Dx$$

for all integers D with $|D| \leqq 200$. We have also dealt with a few higher ranges of A, B and a few larger values of D. The calculations needed for each curve take very little time; as we had to put a great deal of effort into producing a working program, it would have been uneconomical not to do a lot of cases.

From *Notes on elliptic curves I*, 1963

$$\prod_{p<x} \frac{N_p}{p}$$

Poor man's *L*-function

© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

$N_p := \#\tilde{E}(\mathbb{F}_p)$

They start computing, for various elliptic curves E/Q

4. In this section we describe our results. We have applied the methods described in §§ 2, 3 to the curves

(30) $$\Gamma : y^2 = x^3 - Ax - B$$

for all integers A, B with $0 < |A| \leqq 20$, $0 < |B| \leqq 30$; to the curve

(31) $$y^2 = x^3 - D$$

for all integers D with $|D| \leqq 400$; and to the curve

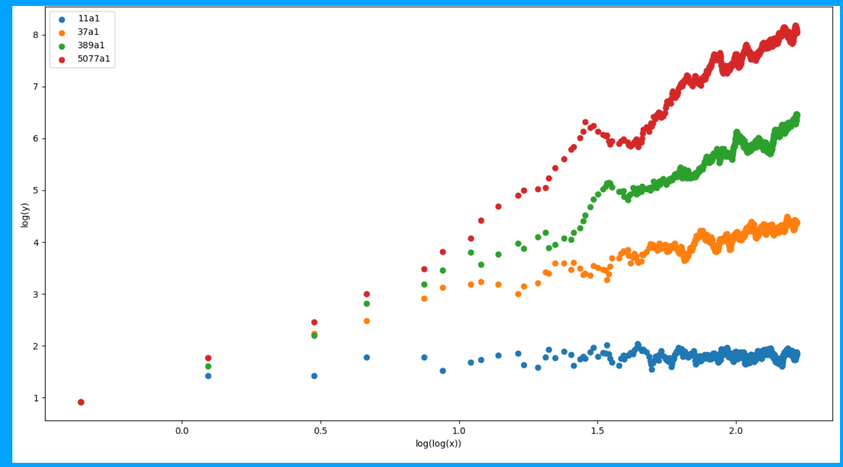
(32) $$y^2 = x^3 - Dx$$

for all integers D with $|D| \leqq 200$. We have also dealt with a few higher ranges of A, B and a few larger values of D. The calculations needed for each curve take very little time; as we had to put a great deal of effort into producing a working program, it would have been uneconomical not to do a lot of cases.

From *Notes on elliptic curves I*, 1963

$$\prod_{p<x} \frac{N_p}{p}$$

Poor man's *L*-function



© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

$r :=$ rank $E(\mathbb{Q})$

$N_p := \#\tilde{E}(\mathbb{F}_p)$

They start computing, for various elliptic curves E/Q

4. In this section we describe our results. We have applied the methods described in §§ 2, 3 to the curves

(30) $$\Gamma : y^2 = x^3 - Ax - B$$

for all integers A, B with $0 < |A| \leqq 20$, $0 < |B| \leqq 30$; to the curve

(31) $$y^2 = x^3 - D$$

for all integers D with $|D| \leqq 400$; and to the curve

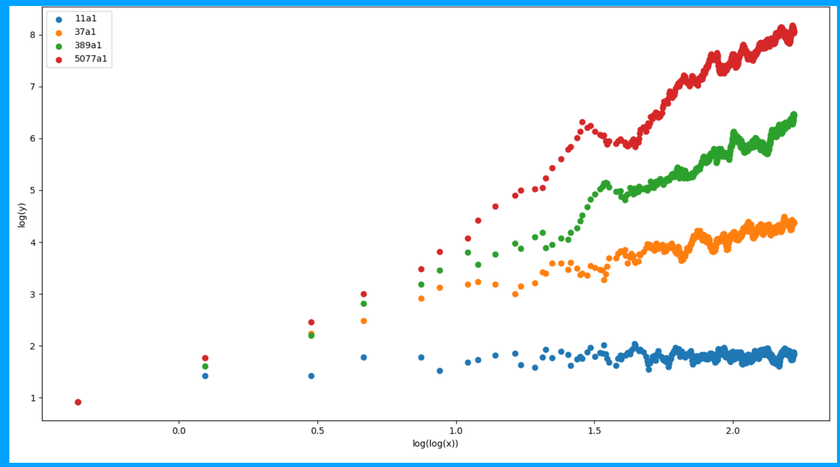
(32) $$y^2 = x^3 - Dx$$

for all integers D with $|D| \leqq 200$. We have also dealt with a few higher ranges of A, B and a few larger values of D. The calculations needed for each curve take very little time; as we had to put a great deal of effort into producing a working program, it would have been uneconomical not to do a lot of cases.

From *Notes on elliptic curves I*, 1963

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

Poor man's *L*-function



© Computer Lab, Cambridge University

1958: Computer laboratory at Cambridge gets EDSAC-2

Swinnerton-Dyer works there on designing operating system to its successor TITAN

Birch arrives back to Cambridge after a year in Princeton

$r :=$ rank $E(\mathbb{Q})$

$N_p := \#\tilde{E}(\mathbb{F}_p)$

They start computing, for various elliptic curves E/Q

4. In this section we describe our results. We have applied the methods described in §§ 2, 3 to the curves

(30) $$\Gamma : y^2 = x^3 - Ax - B$$

for all integers A, B with $0 < |A| \leqq 20$, $0 < |B| \leqq 30$; to the curve

(31) $$y^2 = x^3 - D$$

for all integers D with $|D| \leqq 400$; and to the curve

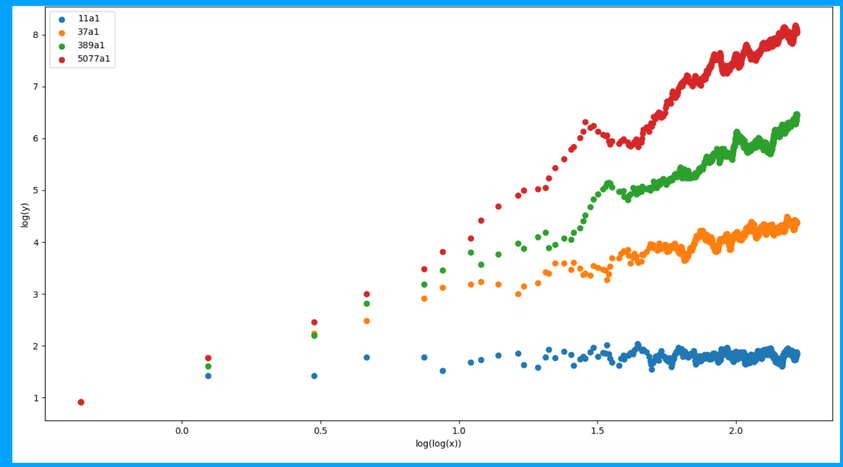
(32) $$y^2 = x^3 - Dx$$

for all integers D with $|D| \leqq 200$. We have also dealt with a few higher ranges of A, B and a few larger values of D. The calculations needed for each curve take very little time; as we had to put a great deal of effort into producing a working program, it would have been uneconomical not to do a lot of cases.

From *Notes on elliptic curves I*, 1963

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

Poor man's *L*-function



Selfie with BJB

"Our application for machine time was approved, with low priority—on certain nights we could use EDSAC from midnight until it broke down, which was typically after a couple of hours." — Bryan Birch

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$a_p = \begin{cases} p+1-N_p & p \nmid N \quad \text{(good reduction)}, \\ 1 & p \mid N, \text{ split multiplicative reduction}, \\ -1 & p \mid N, \text{ non-split multiplicative reduction}, \\ 0 & p \mid N, \text{ additive reduction}. \end{cases}$$

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$a_p = \begin{cases} p+1-N_p & p \nmid N \quad \text{(good reduction)}, \\ 1 & p \mid N, \text{ split multiplicative reduction}, \\ -1 & p \mid N, \text{ non-split multiplicative reduction}, \\ 0 & p \mid N, \text{ additive reduction}. \end{cases}$$

$$L(E,s) := \prod_{p|N} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$a_p = \begin{cases} p+1-N_p & p \nmid N \quad \text{(good reduction)}, \\ 1 & p \mid N, \text{ split multiplicative reduction}, \\ -1 & p \mid N, \text{ non-split multiplicative reduction}, \\ 0 & p \mid N, \text{ additive reduction}. \end{cases}$$

$$L(E,s) := \prod_{p|N} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \qquad (\Re(s) > 3/2)$$

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$a_p = \begin{cases} p+1-N_p & p \nmid N \quad \text{(good reduction)}, \\ 1 & p \mid N, \text{ split multiplicative reduction}, \\ -1 & p \mid N, \text{ non-split multiplicative reduction}, \\ 0 & p \mid N, \text{ additive reduction}. \end{cases}$$

$$L(E,s) := \prod_{p|N} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \qquad (\Re(s) > 3/2)$$

© Clay Mathematical Institute

Conjecture (Birch—Swinnerton-Dyer)

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$a_p = \begin{cases} p+1-N_p & p \nmid N \quad \text{(good reduction)}, \\ 1 & p \mid N, \text{ split multiplicative reduction}, \\ -1 & p \mid N, \text{ non-split multiplicative reduction}, \\ 0 & p \mid N, \text{ additive reduction}. \end{cases}$$

$$L(E,s) := \prod_{p|N} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \qquad (\Re(s) > 3/2)$$

© Clay Mathematical Institute

Conjecture (Birch—Swinnerton-Dyer)

(Weak) $\operatorname{ord}_{s=1} L(E,s) = r_E$

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$a_p = \begin{cases} p+1-N_p & p \nmid N \quad \text{(good reduction)}, \\ 1 & p \mid N, \text{ split multiplicative reduction}, \\ -1 & p \mid N, \text{ non-split multiplicative reduction}, \\ 0 & p \mid N, \text{ additive reduction}. \end{cases}$$

$$L(E,s) := \prod_{p|N} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \qquad (\Re(s) > 3/2)$$

© Clay Mathematical Institute

Conjecture (Birch—Swinnerton-Dyer)

(Weak) $\operatorname{ord}_{s=1} L(E,s) = r_E$

(Strong) $$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

$$\prod_{p<x} \frac{N_p}{p} \to C(\log x)^r$$

$$a_p = \begin{cases} p+1-N_p & p \nmid N \quad \text{(good reduction)}, \\ 1 & p \mid N, \text{ split multiplicative reduction}, \\ -1 & p \mid N, \text{ non-split multiplicative reduction}, \\ 0 & p \mid N, \text{ additive reduction}. \end{cases}$$

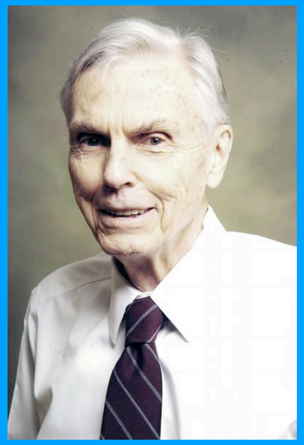
$$L(E,s) := \prod_{p|N} (1 - a_p p^{-s})^{-1} \cdot \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \qquad (\Re(s) > 3/2)$$

© Clay Mathematical Institute

Conjecture (Birch—Swinnerton-Dyer)

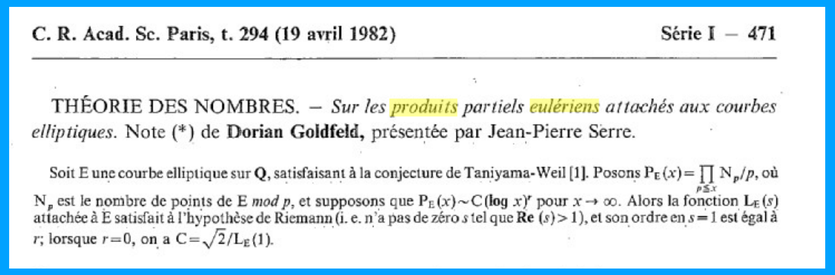
(Weak) $\operatorname{ord}_{s=1} L(E,s) = r_E$

(Strong) $$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathrm{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$



© Uni Texas at Austin

This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite! — John Tate,1974



C. R. Acad. Sc. Paris, t. 294 (19 avril 1982) Série I – 471

THÉORIE DES NOMBRES. – *Sur les produits partiels eulériens attachés aux courbes elliptiques.* Note (*) de **Dorian Goldfeld,** présentée par Jean-Pierre Serre.

Soit E une courbe elliptique sur **Q**, satisfaisant à la conjecture de Taniyama-Weil [1]. Posons $P_E(x)=\prod_{p\leq x} N_p/p$, où N_p est le nombre de points de E *mod p*, et supposons que $P_E(x)\sim C(\log x)^r$ pour $x\to\infty$. Alors la fonction $L_E(s)$ attachée à E satisfait à l'hypothèse de Riemann (i. e. n'a pas de zéro *s* tel que **Re** $(s)>1$), et son ordre en $s=1$ est égal à *r*; lorsque $r=0$, on a $C=\sqrt{2}/L_E(1)$.

$$\prod_{p<x}\frac{N_p}{p}\ \to\ C(\log x)^r$$

$$a_p=\begin{cases} p+1-N_p & p\nmid N \quad \text{(good reduction)},\\ 1 & p\mid N,\ \text{split multiplicative reduction},\\ -1 & p\mid N,\ \text{non-split multiplicative reduction},\\ 0 & p\mid N,\ \text{additive reduction}. \end{cases}$$

$$L(E,s):=\prod_{p\mid N}(1-a_p p^{-s})^{-1}\cdot\prod_{p\nmid N}(1-a_p p^{-s}+p^{1-2s})^{-1} \qquad (\Re(s)>3/2)$$

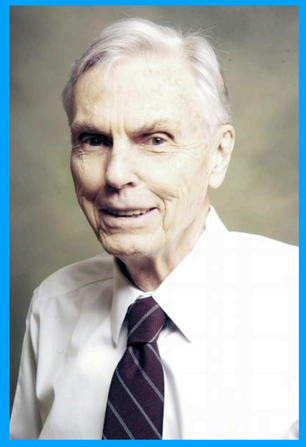
© Clay Mathematical Institute

Conjecture (Birch—Swinnerton-Dyer)

(Weak) $\operatorname{ord}_{s=1}L(E,s)=r_E$

(Strong) $$\frac{L^{(r)}(E,1)}{r!}=\frac{\Omega(E/\mathbb{Q})\cdot \mathrm{Reg}(E/\mathbb{Q})\cdot|Ш(E/\mathbb{Q})|\cdot\prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

This remarkable conjecture relates the behavior of a function L at a point where it is not at present known to be defined to the order of a group Ш which is not known to be finite! — John Tate,1974



© Uni Texas at Austin

What are the known cases of BSD?

What are the known cases of BSD?

© Harvard University

Benedict H. Gross

(7.3) **Theorem.** *Assume that* $L(E,1)=0$. *Then there is a rational point* P *in* $E(\mathbb{Q})$ *such that* $L'(E,1)=\alpha\cdot\Omega\cdot\langle P,P\rangle$ *with* $\alpha\in\mathbb{Q}^\times$. *In particular:*

1) *If* $L'(E,1)\neq 0$, *then* $E(\mathbb{Q})$ *contains elements of infinite order.*

2) *If* $L'(E,1)\neq 0$ *and* $\operatorname{rank} E(\mathbb{Q})=1$, *then formula* (7.2) *is true for some non-zero rational number* α.

© Alchetron

Don B. Zagier

What are the known cases of BSD?

© Harvard University

Benedict H. Gross

(7.3) **Theorem.** *Assume that* $L(E,1)=0$. *Then there is a rational point* P *in* $E(\mathbb{Q})$ *such that* $L'(E,1)=\alpha\cdot\Omega\cdot\langle P,P\rangle$ *with* $\alpha\in\mathbb{Q}^\times$. *In particular:*

1) *If* $L'(E,1)\neq 0$, *then* $E(\mathbb{Q})$ *contains elements of infinite order.*

2) *If* $L'(E,1)\neq 0$ *and* $\operatorname{rank} E(\mathbb{Q})=1$, *then formula* (7.2) *is true for some non-zero rational number* α.

© Alchetron

Don B. Zagier

СЕРИЯ МАТЕМАТИЧЕСКАЯ Том 52, № 3, 1988

УДК 519.4

КОЛЫВАГИН В. А.

КОНЕЧНОСТЬ $E(\mathbf{Q})$ И $Ш(E,\mathbf{Q})$ ДЛЯ ПОДКЛАССА КРИВЫХ ВЕЙЛЯ

Введение

Пусть E — эллиптическая кривая, определенная над полем рациональных чисел $\mathbf{Q}$, $L(E,\mathbf{Q},s)=\sum_{n=1}^{\infty} a_n n^{-s}$, $a_n\in\mathbf{Z}$ — каноническая L-функция E над $\mathbf{Q}$. Гипотеза Берча — Суиннертона — Дайера утверждает, что ранг

© CUNY

What are the known cases of BSD?

© Harvard University

Benedict H. Gross

(7.3) **Theorem.** *Assume that* $L(E,1)=0$. *Then there is a rational point* P *in* $E(\mathbb{Q})$ *such that* $L'(E,1)=\alpha\cdot\Omega\cdot\langle P,P\rangle$ *with* $\alpha\in\mathbb{Q}^\times$. *In particular:*

1) *If* $L'(E,1)\neq 0$, *then* $E(\mathbb{Q})$ *contains elements of infinite order.*

2) *If* $L'(E,1)\neq 0$ *and* $\operatorname{rank} E(\mathbb{Q})=1$, *then formula* (7.2) *is true for some non-zero rational number* α.

© Alchetron

Don B. Zagier

СЕРИЯ МАТЕМАТИЧЕСКАЯ Том 52, № 3, 1988

УДК 519.4

КОЛЫВАГИН В. А.

КОНЕЧНОСТЬ $E(\mathbf{Q})$ И $Ш(E,\mathbf{Q})$ ДЛЯ ПОДКЛАССА КРИВЫХ ВЕЙЛЯ

Введение

Пусть E — эллиптическая кривая, определенная над полем рациональных чисел $\mathbf{Q}$, $L(E,\mathbf{Q},s)=\sum_{n=1}^{\infty} a_n n^{-s}$, $a_n\in\mathbf{Z}$ — каноническая L-функция E над $\mathbf{Q}$. Гипотеза Берча — Суиннертона — Дайера утверждает, что ранг

© CUNY

Theorem (Gross—Zagier, Kolyvagin). If $r_{an}\leq 1$, then weak BSD is true.

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

What about Strong BSD? (If $r_{an} \leq 1$)

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

What about Strong BSD? (If $r_{an} \leq 1$)

Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Mathematics of Computation 78 (2009), no. 268, 2397–2425.

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

What about Strong BSD? (If $r_{an} \leq 1$)

Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Mathematics of Computation 78 (2009), no. 268, 2397–2425.

Robert L. Miller, Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one, LMS Journal of Computation and Mathematics 14 (2011), 327–350.

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

What about Strong BSD? (If $r_{an} \leq 1$)

Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Mathematics of Computation 78 (2009), no. 268, 2397–2425.

Robert L. Miller, Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one, LMS Journal of Computation and Mathematics 14 (2011), 327–350.

Brendan Creutz and Robert L. Miller, Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula, Journal of Algebra 372 (2012), 673–701.

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

What about Strong BSD? (If $r_{an} \leq 1$)

Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Mathematics of Computation 78 (2009), no. 268, 2397–2425.

Robert L. Miller, Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one, LMS Journal of Computation and Mathematics 14 (2011), 327–350.

Brendan Creutz and Robert L. Miller, Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula, Journal of Algebra 372 (2012), 673–701.

Robert Miller and Michael Stoll, Explicit isogeny descent on elliptic curves, Mathematics of Computation 82 (2013), no. 281, 513–529

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

What about Strong BSD? (If $r_{an} \leq 1$)

Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Mathematics of Computation 78 (2009), no. 268, 2397–2425.

Robert L. Miller, Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one, LMS Journal of Computation and Mathematics 14 (2011), 327–350.

Brendan Creutz and Robert L. Miller, Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula, Journal of Algebra 372 (2012), 673–701.

Robert Miller and Michael Stoll, Explicit isogeny descent on elliptic curves, Mathematics of Computation 82 (2013), no. 281, 513–529

Tyler Lawson and Christian Wuthrich, Vanishing of some Galois cohomology groups for elliptic curves, Elliptic Curves, Modular Forms and Iwasawa Theory — Conference in Honour of the 70th Birthday of John Coates (David Loeffler and Sarah Livia Zerbes, eds.), Springer, 2016, pp. 373–399.

Theorem (Gross—Zagier, Kolyvagin). If $r_{an} \leq 1$, then weak BSD is true.

What about Strong BSD? (If $r_{an} \leq 1$)

Grigor Grigorov, Andrei Jorza, Stefan Patrikis, William Stein, and Corina Tarniţă, Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves, Mathematics of Computation 78 (2009), no. 268, 2397–2425.

Robert L. Miller, Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one, LMS Journal of Computation and Mathematics 14 (2011), 327–350.

Brendan Creutz and Robert L. Miller, Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula, Journal of Algebra 372 (2012), 673–701.

Robert Miller and Michael Stoll, Explicit isogeny descent on elliptic curves, Mathematics of Computation 82 (2013), no. 281, 513–529

Tyler Lawson and Christian Wuthrich, Vanishing of some Galois cohomology groups for elliptic curves, Elliptic Curves, Modular Forms and Iwasawa Theory — Conference in Honour of the 70th Birthday of John Coates (David Loeffler and Sarah Livia Zerbes, eds.), Springer, 2016, pp. 373–399.

Theorem. Strong BSD is known if $r_{an} \leq 1$ and $N_E \leq 5{,}000$

Proceeds by verifying BSD(E, p)

Proceeds by verifying BSD(E, p)

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

Proceeds by verifying BSD(E, p)

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

$$\frac{L^{(r)}(E,1)}{r!} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p} = |Ш(E/\mathbb{Q})|$$

Proceeds by verifying BSD(E, p)

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

$$|Ш_{\mathrm{an}}(E/\mathbb{Q})| := \frac{L^{(r)}(E,1)}{r!} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p} = |Ш(E/\mathbb{Q})|$$

Proceeds by verifying BSD(E, p)

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

$$|Ш_{\mathrm{an}}(E/\mathbb{Q})| := \frac{L^{(r)}(E,1)}{r!} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p} = |Ш(E/\mathbb{Q})|$$

BSD(E, p) is the statement:

Proceeds by verifying BSD(E, p)

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

$$|Ш_{\mathrm{an}}(E/\mathbb{Q})| := \frac{L^{(r)}(E,1)}{r!} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p} = |Ш(E/\mathbb{Q})|$$

BSD(E, p) is the statement: $\mathsf{ord}_p\left(|Ш_{\mathrm{an}}(E/\mathbb{Q})|\right) = \mathsf{ord}_p\left(|Ш(E/\mathbb{Q})|\right)$

Proceeds by verifying BSD(E, p)

$$\frac{L^{(r)}(E,1)}{r!} = \frac{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot |Ш(E/\mathbb{Q})| \cdot \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}.$$

$$|Ш_{\mathrm{an}}(E/\mathbb{Q})| := \frac{L^{(r)}(E,1)}{r!} \cdot \frac{|E(\mathbb{Q})_{\mathrm{tors}}|^2}{\Omega(E/\mathbb{Q}) \cdot \mathsf{Reg}(E/\mathbb{Q}) \cdot \prod_p c_p} = |Ш(E/\mathbb{Q})|$$

BSD(E, p) is the statement: $\mathsf{ord}_p\left(|Ш_{\mathrm{an}}(E/\mathbb{Q})|\right) = \mathsf{ord}_p\left(|Ш(E/\mathbb{Q})|\right)$

© MFO

Karl Rubin

Theorem 11.1. *Suppose E is as above and Ш is the Tate-Shafarevich group of E over K.*

(i) If $L(\bar{\psi}, 1) \neq 0$ then $E(K)$ is finite, Ш is finite, and for all primes $\mathfrak{p}$ of K not dividing $\#(\mathcal{O}^\times)$,

$$\#(Ш_{\mathfrak{p}^\infty}) = \mathbf{N}(\mathfrak{p})^{m(\mathfrak{p})} \text{ where } m(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}\left(\#(E(K))\frac{L(\bar{\psi}, 1)}{\Omega}\right).$$

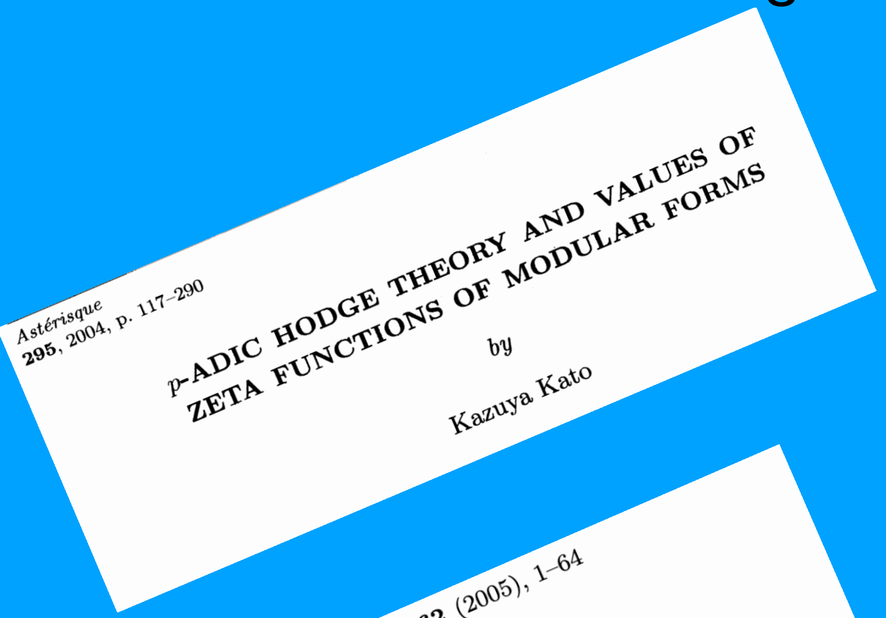
In other words, Gross' refinement [9] of the Birch and Swinnerton-Dyer conjecture for E is true up to powers of primes dividing $\#(\mathcal{O}^\times)$.

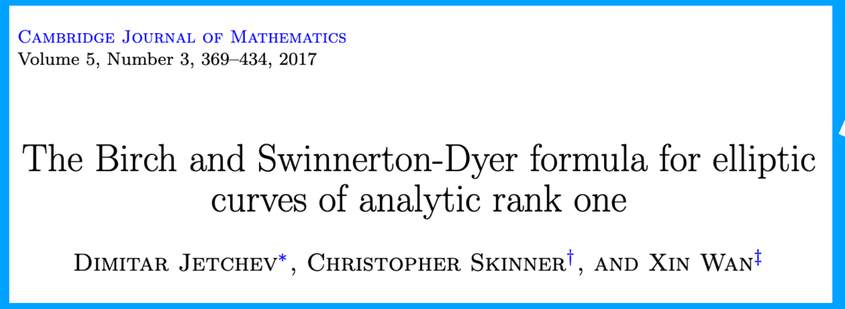
The 'main conjectures' of Iwasawa theory for imaginary quadratic fields, 1991

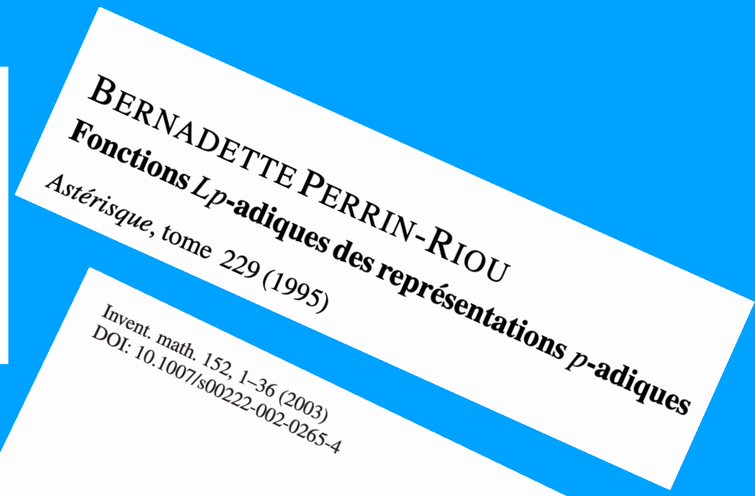
Since Rubin, there's been lots of development towards the Iwasawa main conjecture that I don't have time to get into:

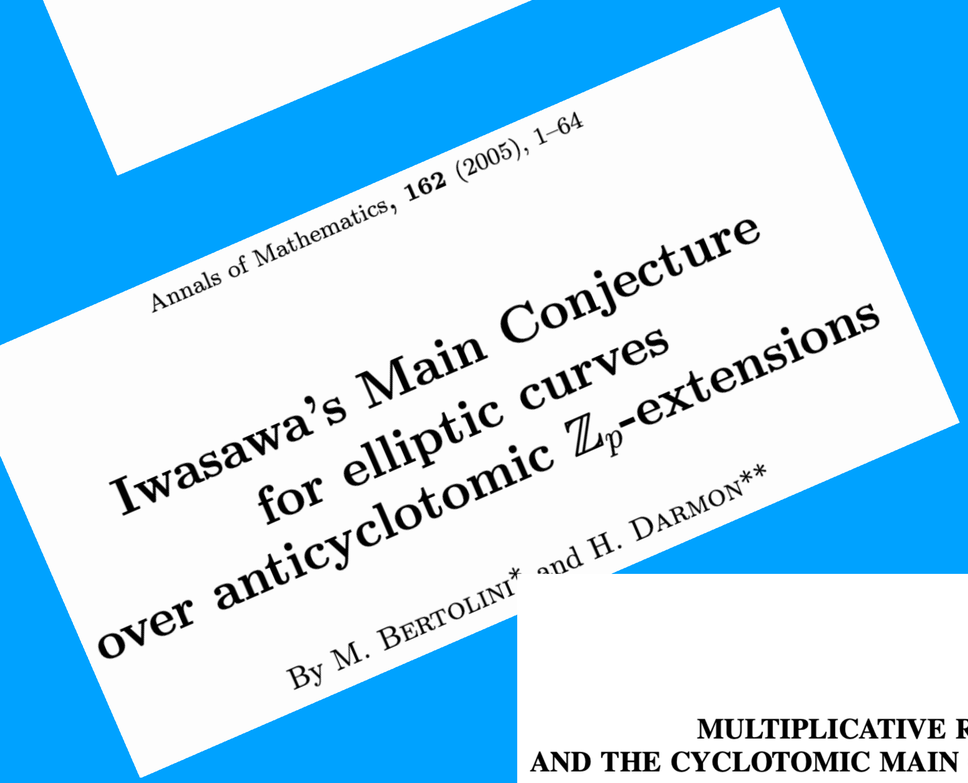
.....

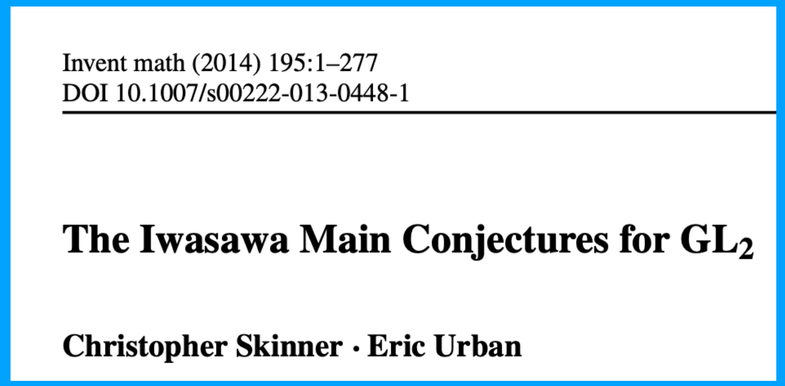
Since Rubin, there's been lots of development towards the Iwasawa main conjecture that I don't have time to get into:

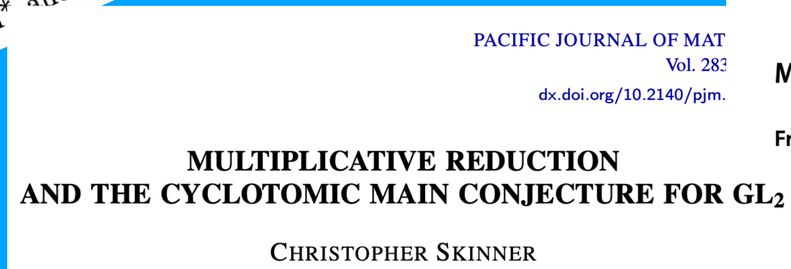


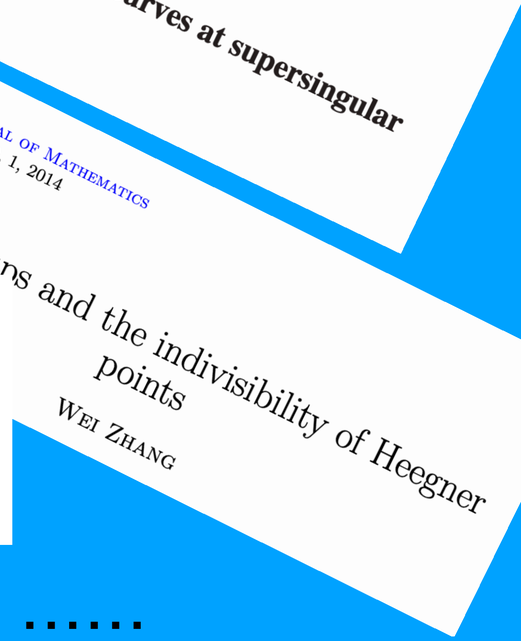












. . . . . .

[math.NT] 11 Sep 2024

ZETA ELEMENTS FOR ELLIPTIC CURVES AND APPLICATIONS

ASHAY A. BURUNGALE, CHRISTOPHER SKINNER, YE TIAN AND XIN WAN

ABSTRACT. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and $p \nmid 2N$ a prime. Let L be an imaginary quadratic field with p split. We prove the existence of p-adic zeta element for E over L, encoding two different p-adic L-functions associated to E over L via explicit reciprocity laws at the primes above p. We formulate a main conjecture for E over L in terms of the zeta element, mediating different main conjectures in which the p-adic L-functions appear, and prove some results toward them.

The zeta element has various applications to the arithmetic of elliptic curves. This includes a proof of main conjecture for semistable elliptic curves E over $\mathbb{Q}$ at supersingular primes p, as conjectured by Kobayashi in 2002. It leads to the p-part of the conjectural Birch and Swinnerton-Dyer (BSD) formula for such curves of analytic rank zero or one, and enables us to present the first infinite families of non-CM elliptic curves for which the BSD conjecture is true. We provide further evidence towards the BSD conjecture: new cases of p-converse to the Gross–Zagier and Kolyvagin theorem, and p-part of the BSD formula for ordinary primes p. Along the way, we give a proof of a conjecture of Perrin-Riou connecting Beilinson–Kato elements with rational points.

ZETA ELEMENTS FOR ELLIPTIC CURVES AND APPLICATIONS

ASHAY A. BURUNGALE, CHRISTOPHER SKINNER, YE TIAN AND XIN WAN

[math.NT] 11 Sep 2024

ABSTRACT. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and $p \nmid 2N$ a prime. Let L be an imaginary quadratic field with p split. We prove the existence of p-adic zeta element for E over L, encoding two different p-adic L-functions associated to E over L via explicit reciprocity laws at the primes above p. We formulate a main conjecture for E over L in terms of the zeta element, mediating different main conjectures in which the p-adic L-functions appear, and prove some results toward them.

The zeta element has various applications to the arithmetic of elliptic curves. This includes a proof of main conjecture for semistable elliptic curves E over $\mathbb{Q}$ at supersingular primes p, as conjectured by Kobayashi in 2002. It leads to the p-part of the conjectural Birch and Swinnerton-Dyer (BSD) formula for such curves of analytic rank zero or one, and enables us to present the first infinite families of non-CM elliptic curves for which the BSD conjecture is true. We provide further evidence towards the BSD conjecture: new cases of p-converse to the Gross–Zagier and Kolyvagin theorem, and p-part of the BSD formula for ordinary primes p. Along the way, we give a proof of a conjecture of Perrin-Riou connecting Beilinson–Kato elements with rational points.

For CM curves,

ZETA ELEMENTS FOR ELLIPTIC CURVES AND APPLICATIONS

ASHAY A. BURUNGALE, CHRISTOPHER SKINNER, YE TIAN AND XIN WAN

n.NT] 11 Sep 2024

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and $p \nmid 2N$ a prime. Let L be an imaginary quadratic field with p split. We prove the existence of p-adic zeta element for E over L, encoding two different p-adic L-functions associated to E over L via explicit reciprocity laws at the primes above p. We formulate a main conjecture for E over L in terms of the zeta element, mediating different main conjectures in which the p-adic L-functions appear, and prove some results toward them.

The zeta element has various applications to the arithmetic of elliptic curves. This includes a proof of main conjecture for semistable elliptic curves E over $\mathbb{Q}$ at supersingular primes p, as conjectured by Kobayashi in 2002. It leads to the p-part of the conjectural Birch and Swinnerton-Dyer (BSD) formula for such curves of analytic rank zero or one, and enables us to present the first infinite families of non-CM elliptic curves for which the BSD conjecture is true. We provide further evidence towards the BSD conjecture: new cases of p-converse to the Gross–Zagier and Kolyvagin theorem, and p-part of the BSD formula for ordinary primes p. Along the way, we give a proof of a conjecture of Perrin-Riou connecting Beilinson–Kato elements with rational points.

For CM curves,

Proc. London Math. Soc. Page 1 of 38 © 2014 London Mathematical Society
doi:10.1112/plms/pdu059

Quadratic Twists of elliptic curves

John Coates, Yongxiong Li, Ye Tian and Shuai Zhai

For Bryan Birch and Peter Swinnerton-Dyer

ZETA ELEMENTS FOR ELLIPTIC CURVES AND APPLICATIONS

ASHAY A. BURUNGALE, CHRISTOPHER SKINNER, YE TIAN AND XIN WAN

.NT] 11 Sep 2024

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and $p \nmid 2N$ a prime. Let L be an imaginary quadratic field with p split. We prove the existence of p-adic zeta element for E over L, encoding two different p-adic L-functions associated to E over L via explicit reciprocity laws at the primes above p. We formulate a main conjecture for E over L in terms of the zeta element, mediating different main conjectures in which the p-adic L-functions appear, and prove some results toward them.

The zeta element has various applications to the arithmetic of elliptic curves. This includes a proof of main conjecture for semistable elliptic curves E over $\mathbb{Q}$ at supersingular primes p, as conjectured by Kobayashi in 2002. It leads to the p-part of the conjectural Birch and Swinnerton-Dyer (BSD) formula for such curves of analytic rank zero or one, and enables us to present the first infinite families of non-CM elliptic curves for which the BSD conjecture is true. We provide further evidence towards the BSD conjecture: new cases of p-converse to the Gross–Zagier and Kolyvagin theorem, and p-part of the BSD formula for ordinary primes p. Along the way, we give a proof of a conjecture of Perrin-Riou connecting Beilinson–Kato elements with rational points.

ZETA ELEMENTS FOR ELLIPTIC CURVES AND APPLICATIONS

ASHAY A. BURUNGALE, CHRISTOPHER SKINNER, YE TIAN AND XIN WAN

.NT] 11 Sep 2024

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N and $p \nmid 2N$ a prime. Let L be an imaginary quadratic field with p split. We prove the existence of p-adic zeta element for E over L, encoding two different p-adic L-functions associated to E over L via explicit reciprocity laws at the primes above p. We formulate a main conjecture for E over L in terms of the zeta element, mediating different main conjectures in which the p-adic L-functions appear, and prove some results toward them.

The zeta element has various applications to the arithmetic of elliptic curves. This includes a proof of main conjecture for semistable elliptic curves E over $\mathbb{Q}$ at supersingular primes p, as conjectured by Kobayashi in 2002. It leads to the p-part of the conjectural Birch and Swinnerton-Dyer (BSD) formula for such curves of analytic rank zero or one, and enables us to present the first infinite families of non-CM elliptic curves for which the BSD conjecture is true. We provide further evidence towards the BSD conjecture: new cases of p-converse to the Gross–Zagier and Kolyvagin theorem, and p-part of the BSD formula for ordinary primes p. Along the way, we give a proof of a conjecture of Perrin-Riou connecting Beilinson–Kato elements with rational points.

Theorem 1.7. *Let E be an elliptic curve of conductor N denoted by* 46a1, 62a1, 66b1, 69a1, 77c1, 94a1, 105a1, 106d1, 114b1, 115a1, 118c1, 118d1, 141b1, 141c1, 141e1 *or* 142c1 *in Cremona's labelling. Let $M > 1$ be a square-free integer with $(M, N) = 1$ and E^M the quadratic twist of E by the character associated to the extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold:*

(a) *$L(1, E^M) \neq 0$, and*
(b) *E has ordinary reduction at the primes dividing M.*

Then the BSD conjecture holds for E^M, i.e. $E^M(\mathbb{Q})$ and $Ш(E^M)$ are finite, and

$$\frac{L(1, E^M)}{\Omega_{E^M}} = \frac{\#Ш(E^M) \cdot \prod_{\ell \nmid \infty} c_\ell(E^M)}{\#E^M(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Moreover, the conditions (a) and (b) are satisfied by infinitely many M.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) $a_3(E) = 0$,
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) *$a_3(E) = 0$,*
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) $a_3(E) = 0$,
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) *$a_3(E) = 0$,*
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

THEOREM 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) *$Ш(E')[2] = 0$;*
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) $a_3(E) = 0$,
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

THEOREM 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) *$Ш(E')[2] = 0$;*
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) *$a_3(E) = 0$,*
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

Our proof of this theorem is based on Theorem 1.5 and prior work on the p-part of the BSD formula. The existence of infinitely many M satisfying the conditions (a) and (b) relies on [41, 148].

THEOREM 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) *$Ш(E')[2] = 0$;*
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) *$a_3(E) = 0$,*
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

Our proof of this theorem is based on Theorem 1.5 and prior work on the p-part of the BSD formula. The existence of infinitely many M satisfying the conditions (a) and (b) relies on [41, 148].

THEOREM 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) *$Ш(E')[2] = 0$;*
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) *$a_3(E) = 0$,*
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

Our proof of this theorem is based on Theorem 1.5 and prior work on the p-part of the BSD formula. The existence of infinitely many M satisfying the conditions (a) and (b) relies on [41, 148].

[22] We are grateful to Shuai Zhai for his assistance in finding these examples.

THEOREM 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) *$Ш(E')[2] = 0$;*
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) *$a_3(E) = 0$,*
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

Our proof of this theorem is based on Theorem 1.5 and prior work on the p-part of the BSD formula. The existence of infinitely many M satisfying the conditions (a) and (b) relies on [41, 148].

[22] We are grateful to Shuai Zhai for his assistance in finding these examples.

THEOREM 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) *$Ш(E')[2] = 0$;*
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

10.4.3. *The Birch and Swinnerton-Dyer formula: a rank zero quadratic twist family.*

Theorem 10.12. *Let E be a semistable elliptic curve defined over $\mathbb{Q}$ with conductor N, and $M > 1$ a square-free integer with $(M, N) = 1$. Let $E^{(M)}$ denote the quadratic twist of E by the character associated to the quadratic extension $\mathbb{Q}(\sqrt{M})/\mathbb{Q}$. Suppose that the following conditions hold.*

(i) *We have*
$$L(1, E^{(M)}) \neq 0,$$
(ii) *The 2-part of the BSD formula holds for $E^{(M)}$,*
(iii) *$a_3(E) = 0$,*
(iv) *For all odd primes p, $E[p]$ is an absolutely irreducible $G_{\mathbb{Q}}$-representation,*
(v) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified,*
(vi) *E has ordinary reduction at prime divisors of M.*

Then the Birch and Swinnerton-Dyer conjecture is true for $E^{(M)}$, that is, $E^{(M)}(\mathbb{Q})$ and $Ш(E^{(M)})$ are finite, and
$$\frac{L(1, E^{(M)})}{\Omega_{E^{(M)}}} = \frac{\#Ш(E^{(M)}) \cdot \prod_{\ell \nmid \infty} c_\ell(E^{(M)})}{\#E^{(M)}(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Example 1. For semistable elliptic curves E up to conductor 150, the conditions of Theorem 10.12 are satisfied by[22] the curves denoted in the LMFDB database by

- 46a1, 69a1, 77c1, 94a1, 114b1, 141b1 and 142c1,
- 62a1, 66b1, 105a1, 106d1, 115a1, 118c1, 118d1, 141c1 and 141e1

for infinitely many M. Here for the elliptic curves in the first bullet point we rely on [41, Thm. 1.5] for the conditions (i)-(ii), and for the curves in the second bullet point on [148, Thm. 1]. This gives the first infinite families of non-CM elliptic curves satisfying the Birch and Swinnerton-Dyer conjecture.

Why stop at 150?

Our proof of this theorem is based on Theorem 1.5 and prior work on the p-part of the BSD formula. The existence of infinitely many M satisfying the conditions (a) and (b) relies on [41, 148].

[22] We are grateful to Shuai Zhai for his assistance in finding these examples.

THEOREM 1.5. *Let E and M be as in Theorem 1.1. Assume further that*

(1) *$Ш(E')[2] = 0$;*
(2) *all primes ℓ which divide $2C$ split in $\mathbb{Q}(\sqrt{M})$;*
(3) *the 2-part of the Birch and Swinnerton-Dyer conjecture holds for E.*

Then the 2-primary component of $Ш(E^{(M)})$ is zero, and the 2-part of the Birch and Swinnerton-Dyer conjecture holds for $E^{(M)}$.

What we did (1/2)

What we did (1/2)

We extended 150 to 500,000. This required:

What we did (1/2)

We extended 150 to 500,000. This required:

1. Carefully collecting the conditions from: BSTW, CLZ, Z, SU, S, CGS

What we did (1/2)

We extended 150 to 500,000. This required:

IWASAWA-LAND

1. Carefully collecting the conditions from:(BSTW, CLZ, Z, SU, S, CGS)

What we did (1/2)

We extended 150 to 500,000. This required:

IWASAWA-LAND

1. Carefully collecting the conditions from:(BSTW, CLZ, Z, SU, S, CGS)
2. Actually proving and identifying infinitude of twists

What we did (1/2)

We extended 150 to 500,000. This required:

IWASAWA-LAND

1. Carefully collecting the conditions from:(BSTW, CLZ, Z, SU, S, CGS)

2. Actually proving and identifying infinitude of twists

Theorem 2.18. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N that satisfies the following conditions:*

(1) *E is semistable.*
(2) *$a_3(E) \in \{-2, -1, 0, 1, 2\}$.*
(3) *E does not admit a rational p-isogeny for $p \in \{3, 5, 7\}$.*
(4) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified.*
(5) *E is optimal in its isogeny class.*
(6) *E has analytic rank 0.*
(7) *$\mathrm{BSD}(E, 2)$ is true.*
(8) *One of the following two sets of conditions hold.*
  (a) *$E(\mathbb{Q})[2] = 0$, $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 0$*
  (b) *$E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$; $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = -1$; writing $E : y^2 = f(x)$ and the 2-torsion point as $(x_0, 0)$, none of $f'(x_0)$, $-f'(x_0)$ or $-\Delta_E$ are squares in $\mathbb{Q}$; $Ш(E')[2] = 0$, where $E' := E/E(\mathbb{Q})[2]$ is the 2-isogenous curve of E.*

What we did (1/2)

We extended 150 to 500,000. This required:

IWASAWA-LAND

1. Carefully collecting the conditions from:(BSTW, CLZ, Z, SU, S, CGS)

2. Actually proving and identifying infinitude of twists

Theorem 2.18. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N that satisfies the following conditions:*

(1) E is semistable.
(2) $a_3(E) \in \{-2, -1, 0, 1, 2\}$.
(3) E does not admit a rational p-isogeny for $p \in \{3, 5, 7\}$.
(4) For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified.
(5) E is optimal in its isogeny class.
(6) E has analytic rank 0.
(7) $\mathrm{BSD}(E, 2)$ is true.
(8) One of the following two sets of conditions hold.
  (a) $E(\mathbb{Q})[2] = 0$, $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 0$
  (b) $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$; $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = -1$; writing $E : y^2 = f(x)$ and the 2-torsion point as $(x_0, 0)$, none of $f'(x_0)$, $-f'(x_0)$ or $-\Delta_E$ are squares in $\mathbb{Q}$; $Ш(E')[2] = 0$, where $E' := E/E(\mathbb{Q})[2]$ is the 2-isogenous curve of E.

Then there exist infinitely many squarefree integers d satisfying the following:

What we did (1/2)

We extended 150 to 500,000. This required:

IWASAWA-LAND

1. Carefully collecting the conditions from:(BSTW, CLZ, Z, SU, S, CGS)

2. Actually proving and identifying infinitude of twists

Theorem 2.18. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N that satisfies the following conditions:*

(1) *E is semistable.*
(2) *$a_3(E) \in \{-2, -1, 0, 1, 2\}$.*
(3) *E does not admit a rational p-isogeny for $p \in \{3, 5, 7\}$.*
(4) *For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified.*
(5) *E is optimal in its isogeny class.*
(6) *E has analytic rank 0.*
(7) *$\mathrm{BSD}(E, 2)$ is true.*
(8) *One of the following two sets of conditions hold.*
  (a) *$E(\mathbb{Q})[2] = 0$, $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 0$*
  (b) *$E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$; $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = -1$; writing $E : y^2 = f(x)$ and the 2-torsion point as $(x_0, 0)$, none of $f'(x_0)$, $-f'(x_0)$ or $-\Delta_E$ are squares in $\mathbb{Q}$; $Ш(E')[2] = 0$, where $E' := E/E(\mathbb{Q})[2]$ is the 2-isogenous curve of E.*

Then there exist infinitely many squarefree integers d satisfying the following:

(1) *$(d, 3N) = 1$.*
(2) *$d \equiv 1 \pmod 4$.*
(3) *E has ordinary reduction at prime divisors of d.*
(4) *(a) in Item 8a, for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E; for every $p \mid N$, p splits in $\mathbb{Q}(\sqrt{d})$; if $\Delta_E > 0$, then $d > 0$.*
  (b) in Item 8b, for every $p|d$, $p \equiv 1 \pmod 4$, and $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$; and for every $p \mid 2N$, p splits in $\mathbb{Q}(\sqrt{d})$.

What we did (1/2)

We extended 150 to 500,000. This required:

IWASAWA-LAND

1. Carefully collecting the conditions from:(BSTW, CLZ, Z, SU, S, CGS)

2. Actually proving and identifying infinitude of twists

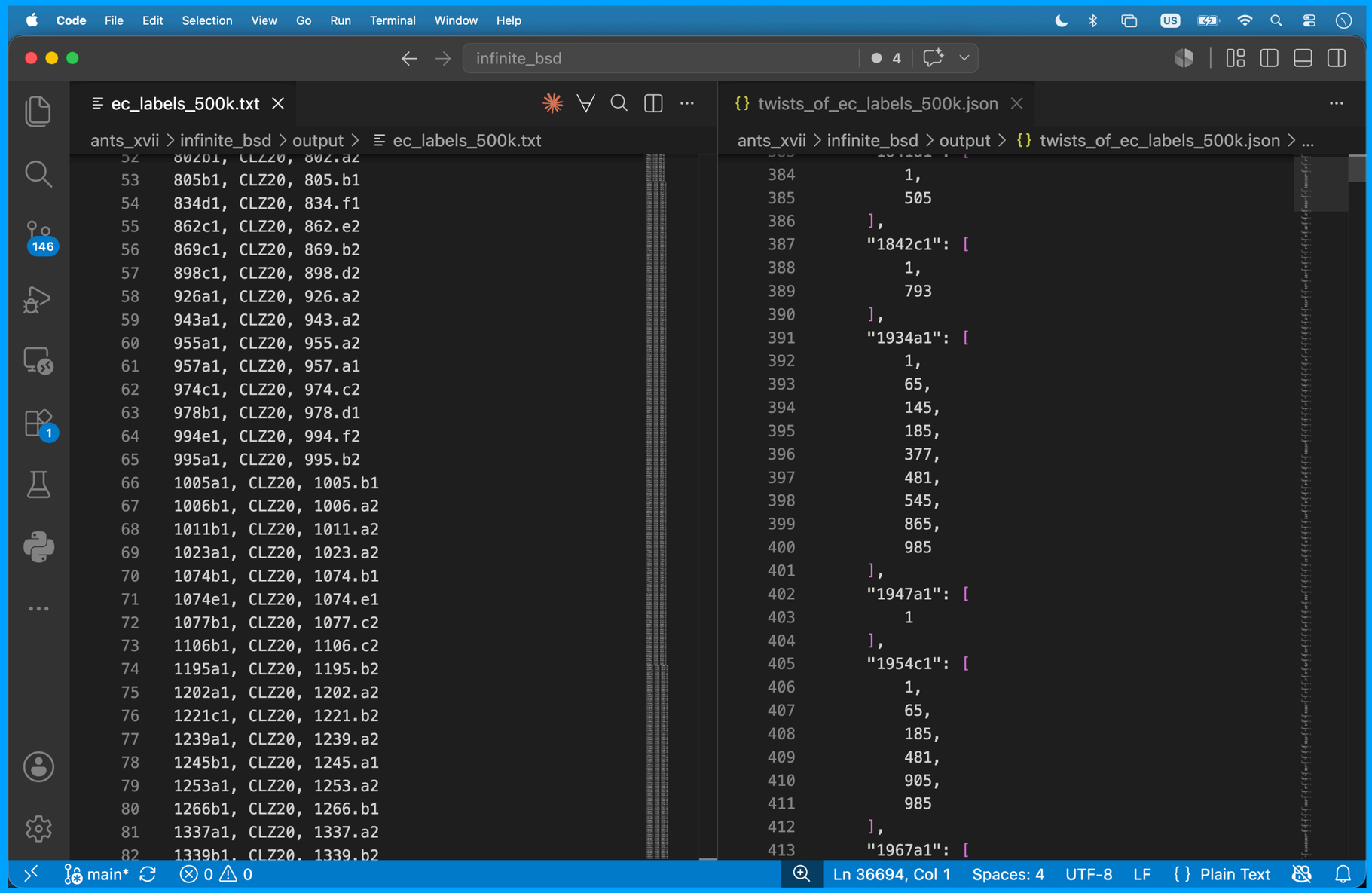
Theorem 2.18. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N that satisfies the following conditions:*

(1) E is semistable.
(2) $a_3(E) \in \{-2, -1, 0, 1, 2\}$.
(3) E does not admit a rational p-isogeny for $p \in \{3, 5, 7\}$.
(4) For any prime $p|N$, there exists a multiplicative prime $q \neq p$ at which $E[p]$ is ramified.
(5) E is optimal in its isogeny class.
(6) E has analytic rank 0.
(7) $\mathrm{BSD}(E, 2)$ is true.
(8) One of the following two sets of conditions hold.
  (a) $E(\mathbb{Q})[2] = 0$, $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = 0$
  (b) $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z}$; $\mathrm{ord}_2(L^{(\mathrm{alg})}(E, 1)) = -1$; writing $E : y^2 = f(x)$ and the 2-torsion point as $(x_0, 0)$, none of $f'(x_0)$, $-f'(x_0)$ or $-\Delta_E$ are squares in $\mathbb{Q}$; $Ш(E')[2] = 0$, where $E' := E/E(\mathbb{Q})[2]$ is the 2-isogenous curve of E.

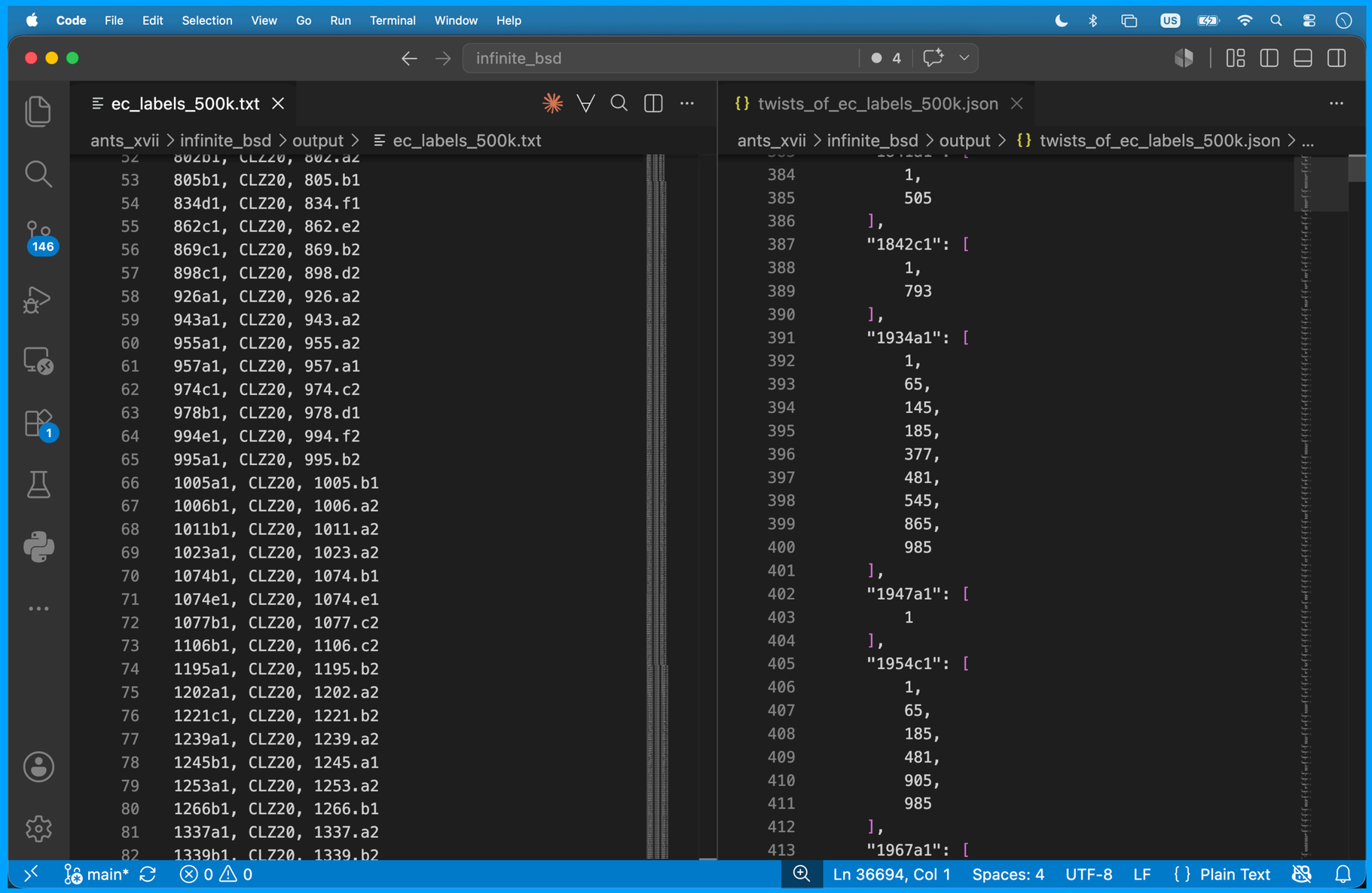
Then there exist infinitely many squarefree integers d satisfying the following:

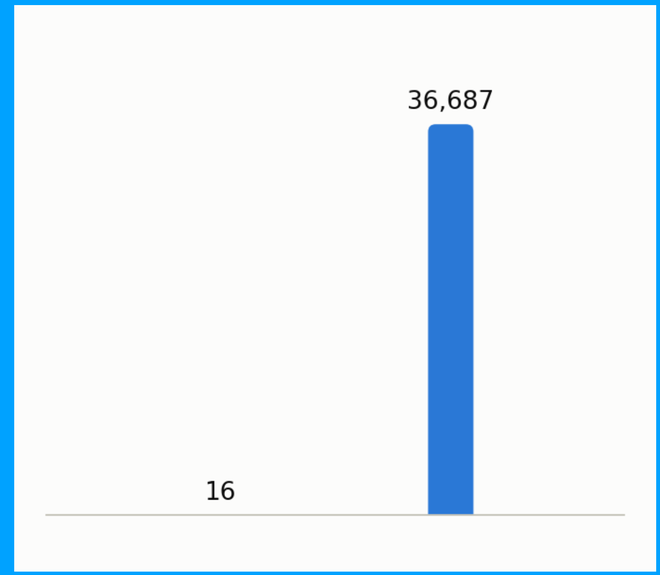
(1) $(d, 3N) = 1$.
(2) $d \equiv 1 \pmod 4$.
(3) E has ordinary reduction at prime divisors of d.
(4) (a) in Item 8a, for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E; for every $p \mid N$, p splits in $\mathbb{Q}(\sqrt{d})$; if $\Delta_E > 0$, then $d > 0$.
  (b) in Item 8b, for every $p|d$, $p \equiv 1 \pmod 4$, and $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$; and for every $p \mid 2N$, p splits in $\mathbb{Q}(\sqrt{d})$.

Therefore, by Theorem 2.13 and Theorem 2.14, such E as above admit infinitely many quadratic twists E_d that unconditionally satisfy BSD.



https://github.com/cocoxhuang/ants_xvii/tree/main/ants_xvii/infinite_bsd





~2,300x more curves 😎

https://github.com/cocoxhuang/ants_xvii/tree/main/ants_xvii/infinite_bsd

Why infinitely many twists?

Why infinitely many twists?

The conditions on d are mostly there to let one deduce BSD(E_d, 2) from BSD(E, 2).

Why infinitely many twists?

The conditions on d are mostly there to let one deduce BSD(E_d, 2) from BSD(E, 2).

(1) $(d, 3N) = 1$.
(2) $d \equiv 1 \pmod 4$.
(3) *E has ordinary reduction at prime divisors of d.*
(4) (a) *in Item 8a, for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E; for every $p \mid N$, p splits in $\mathbb{Q}(\sqrt{d})$; if $\Delta_E > 0$, then $d > 0$.*
(b) *in Item 8b, for every $p|d$, $p \equiv 1 \pmod 4$, and $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$; and for every $p \mid 2N$, p splits in $\mathbb{Q}(\sqrt{d})$.*

Why infinitely many twists?

The conditions on d are mostly there to let one deduce BSD(E_d, 2) from BSD(E, 2).

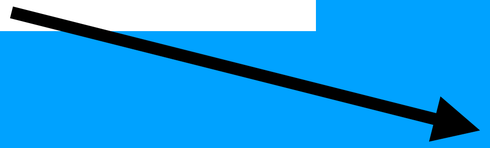
(1) $(d, 3N) = 1$.
(2) $d \equiv 1 \pmod 4$.
(3) *E has ordinary reduction at prime divisors of d.*
(4) (a) *in Item 8a, for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E; for every $p \mid N$, p splits in $\mathbb{Q}(\sqrt{d})$; if $\Delta_E > 0$, then $d > 0$.*
(b) *in Item 8b, for every $p|d$, $p \equiv 1 \pmod 4$, and $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$; and for every $p \mid 2N$, p splits in $\mathbb{Q}(\sqrt{d})$.*

“Chebotarev conditions”

Why infinitely many twists?

The conditions on d are mostly there to let one deduce BSD(E_d, 2) from BSD(E, 2).

(1) $(d, 3N) = 1$.
(2) $d \equiv 1 \pmod 4$.
(3) *E has ordinary reduction at prime divisors of d.*
(4) (a) *in Item 8a, for every $p|d$, p is inert in the number field $\mathbb{Q}[x]/(f(x))$, where $f(x)$ is the two-division polynomial of E; for every $p \mid N$, p splits in $\mathbb{Q}(\sqrt{d})$; if $\Delta_E > 0$, then $d > 0$.*
(b) *in Item 8b, for every $p|d$, $p \equiv 1 \pmod 4$, and $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$; and for every $p \mid 2N$, p splits in $\mathbb{Q}(\sqrt{d})$.*



“Chebotarev conditions”

Why infinitely many twists?

The conditions on d are mostly there to let one deduce BSD(E_d, 2) from BSD(E, 2).

(1) $(d, 3N) = 1$.
(2) $d \equiv 1 \pmod 4$.
(3) E *has ordinary reduction at prime divisors of* d.
(4) (a) *in Item 8a, for every* $p|d$, p *is inert in the number field* $\mathbb{Q}[x]/(f(x))$, *where* $f(x)$ *is the two-division polynomial of* E; *for every* $p \mid N$, p *splits in* $\mathbb{Q}(\sqrt{d})$; *if* $\Delta_E > 0$, *then* $d > 0$.
(b) *in Item 8b, for every* $p|d$, $p \equiv 1 \pmod 4$, *and* $\mathrm{ord}_2(\#\widetilde{E}(\mathbb{F}_p)) = 1$; *and for every* $p \mid 2N$, p *splits in* $\mathbb{Q}(\sqrt{d})$.

"Chebotarev conditions"

Lemma 4.1. *Let* $\ell \nmid N$ *be a prime. Then the following are equivalent:*

1) $|E(\mathbb{F}_\ell)| \not\equiv 0 \pmod 4$,
2) $E(\mathbb{F}_\ell)[2] \cong E_0(\mathbb{F}_\ell)[2] \cong \mathbb{Z}/2\mathbb{Z}$,
3) ℓ *is inert in both* $\mathbb{Q}(E[2])$ *and* $\mathbb{Q}(E_0[2])$.

Kriz, Li, 2019

How did we end up doing this?

How did we end up doing this?

What we did (2/2)

How did we end up doing this?

What we did (2/2)

We were actually attempting to verify a conjecture of Radziwill—Soundararajan:

How did we end up doing this?

What we did (2/2)

We were actually attempting to verify a conjecture of Radziwill—Soundararajan:

straightforward, and combining this with the Keating-Snaith conjecture for $L\left(\frac{1}{2}, E_d\right)$, we are led to formulate the following conjecture.

Conjecture 1 *Let E be given by the model $y^2 = f(x)$ for a monic cubic polynomial f with integer coefficients. Let K denote the splitting field of f over $\mathbb{Q}$, and let $G = Gal(K/\mathbb{Q})$ denote the associated Galois group, which we view as a subgroup of S_3. Given $g \in G$ let $c(g)$ denote one plus the number of fixed points of g (viewed as an element of S_3), and define*

$$\mu(E) = -\frac{1}{2} - \frac{1}{|G|}\sum_{g\in G} \log c(g) \text{ and } \sigma(E) = 1 + \frac{1}{|G|}\sum_{g\in G} (\log c(g))^2 .$$

As d ranges over $\mathcal{E}$, the distribution of $\log\left(|Ш(E_d)|/\sqrt{|d|}\right)$ is approximately Gaussian with mean $\mu(E)\log\log|d|$ and variance $\sigma(E)^2\log\log|d|$. More precisely, for any fixed $V \in \mathbb{R}$ and as $X \to \infty$,

$$\left|\left\{d \in \mathcal{E}, 20 < |d| \le X : \frac{\log\left(|Ш(E_d)|/\sqrt{|d|}\right) - \mu(E)\log\log|d|}{\sqrt{\sigma(E)^2\log\log|d|}} \ge V\right\}\right|$$

is

$$\sim |\{d \in \mathcal{E}, |d| \le X\}\left(\frac{1}{\sqrt{2\pi}}\int_V^\infty e^{-\frac{x^2}{2}}dx\right).$$

How did we end up doing this?

What we did (2/2)

We were actually attempting to verify a conjecture of Radziwill—Soundararajan:

straightforward, and combining this with the Keating-Snaith conjecture for $L\left(\frac{1}{2}, E_d\right)$, we are led to formulate the following conjecture.

Conjecture 1 *Let E be given by the model $y^2 = f(x)$ for a monic cubic polynomial f with integer coefficients. Let K denote the splitting field of f over $\mathbb{Q}$, and let $G = Gal(K/\mathbb{Q})$ denote the associated Galois group, which we view as a subgroup of S_3. Given $g \in G$ let $c(g)$ denote one plus the number of fixed points of g (viewed as an element of S_3), and define*

$$\mu(E) = -\frac{1}{2} - \frac{1}{|G|}\sum_{g\in G} \log c(g) \text{ and } \sigma(E) = 1 + \frac{1}{|G|}\sum_{g\in G} (\log c(g))^2 .$$

As d ranges over $\mathcal{E}$, the distribution of $\log\left(|Ш(E_d)|/\sqrt{|d|}\right)$ is approximately Gaussian with mean $\mu(E)\log\log|d|$ and variance $\sigma(E)^2\log\log|d|$. More precisely, for any fixed $V \in \mathbb{R}$ and as $X \to \infty$,

$$\left|\left\{d \in \mathcal{E}, 20 < |d| \le X : \frac{\log\left(|Ш(E_d)|/\sqrt{|d|}\right) - \mu(E)\log\log|d|}{\sqrt{\sigma(E)^2\log\log|d|}} \ge V\right\}\right|$$

is

$$\sim |\{d \in \mathcal{E}, |d| \le X\}\left(\frac{1}{\sqrt{2\pi}}\int_V^\infty e^{-\frac{x^2}{2}}dx\right).$$

https://radzi-sound-conjecture.netlify.app/46a1_maxd100000_nf100_20260116_185105_pdf

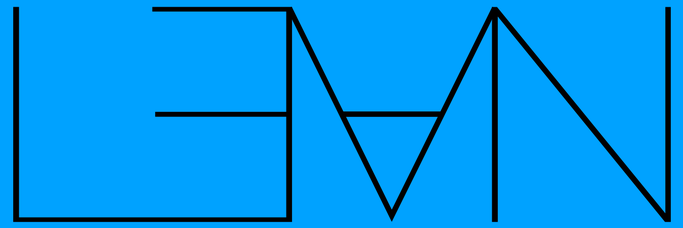
Where do we go from here?

Where do we go from here?

LeanBridge: Issuing formally verified certificates showing full BSD

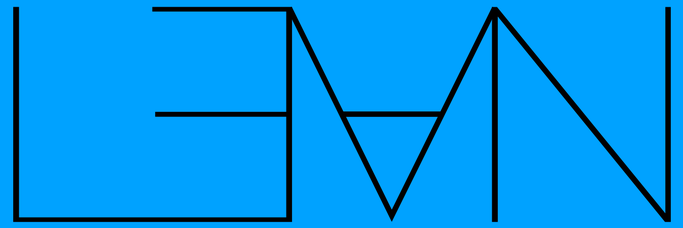
Where do we go from here?

LeanBridge: Issuing formally verified certificates showing full BSD



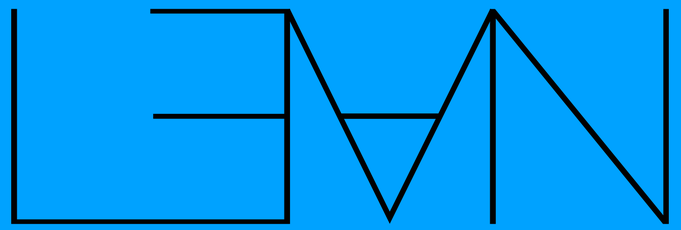
Where do we go from here?

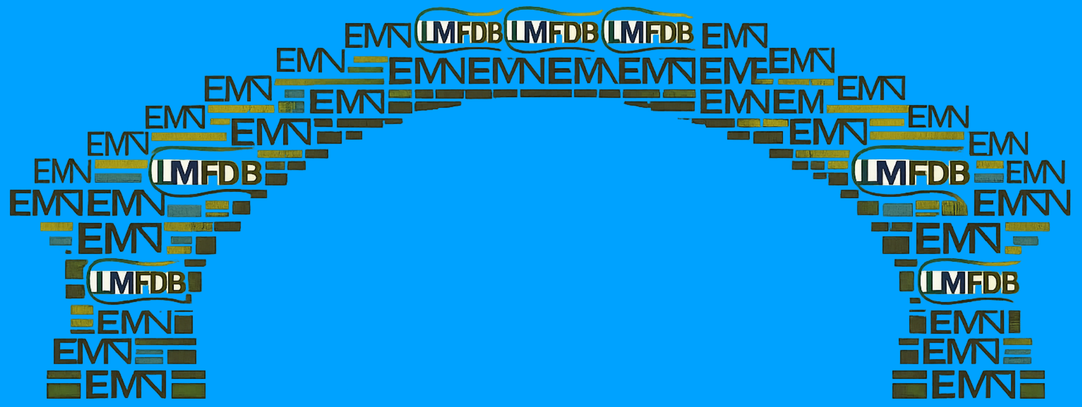
LeanBridge: Issuing formally verified certificates showing full BSD



Where do we go from here?

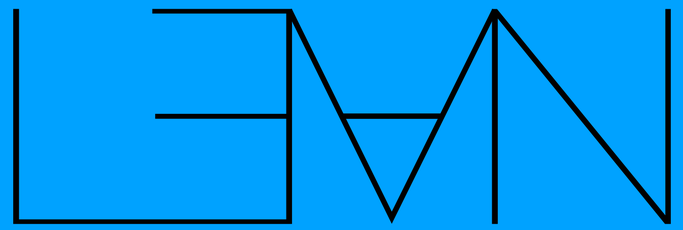
LeanBridge: Issuing formally verified certificates showing full BSD

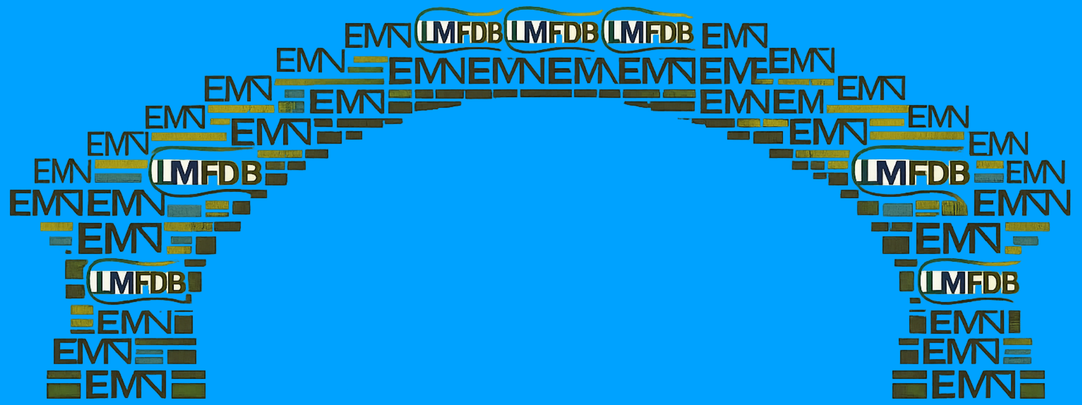




Where do we go from here?

LeanBridge: Issuing formally verified certificates showing full BSD





Fin