Products of point counts of higher genus curves over finite fields

Kiran S. Kedlaya
joint with Alina Bucur (UC San Diego), Arshay Sheth (TIFR, Mumbai); arXiv:2608.18014

Department of Mathematics, University of California San Diego
kedlaya@ucsd.edu
These slides can be downloaded from https://kskedlaya.org/slides/.

ICEAGE (Isogenies, Cryptography & Explicit Arithmetic GEometry)
University of Lleida, Catalonia, Spain
October 29, 2026

Supported by (grant DMS-2401536) and UC San Diego (Warschawski Professorship).

I acknowledge that my workplace occupies unceded ancestral land of the Kumeyaay Nation.

Contents

1 Elliptic curves

2 Abelian varieties

The conjecture of Birch and Swinnerton-Dyer, modern formulation

Let E be an elliptic curve over $\mathbb{Q}$. For p a prime of good reduction, set $N_p := \#E(\mathbb{F}_p)$ and let $a_p := p + 1 - N_p$ be the trace of Frobenius.

Conjecture (BSD)

The L-function

$$L(E,s) := \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

extended by analytic continuation, satisfies

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}\, E(\mathbb{Q}).$$

At the time the conjecture was made, analytic continuation to $s = 1$ was not known. It is now thanks to the modularity of elliptic curves (Wiles, Taylor–Wiles, ..., Breuil–Conrad–Diamond–Taylor).

The conjecture of Birch and Swinnerton-Dyer, modern formulation

Let E be an elliptic curve over $\mathbb{Q}$. For p a prime of good reduction, set $N_p := \#E(\mathbb{F}_p)$ and let $a_p := p + 1 - N_p$ be the trace of Frobenius.

Conjecture (BSD)

The L-function

$$L(E,s) := \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

extended by analytic continuation, satisfies

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}\, E(\mathbb{Q}).$$

At the time the conjecture was made, analytic continuation to $s = 1$ was not known. It is now thanks to the modularity of elliptic curves (Wiles, Taylor–Wiles, ..., Breuil–Conrad–Diamond–Taylor).

The conjecture of Birch and Swinnerton-Dyer, modern formulation

Let E be an elliptic curve over $\mathbb{Q}$. For p a prime of good reduction, set $N_p := \#E(\mathbb{F}_p)$ and let $a_p := p + 1 - N_p$ be the trace of Frobenius.

Conjecture (BSD)

The L-function

$$L(E,s) := \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1},$$

extended by analytic continuation, satisfies

$$\mathrm{ord}_{s=1} L(E,s) = \mathrm{rank}\, E(\mathbb{Q}).$$

At the time the conjecture was made, analytic continuation to $s = 1$ was not known. It is now thanks to the modularity of elliptic curves (Wiles, Taylor–Wiles, ..., Breuil–Conrad–Diamond–Taylor).

The conjecture of Birch and Swinnerton-Dyer, original formulation

Conjecture (OBSD)

For some constant $K > 0$, we have

$$\prod_{p \le x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} E(\mathbb{Q})} \qquad x \to \infty.$$

Given analytic continuation of $L(E, s)$, Goldfeld showed that OBSD implies BSD **and** the Riemann hypothesis for $L(E, s)$. In addition, one has

$$K = \frac{L^{(r)}(E, 1)}{r!} \frac{1}{\sqrt{\text{Ш}} e^r \gamma}$$

where $r = \operatorname{rank} E(\mathbb{Q})$ and $\gamma = 0.577215\cdots$ is the Euler–Mascheroni constant.

The conjecture of Birch and Swinnerton-Dyer, original formulation

Conjecture (OBSD)

For some constant $K > 0$, we have

$$\prod_{p \leq x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} E(\mathbb{Q})} \qquad x \to \infty.$$

Given analytic continuation of $L(E, s)$, Goldfeld showed that OBSD implies BSD **and** the Riemann hypothesis for $L(E, s)$. In addition, one has

$$K = \frac{L^{(r)}(E, 1)}{r!} \frac{1}{\sqrt{\text{Ш}} e^{r\gamma}}$$

where $r = \operatorname{rank} E(\mathbb{Q})$ and $\gamma = 0.577215\cdots$ is the Euler–Mascheroni constant.

Mestre–Nagao sums

Mestre and Nagao considered the quantities

$$\frac{1}{\log x} \sum_{p \leq x} \frac{a_p \log p}{p}.$$

BSD implies that this converges to $\frac{1}{2} - \operatorname{rank} E(\mathbb{Q})$ (as then does OBSD). This is a very useful way to sift through L-functions to find elliptic curves of high analytic rank!

Mestre–Nagao sums

Mestre and Nagao considered the quantities

$$\frac{1}{\log x} \sum_{p \leq x} \frac{a_p \log p}{p}.$$

BSD implies that this converges to $\frac{1}{2} - \operatorname{rank} E(\mathbb{Q})$ (as then does OBSD). This is a very useful way to sift through L-functions to find elliptic curves of high analytic rank!

Contents

1 Elliptic curves

2 Abelian varieties

The BSD conjecture for abelian varieties

Let A be an abelian variety of genus g over $\mathbb{Q}$. For p a prime of good reduction, set $N_p := \#A(\mathbb{F}_p)$. The L-function now has the form

$$L(A, s) := \prod_p L_{A,p}(p^{-s})^{-1}$$

where $L_{A,p}(T)$ (the L-**polynomial** of A at p) is the reverse characteristic polynomial of Frobenius on the ℓ-adic Tate module of A for any prime $\ell \neq p$. It is again conjectured that

$$\mathrm{ord}_{s=1} L(A, s) = \mathrm{rank}\, A(\mathbb{Q}).$$

The "OBSD conjecture" for abelian varieties

The analogue of OBSD for A would assert that for some $K > 0$,

$$\prod_{p \le x} \frac{N_p}{p^g} \sim K(\log x)^{\operatorname{rank} A(\mathbb{Q})} \qquad x \to \infty.$$

This again implies BSD for A, and is also supported by numerical evidence.

The "OBSD conjecture" for abelian varieties

The analogue of OBSD for A would assert that for some $K > 0$,

$$\prod_{p \leq x} \frac{N_p}{p^g} \sim K(\log x)^{\operatorname{rank} A(\mathbb{Q})} \qquad x \to \infty.$$

This again implies BSD for A, and is also supported by numerical evidence.

Curves of higher genus

Let C be a curve of genus g over $\mathbb{Q}$. Then the L-function of C is the same as that of its Jacobian $J(C)$, so BSD for C and $J(C)$ are identical statements.

For p a prime of good reduction, set $N_p := \#E(\mathbb{F}_p)$. The natural analogue of OBSD for C would seem to be

$$\prod_{p \leq x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q})} \qquad x \to \infty.$$

However, this is neither equivalent to OBSD for $J(C)$ nor supported by numerical evidence!

Or rather, this is supported by numerical evidence for **most** C, but not all. Explaining this phenomenon was the starting point of this collaboration.

Curves of higher genus

Let C be a curve of genus g over $\mathbb{Q}$. Then the L-function of C is the same as that of its Jacobian $J(C)$, so BSD for C and $J(C)$ are identical statements.

For p a prime of good reduction, set $N_p := \#E(\mathbb{F}_p)$. The natural analogue of OBSD for C would seem to be

$$\prod_{p \leq x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q})} \qquad x \to \infty.$$

However, this is neither equivalent to OBSD for $J(C)$ nor supported by numerical evidence!

Or rather, this is supported by numerical evidence for **most** C, but not all. Explaining this phenomenon was the starting point of this collaboration.

Curves of higher genus

Let C be a curve of genus g over $\mathbb{Q}$. Then the L-function of C is the same as that of its Jacobian $J(C)$, so BSD for C and $J(C)$ are identical statements.

For p a prime of good reduction, set $N_p := \#E(\mathbb{F}_p)$. The natural analogue of OBSD for C would seem to be

$$\prod_{p \leq x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q})} \qquad x \to \infty.$$

However, this is neither equivalent to OBSD for $J(C)$ nor supported by numerical evidence!

Or rather, this is supported by numerical evidence for **most** C, but not all. Explaining this phenomenon was the starting point of this collaboration.

Curves of higher genus

Let C be a curve of genus g over $\mathbb{Q}$. Then the L-function of C is the same as that of its Jacobian $J(C)$, so BSD for C and $J(C)$ are identical statements.

For p a prime of good reduction, set $N_p := \#E(\mathbb{F}_p)$. The natural analogue of OBSD for C would seem to be

$$\prod_{p \leq x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q})} \qquad x \to \infty.$$

However, this is neither equivalent to OBSD for $J(C)$ nor supported by numerical evidence!

Or rather, this is supported by numerical evidence for **most** C, but not all. Explaining this phenomenon was the starting point of this collaboration.

OBSD for curves of higher genus

The correct analogue of OBSD for C is the following.

Conjecture (Bucur–K–Sheth)

For some constant $K > 0$,

$$\prod_{p \le x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q}) - \operatorname{rank} \mathrm{NS}(J(C))+1} \qquad x \to \infty$$

where $\mathrm{NS}(J(C))$ denotes the Néron–Severi group.

In the generic case, $\operatorname{rank} \mathrm{NS}(J(C)) = 1$ and so there is no discrepancy with the naive conjecture. However, one can easily find examples where the discrepancy exists and numerical evidence favors the corrected analogue of OBSD over the naive analogue.

OBSD for curves of higher genus

The correct analogue of OBSD for C is the following.

Conjecture (Bucur–K–Sheth)

For some constant $K > 0$,

$$\prod_{p \le x} \frac{N_p}{p} \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q}) - \operatorname{rank} \mathrm{NS}(J(C))+1} \qquad x \to \infty$$

where $\mathrm{NS}(J(C))$ denotes the Néron–Severi group.

In the generic case, $\operatorname{rank} \mathrm{NS}(J(C)) = 1$ and so there is no discrepancy with the naive conjecture. However, one can easily find examples where the discrepancy exists and numerical evidence favors the corrected analogue of OBSD over the naive analogue.

OBSD and Sato–Tate groups

The quantity $\operatorname{rank} \mathrm{NS}(J(C))$ can also be interpreted as the moment $\mathrm{M}_1[a_2]$ where a_2 denotes the normalized second coefficient of the L-polynomial $L_{C,p}$, viewed as a random variable dependent on p. Assuming the Sato–Tate conjecture for C, we can also interpret a_2 as the second coefficient of the reverse characteristic polynomial of a random element of the Sato–Tate group $\mathrm{ST}(C)$.

This means that we can easily find examples of the discrepancy by consulting LMFDB to find curves of genus 2 with nongeneric Sato–Tate groups.

OBSD and Sato–Tate groups

The quantity $\operatorname{rank} \mathrm{NS}(J(C))$ can also be interpreted as the moment $\mathrm{M}_1[a_2]$ where a_2 denotes the normalized second coefficient of the L-polynomial $L_{C,p}$, viewed as a random variable dependent on p. Assuming the Sato–Tate conjecture for C, we can also interpret a_2 as the second coefficient of the reverse characteristic polynomial of a random element of the Sato–Tate group $\mathrm{ST}(C)$.

This means that we can easily find examples of the discrepancy by consulting LMFDB to find curves of genus 2 with nongeneric Sato–Tate groups.

Connection with the work of Kurokawa

Kaneko—Koyama—Kurokawa stated an analogue of OBSD (and Goldfeld's refinement) for an arbitrary cuspidal automorphic representation. For C, this corresponds to OBSD for $J(C)$ rather than C.

Let $\{\alpha_{i,p}\}_{i=1}^{2g}$ be the reciprocal roots of $L_{C,p} = L_{J(C),p}$. Then OBSD for $J(C)$ asserts that

$$\prod_{p \leq x} \prod_{i=1}^{2g} \left(1 - \frac{\alpha_{i,p}}{p}\right) \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q})}.$$

Expanding the left-hand side gives

$$\prod_{p \leq x} \left(1 - \sum_{i=1}^{2g} \frac{\alpha_{i,p}}{p} + \sum_{1 \leq i < j \leq 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} + O(p^{-3/2})\right).$$

Connection with the work of Kurokawa

Kaneko—Koyama—Kurokawa stated an analogue of OBSD (and Goldfeld's refinement) for an arbitrary cuspidal automorphic representation. For C, this corresponds to OBSD for $J(C)$ rather than C.

Let $\{\alpha_{i,p}\}_{i=1}^{2g}$ be the reciprocal roots of $L_{C,p} = L_{J(C),p}$. Then OBSD for $J(C)$ asserts that

$$\prod_{p \leq x} \prod_{i=1}^{2g} \left(1 - \frac{\alpha_{i,p}}{p}\right) \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q})}.$$

Expanding the left-hand side gives

$$\prod_{p \leq x} \left(1 - \sum_{i=1}^{2g} \frac{\alpha_{i,p}}{p} + \sum_{1 \leq i < j \leq 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} + O(p^{-3/2})\right).$$

Connection with the work of Kurokawa

Kaneko—Koyama—Kurokawa stated an analogue of OBSD (and Goldfeld's refinement) for an arbitrary cuspidal automorphic representation. For C, this corresponds to OBSD for $J(C)$ rather than C.

Let $\{\alpha_{i,p}\}_{i=1}^{2g}$ be the reciprocal roots of $L_{C,p} = L_{J(C),p}$. Then OBSD for $J(C)$ asserts that

$$\prod_{p \leq x} \prod_{i=1}^{2g} \left(1 - \frac{\alpha_{i,p}}{p}\right) \sim K(\log x)^{\operatorname{rank} J(C)(\mathbb{Q})}.$$

Expanding the left-hand side gives

$$\prod_{p \leq x} \left(1 - \sum_{i=1}^{2g} \frac{\alpha_{i,p}}{p} + \sum_{1 \leq i < j \leq 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} + O(p^{-3/2})\right).$$

Connection with the work of Kurokawa (continued)

Repeating, the left-hand side of OBSD for $J(C)$ is

$$\prod_{p \le x} \left(1 - \sum_{i=1}^{2g} \frac{\alpha_{i,p}}{p} + \sum_{1 \le i < j \le 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} + O(p^{-3/2}) \right).$$

In terms of $N_p = \#C(\mathbb{F}_p) = p + O(p^{1/2})$, the previous expression becomes

$$\prod_{p \le x} \left(\frac{N_p}{p} + \sum_{1 \le i < j \le 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} - \frac{1}{p} + O(p^{-3/2}) \right) = \prod_{p \le x} \frac{N_p}{p} \left(1 + \sum_{1 \le i < j \le 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} - \frac{1}{p} \right).$$

The product of the second factors is asymptotic to $K(\log x)^{M_1[a_2]-1}$, as predicted.

Connection with the work of Kurokawa (continued)

Repeating, the left-hand side of OBSD for $J(C)$ is

$$\prod_{p \le x} \left(1 - \sum_{i=1}^{2g} \frac{\alpha_{i,p}}{p} + \sum_{1 \le i < j \le 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} + O(p^{-3/2})\right).$$

In terms of $N_p = \#C(\mathbb{F}_p) = p + O(p^{1/2})$, the previous expression becomes

$$\prod_{p \le x} \left(\frac{N_p}{p} + \sum_{1 \le i < j \le 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} - \frac{1}{p} + O(p^{-3/2})\right) = \prod_{p \le x} \frac{N_p}{p} \left(1 + \sum_{1 \le i < j \le 2g} \frac{\alpha_{i,p}\alpha_{j,p}}{p^2} - \frac{1}{p}\right).$$

The product of the second factors is asymptotic to $K(\log x)^{M_1[a_2]-1}$, as predicted.

Happy birthday David! (and here is the QR code again)

