On the Arithmetic of Elliptic Curves: From the Birch and Swinnerton-Dyer Conjecture to the Iwasawa Main Conjecture and Beyond

By Justin Sirotin, Provocateur of Novelty

Abstract: We present a comprehensive survey of the theory of elliptic curves over the rational numbers, centered on the Birch and Swinnerton-Dyer (BSD) conjecture. We trace the historical development of the subject, from the foundational results of Gross-Zagier and Kolyvagin for curves of rank at most one, through the development of Iwasawa theory and the proof of the Main Conjecture for GL(2), to the recent breakthroughs in arithmetic statistics by Bhargava, Skinner, and Zhang. Throughout, we ground the discussion in explicit computational data from the L-functions and Modular Forms Database (LMFDB), illustrating the deep interplay between theory, computation, and conjecture that defines modern number theory.

Section 1: The Birch and Swinnerton-Dyer Conjecture: An Analytic-Algebraic Dictionary

The study of Diophantine equations—polynomial equations for which one seeks integer or rational solutions—is one of the oldest branches of mathematics. Among the most studied and arithmetically rich are those defining elliptic curves. An elliptic curve is, at its heart, a simple object, yet its structure has proven to be a gateway to some of the deepest and most challenging problems in modern number theory. For the past six decades, research in this area has been overwhelmingly guided by a single, unifying problem: the Birch and Swinnerton-Dyer (BSD) conjecture. This conjecture proposes a profound and precise dictionary, translating the algebraic properties of a curve's rational solutions into the analytic language of a complex function, its associated L-function. This section introduces these fundamental objects and lays out the statement of the conjecture that will serve as the narrative thread for this entire work.

1.1. Elliptic Curves over the Rational Numbers

An elliptic curve E defined over the field of rational numbers, Q, can be represented by a generalized Weierstrass equation of the form

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

where the coefficients a_i are rational numbers.1 The condition that this equation defines an elliptic curve is that its discriminant, a polynomial expression in the a_i, is non-zero, which ensures the curve is smooth. The set of rational points on the curve, denoted $E(Q)$, consists of all pairs $(x,y) \in Q^2$ that satisfy the equation, together with a special point at infinity, denoted O, which serves as the identity element for a remarkable algebraic structure. The points on an elliptic curve form an abelian group under a geometrically defined addition law.

A cornerstone of the theory is the Mordell-Weil theorem, which states that this group is finitely generated. This means its structure is completely described by two components: a finite torsion subgroup and a free part consisting of a finite number of copies of the integers.[2] We write this decomposition as:

$$E(Q) \cong E(Q)_{tors} \oplus Z^r$$

The non-negative integer r is a fundamental invariant of the curve known as its algebraic rank. While the torsion part is well-understood and can be effectively computed—Mazur's theorem famously classifies all possible torsion subgroups over Q—the rank remains deeply mysterious.5 There is no known algorithm guaranteed to compute the rank of an arbitrary elliptic curve.
Associated with any elliptic curve are several other key invariants. The *conductor* N is an integer that encodes information about the primes where the curve has "bad reduction," meaning primes where its reduction modulo p becomes singular. More precisely, the conductor is an ideal divisible by the prime ideals of bad reduction and no others, with exponents determined by the type of reduction (multiplicative or additive) according to Tate's algorithm.[6] The discriminant

Δ and the j-invariant are other crucial quantities derived from the Weierstrass coefficients that characterize the curve up to isomorphism and twisting.[1]

The systematic collection and organization of these invariants for millions of curves is the monumental achievement of the L-functions and Modular Forms Database (LMFDB). The LMFDB is not merely a static repository but a dynamic, relational

database that charts the landscape of modern number theory.[8] It contains comprehensive data on elliptic curves, modular forms, L-functions, number fields, and Galois representations, illustrating the profound connections between these objects predicted by the overarching Langlands program.[8] With data on over 7.5 million varieties, including elliptic curves over

Q and other number fields, the LMFDB provides the computational bedrock upon which much of the modern theory is tested and developed.[11]

1.2. The Hasse-Weil L-function

The bridge between the algebraic world of rational points and the analytic world of complex functions is the Hasse-Weil L-function of the elliptic curve, L(E,s). For each prime p of good reduction (i.e., p does not divide the conductor N), one can count the number of points on the reduced curve over the finite field Fp, denoted #E(Fp). The trace of Frobenius, ap, is then defined as ap=p+1−#E(Fp). The L-function is constructed as an Euler product over all primes:

$$L(E,s)=p|N\Pi Lp(E,s)^{-1}p\nmid N\Pi(1-app^{-s}+p1-2s)^{-1}$$

where the local factors Lp(E,s) for primes of bad reduction are defined according to the reduction type.3 This product converges for complex numbers
s with real part $\Re(s)>3/2$.

A priori, this function is only defined in a right half-plane. However, the *Modularity Theorem*—a profound result conjectured by Taniyama and Shimura, and proven for semistable curves by Wiles and for all rational curves by Breuil, Conrad, Diamond, and Taylor—states that every elliptic curve over Q is modular.[4] This means that the sequence of

ap coefficients for an elliptic curve E is identical to the sequence of Fourier coefficients of a certain type of modular form. A critical consequence of modularity is that the function L(E,s) has an analytic continuation to the entire complex plane and satisfies a functional equation. This equation relates the value of the L-function at s to its value at 2−s. The completed L-function $\Lambda(E,s)=(2\pi)^{-s}\Gamma(s)N^{s/2}L(E,s)$ satisfies:

$$\Lambda(E,s)=w(E)\Lambda(E,2-s)$$

where the root number w(E) is either +1 or −1.14 The existence of this analytic continuation and functional equation is the essential prerequisite for the formulation of the BSD

conjecture, which concerns the behavior of
L(E,s) at the central point s=1.

1.3. The Statement of the BSD Conjecture

The Birch and Swinnerton-Dyer conjecture provides a dictionary between the algebraic invariants of E(Q) and the analytic invariants of L(E,s). It consists of two parts.

First, the weak BSD conjecture predicts an equality of ranks:

ords=1L(E,s)=rank(E(Q))

The order of vanishing of the L-function at the central point s=1, an analytic quantity, is conjectured to be precisely the algebraic rank r.3 The integer
ords=1L(E,s) is thus often referred to as the *analytic rank*, ran.

Second, the strong BSD conjecture gives a precise formula for the leading term in the Taylor expansion of L(E,s) at s=1. It states that:
$$ \frac{L^{(r)}(E,1)}{r!} = \frac{\Omega_E \cdot \mathrm{Reg}(E) \cdot \prod_p c_p \cdot |\text{Ш}(E)|}{|E(\mathbb{Q})_{\text{tors}}|^2} $$
where $r=r_{\text{an}}$.2 Each term in this formula is a deep arithmetic invariant:

- ΩE is the fundamental real period of the curve, computed from an integral over the real points.
- Reg(E) is the *regulator*, the determinant of the canonical height pairing matrix on a basis of the free part of E(Q). By convention, if the rank is 0, the regulator is 1.[18]
- cp are the *Tamagawa numbers*, local factors correcting for bad reduction at each prime p. For a prime p of good reduction, cp=1.
- |E(Q)tors| is the order of the finite torsion subgroup.
- Ш(E) is the *Tate-Shafarevich group*. This group, defined using Galois cohomology, measures the obstruction to the Hasse principle for torsors of E. It is conjectured to be finite, but this is not known in general. Its (conjecturally finite) order is denoted |Ш(E)|.[19]

To ground these abstract definitions, we introduce four key elliptic curves from the LMFDB that will serve as running examples throughout this paper. Their fundamental invariants, as predicted by the BSD conjecture, are summarized in Table 1.1.

Table 1.1: Arithmetic Invariants of Key Elliptic Curves from the LMFDB

LMFDB Label	Conductor N	Rank r	Torsion Group	Regulator Reg(E)	Real Period ΩE	Tamagawa Product Пcp	Analytic Ш
11.a1	11	0	Trivial	1.0	6.788...	5	1
37.a1	37	1	Trivial	0.0511...	7.338...	1	1
389.a1	389	2	Trivial	0.231...	5.239...	1	1
5077.a1	5077	3	Trivial	19.35...	3.518...	1	1

Data for this table is compiled from the LMFDB and associated computational resources.[6] The analytic order of Ш is computed assuming the validity of the strong BSD formula.

The curve 11.a1 is the first elliptic curve with a trivial Mordell-Weil group (r=0 and trivial torsion).[21] The curve

37.a1 is the elliptic curve of minimal conductor with positive rank (r=1).[6] The curve

389.a1 is the elliptic curve of smallest conductor with rank 2 [22], and

5077.a1 is an example of a rank 3 curve.[23] This table immediately illustrates the conjecture's predictive power. For

37.a1, the LMFDB provides the value of the regulator, real period, and Tamagawa numbers.[20] Assuming the BSD formula and that

|Ш|=1, one can compute the predicted value of the first derivative of the L-function. Conversely, given the analytic data, one can predict the algebraic invariants. This deep interplay between computation and theory is a central theme of the subject.

1.4. Guiding Principles and Emerging Themes

The very formulation of the BSD conjecture reveals a foundational principle in modern number theory: the idea that "easy" local information can determine "hard" global

structure. The computation of the ap coefficients, which define the L-function, is an algorithmic, finite process for any given prime p. One simply counts points on a curve over a finite field. The construction of the L-function from these local data is then a standard procedure in complex analysis. In stark contrast, determining the global structure of E(Q)—specifically, its rank—is an unbounded problem. A priori, there is no algorithm guaranteed to find all generators of the Mordell-Weil group or even to determine if a single point has infinite order. The BSD conjecture posits that these two objects, one built from finite local computations and the other describing an infinite global structure, are not just related but are two sides of the same coin. This is not merely a formula; it is a philosophical statement about the deep arithmetic unity between the local and the global.

This principle is not just theoretical; it is deeply computational. The history of the BSD conjecture is inextricably linked with the history of computational number theory. The conjecture itself arose from early computer experiments by Birch and Swinnerton-Dyer, who noticed patterns in the product of local factors $\Pi_{p \le x} N_p/p$.[3] Today, this symbiotic relationship between theory and computation is embodied by the LMFDB.[8] The database serves as a laboratory where theoretical predictions can be tested on a massive scale. The existence of computational algebra systems like Magma, Sage, and Pari/GP, which are directly integrated with or referenced by the LMFDB, allows researchers to move seamlessly between theoretical formulation, algorithmic implementation, and data verification.[6] This creates a powerful feedback loop: theory suggests what to compute, and computation provides the evidence and discovers the exceptions that shape the next generation of theory. The story of the progress on the BSD conjecture, which we will now trace, is a testament to the power of this synthesis.

Section 2: The Breakthrough for Rank One: Heegner Points and the Gross-Zagier Formula

For nearly two decades after its formulation, the BSD conjecture remained largely a matter of heuristics and numerical evidence. The first major theoretical breakthrough came in the 1980s with the work of Benedict Gross and Don Zagier. They established a stunningly precise formula that connected the analytic world of L-functions to the algebraic geometry of special points on modular curves. This work provided the first concrete, theoretical evidence for the rank part of the BSD conjecture and laid the

groundwork for the subsequent algebraic advances of Kolyvagin.

2.1. Heegner Points on Modular Curves

The key objects in the Gross-Zagier theory are *Heegner points*. To define them, one must first introduce the concept of modular curves. A modular curve, such as $X_0(N)$, can be understood as a geometric object that parameterizes isomorphism classes of elliptic curves equipped with some additional structure. Specifically, a point on the complex curve $X_0(N)$ corresponds to a pair (E, C), where E is an elliptic curve and C is a cyclic subgroup of order N.[6] By the Modularity Theorem, any elliptic curve

$E/\mathbb{Q}$ of conductor N admits a non-constant map, called a modular parametrization, $\pi_E: X_0(N) \to E$.

Heegner points are special, arithmetically significant points on the modular curve $X_0(N)$. They arise from elliptic curves that possess an extra symmetry, namely *complex multiplication* (CM). An elliptic curve is said to have CM if its endomorphism ring is larger than the integers, $\mathbb{Z}$; in this case, it must be an order $\mathcal{O}$ in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ for some square-free $d > 0$.[30] A Heegner point on

$X_0(N)$ corresponds to a pair (E', C'), where E' is an elliptic curve with CM by an order $\mathcal{O}$ in an imaginary quadratic field K.

For these points to be well-defined and useful, the field K must satisfy the *Heegner hypothesis* relative to the conductor N: every prime factor of N must split into two distinct prime ideals in the ring of integers of K. When this condition holds, the theory of complex multiplication shows that the Heegner points are defined over certain abelian extensions of K, known as ring class fields. The image of a Heegner point under the modular parametrization, π_E, gives a point on the elliptic curve E that is also defined over a ring class field of K. By taking the trace of this point from the ring class field down to the field K, one obtains a canonical point $y_K \in E(K)$.

2.2. The Gross-Zagier Formula

The landmark result of Gross and Zagier, published in 1986, provides an explicit

formula relating the arithmetic height of the Heegner point yK to the analytic behavior of an L-function.[30] Specifically, they considered the L-function of the elliptic curve

E over the quadratic field K, denoted L(E/K,s). This L-function factors as L(E/K,s)=L(E,s)L(ED,s), where ED is the quadratic twist of E by the discriminant D of the field K. The Gross-Zagier formula states that the canonical height of the point yK is proportional to the first derivative of the L-function L(E/K,s) at the central point s=1:

L′(E/K,1)=C·h^(yK)

where C is a non-zero constant involving periods and other arithmetic terms.30
The most profound consequence of this formula is a non-vanishing statement. If the analytic rank of E over Q is one, one can choose the imaginary quadratic field K such that the root number of L(E,s) is −1 and the root number of L(ED,s) is +1. This implies that L(E,1)=0 and L(ED,1)僾=0. In this situation, the derivative L′(E/K,1) is non-zero, and the Gross-Zagier formula then forces the height h^(yK) to be non-zero as well. Since only points of infinite order can have non-zero canonical height, this proves that the Heegner point yK is a point of infinite order in E(K). This provided the first theoretical construction of a point of infinite order on an elliptic curve, conditioned only on the analytic rank being one, thereby giving powerful evidence for the BSD conjecture.

The elliptic curve 37.a1 provides a perfect illustration. It is the quotient of the modular curve X0(37) by the Fricke involution.[6] Its L-function has a simple zero at

s=1, so its analytic rank is one.[6] The Gross-Zagier theorem thus predicts the existence of a Heegner point of infinite order. Indeed, the Mordell-Weil group

E(Q) has rank 1. The regulator, which for a rank 1 curve is simply the canonical height of a generator, is found in the LMFDB to be Reg(E)≈0.0511....[20] The Gross-Zagier machinery constructs a generator whose height is precisely this value, confirming the prediction.

2.3. A Quantitative Foundation and Its Inherent Limitations

The Gross-Zagier formula represents a crucial pattern in the development of number theory: a precise, quantitative formula often serves as the necessary foundation for a more general, qualitative structural theory. The formula provided an explicit link between an analytic value, L′(E/K,1), and an algebraic quantity, h^(yK). The most

critical consequence was the non-vanishing result: if the derivative is non-zero, the point is non-trivial. This non-trivial point was precisely the "seed" that Viktor Kolyvagin needed to initialize his powerful algebraic machinery of Euler systems, which we will discuss in the next section. Without the guarantee from Gross and Zagier that a non-torsion point existed under the appropriate analytic conditions, the entire Euler system construction would have yielded only trivial results. Thus, the analytic breakthrough of Gross and Zagier was the direct catalyst for the algebraic breakthrough of Kolyvagin.

However, the very specificity that makes the Heegner point construction so powerful is also the source of its fundamental limitation. The construction is tailored to the analytic rank one case and fails dramatically for curves of higher rank. Consider an elliptic curve E with analytic rank 2. The root number of its L-function must be +1. One can typically choose an imaginary quadratic field K (satisfying the Heegner hypothesis) such that the twisted curve ED also has analytic rank 1. In this scenario, both L(E,s) and L(ED,s) have root number −1, which forces L(E,1)=0 and L(ED,1)=0. The derivative of the product L-function is given by the product rule:

$$L'(E/K,1)=L'(E,1)L(ED,1)+L(E,1)L'(ED,1)$$

Since both terms are zero, $L'(E/K,1)=0$. The Gross-Zagier formula then implies that $h^(yK)=0$, meaning the constructed Heegner point yK must be a torsion point. The method is constitutionally incapable of producing points of infinite order for curves of rank greater than one.34 This "creative failure" was a major impetus for the development of the more sophisticated theories that will be explored in the subsequent sections, as mathematicians sought to generalize these ideas to the elusive higher rank setting.

Section 3: The Finiteness of Ш: Kolyvagin's Euler Systems

Building directly on the foundation laid by Gross and Zagier, Viktor Kolyvagin introduced a revolutionary algebraic framework in the late 1980s. He constructed what he termed an "Euler system" from the collection of Heegner points. This powerful machine allowed him to control the size of the Selmer group, leading to the first proofs of the finiteness of the Tate-Shafarevich group for elliptic curves and a full proof of the BSD conjecture for all curves of analytic rank zero and one.

3.1. Descent, Selmer Groups, and the Tate-Shafarevich Group

The primary tool for relating the global Mordell-Weil group to local data is the method of descent, which is formalized using Galois cohomology. For a prime p, the multiplication-by-p map on an elliptic curve gives rise to a short exact sequence of Galois modules. The long exact sequence in Galois cohomology then yields the fundamental descent sequence:
$$ 0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[p] \to 0 $$
where Selp(E/Q) is the p-Selmer group and Ш$(E/\mathbb{Q})[p]$ is the p-torsion part of the Tate-Shafarevich group. The Selmer group is a subgroup of the Galois cohomology group H1(Gal(Q¯/Q),E[p]) defined by imposing local conditions at every prime. While defined abstractly, it is, in principle, a finite and computable group.
The descent sequence is of paramount importance because it connects the three key objects of interest. The term on the left, E(Q)/pE(Q), is a finite group whose dimension as an Fp-vector space is r+dim(E(Q)tors[p]). The term on the right, Ш$(E/\mathbb{Q})[p]$, is the mysterious p-part of the Tate-Shafarevich group. The sequence shows that if one can compute or bound the size of the Selmer group, one simultaneously obtains bounds on both the algebraic rank r and the size of Ш$(E/\mathbb{Q})$. The central difficulty in arithmetic geometry is that while E(Q)/pE(Q) is hard to compute directly, Selp(E/Q) is more accessible, but it is generally larger. The goal is to prove that the Selmer group is no larger than necessary.

3.2. Kolyvagin's Euler System

Kolyvagin's ingenious insight was to use the entire system of Heegner points, not just a single one, to systematically build cohomology classes that would constrain the size of the Selmer group. He considered not just a single imaginary quadratic field K, but the tower of ring class fields Kn of K with conductors n for a set of suitable primes. Over each field Kn, there is a Heegner point yKn. This collection of points {yKn} forms an *Euler system*.[35]

The defining property of an Euler system is that the points are related by norm maps. Specifically, if n=mℓ for a prime ℓ, the trace of the point yKmℓ from E(Kmℓ) down to E(Km) is related to the point yKm via the action of a Hecke operator.[37] This compatibility relation is the algebraic engine that drives the entire theory.

From this norm-compatible system of points, Kolyvagin used the machinery of Galois cohomology (specifically, a construction now known as the "Kolyvagin derivative") to

produce a set of cohomology classes {κn∈H1(Gal(K¯/K),E[pk])}.[39] These classes are constructed to be trivial when restricted to decomposition groups at most primes, but are non-trivial at primes dividing

n. By carefully choosing the primes n, he could produce classes in the Selmer group and use local Tate duality to show that these classes must annihilate corresponding elements in the Tate-Shafarevich group.

3.3. Main Results and Consequences

The culmination of this intricate algebraic construction is Kolyvagin's main theorem.

Theorem (Kolyvagin): Let E/Q be a modular elliptic curve and K an imaginary quadratic field satisfying the Heegner hypothesis. If the Heegner point yK∈E(K) has infinite order, then:

1. The Mordell-Weil group E(Q) has rank one.
2. The Tate-Shafarevich group Ш$(E/\mathbb{Q})$ is finite.

33

Combining this with the Gross-Zagier formula provides a stunning result. If the analytic rank of E is one, then L′(E,1)僾=0. By Gross-Zagier, the Heegner point yK must have infinite order. Kolyvagin's theorem then implies that the algebraic rank is one and Ш is finite. This proves that ran=1⟹r=1 and ∣Ш∣<∞.

A similar argument applies when the analytic rank is zero. In this case, L(E,1)僾=0. A variant of the Euler system argument, initiated with a different set of cohomology classes, proves that the Selmer group is trivial, which in turn implies that the algebraic rank is zero and Ш is finite.[38]

Together, these results provide a complete proof of both the weak and strong forms of the Birch and Swinnerton-Dyer conjecture for all elliptic curves over Q with analytic rank at most one.[3] The curve

11.a1, with rank 0, and 37.a1, with rank 1, are the quintessential examples where this theory applies perfectly. For 37.a1, the finiteness of its Shafarevich-Tate group is a direct consequence of Kolyvagin's theorem. Modern computational tools can even provide an explicit bound; for instance, the SageMath command E.sha().bound() for

the curve 37.a1 returns (, 1), indicating that the only possible prime divisor of the order of Ш is 2.[22] The LMFDB confirms the final result that

|Ш|=1, perfectly consistent with the theory.[20]

3.4. A New Paradigm and Its Implications

Kolyvagin's work represented a monumental paradigm shift in the field. It moved beyond the specific, quantitative formula of Gross and Zagier to a general, structural machine. The concept of an "Euler system" is purely algebraic and cohomological, defined by the abstract property of norm-compatibility.[37] The proof that a non-trivial Euler system can be used to bound a Selmer group is a masterclass in Galois cohomology, relying on the intricate machinery of local and global duality theorems.[35]

The power of this abstraction is that the method is not limited to elliptic curves. The Euler system machine is general; one only needs to supply a valid input. For modular elliptic curves, Heegner points provide this input. But for other arithmetic objects, other constructions can be used. For example, in his work on cyclotomic fields, which was a direct inspiration for Kolyvagin, Francisco Thaine used cyclotomic units as the input for an Euler system to bound ideal class groups.[37] As we will see in the next section, Kazuya Kato later constructed a new Euler system from elements in algebraic K-theory to tackle the Iwasawa Main Conjecture. Kolyvagin's deepest contribution was therefore not merely the resolution of the rank one case of BSD, but the invention of a powerful and general method that has become a cornerstone of modern arithmetic geometry.

Furthermore, the proof of the finiteness of the Tate-Shafarevich group was a landmark achievement in its own right. Before Kolyvagin's work, it was not known whether Ш was finite for even a single elliptic curve.[38] His result provided the first general finiteness theorem in the subject. This has profound theoretical consequences. For instance, the Cassels-Tate pairing on Ш is an alternating, non-degenerate bilinear form. A direct consequence is that if the order of Ш is finite, it must be a perfect square.[19] This provides a powerful internal consistency check for computations related to the BSD conjecture. The numerical verifications of BSD for higher-dimensional abelian varieties, for example, explicitly check whether the analytically predicted order of Ш is a rational square, a test that is only meaningful

because of the finiteness established by these methods.[45] For our example

37.a1, the LMFDB gives |Ш|=1=12, in perfect agreement with this structural constraint.[20]

Section 4: The p-adic World: Iwasawa Theory and the Main Conjecture

The resolution of the BSD conjecture for curves of rank at most one was a watershed moment. However, the methods of Gross-Zagier and Kolyvagin were fundamentally limited to this case. To move forward, a deeper and more refined theory was needed. This theory emerged from the p-adic realm, in the form of Iwasawa theory. By studying arithmetic objects not just over Q, but over an infinite tower of number fields, Iwasawa theory reveals a hidden structure governed by a "Main Conjecture" that can be seen as a vast p-adic generalization of the BSD conjecture.

4.1. Iwasawa Theory for Elliptic Curves

The central idea of Iwasawa theory is to study the growth of arithmetic objects, such as Selmer groups, in a tower of number fields. For an elliptic curve E/Q and a prime p, the relevant tower is the *cyclotomic Zp-extension* of Q, denoted Q∞. This is the unique Galois extension of Q whose Galois group Γ=Gal(Q∞/Q) is isomorphic to the additive group of p-adic integers, Zp.

Instead of studying the Selmer group Selp∞(E/Q), Iwasawa theory considers the Selmer group over the entire tower, Selp∞(E/Q∞). This object is no longer just a finite group; it is a module over the *Iwasawa algebra*, Λ=Zp[[Γ]]≅Zp].[48] The Iwasawa algebra is a powerful algebraic object, a two-dimensional regular local ring. Modules over this ring have a well-understood structure theory, analogous to the structure theory of finitely generated modules over a principal ideal domain.

The Pontryagin dual of the Selmer group, X(E/Q∞)=Homcont(Selp∞(E/Q∞),Qp/Zp), is a finitely generated, torsion Λ-module. According to the structure theory, any such module has a *characteristic ideal*, generated by a power series charΛ(X(E/Q∞))∈Λ.

This characteristic ideal is a purely algebraic object that encodes the precise growth of the sizes of the Selmer groups $Sel_{p^\infty}(E/Q_n)$ as one moves up the tower of fields $Q_n \subset Q_\infty$.

4.2. p-adic L-functions and the Main Conjecture

The analytic counterpart to the algebraic characteristic ideal is the *p-adic L-function*. In the 1970s, Amice, Vélu, and Vishik showed how to construct a p-adic analytic function, $L_p(E,s)$, which can be viewed as an element of the Iwasawa algebra Λ. This function is characterized by an interpolation property: its values at certain special points correspond to the classical special values of the complex L-function $L(E,\chi,s)$ twisted by Dirichlet characters χ of p-power order.[48] The p-adic L-function is the analytic object that captures the p-adic behavior of the special values of the complex L-function.

With these two objects defined—the algebraic characteristic ideal and the analytic p-adic L-function—one can state the Iwasawa Main Conjecture for GL(2). It asserts a profound equality of ideals within the Iwasawa algebra:

$$char_\Lambda(X(E/Q_\infty)) = (L_p(E,s))$$

.48 This conjecture states that the algebraic object governing the growth of Selmer groups is precisely the analytic object that interpolates special values of L-functions. It is a vast and deep refinement of the BSD conjecture, connecting not just two numbers, but two entire power series.

4.3. Kato's Euler System and the Proof of the Main Conjecture

The proof of the Iwasawa Main Conjecture for GL(2) is one of the crowning achievements of modern number theory, requiring the synthesis of two entirely different and monumental research programs.

The first half of the proof, establishing the divisibility $(L_p(E,s)) \subseteq char_\Lambda(X(E/Q_\infty))$, was accomplished by Kazuya Kato. Kato constructed a new and highly sophisticated Euler system for modular forms.[52] Unlike Kolyvagin's system built from Heegner points,

Kato's system is constructed from

Beilinson elements in the algebraic K-theory group K2 of modular curves. The construction and manipulation of these classes required the development of powerful new tools in p-adic Hodge theory, including an explicit reciprocity law that relates the Euler system classes to the p-adic L-function.[52] Kato's Euler system is more general than Kolyvagin's and, crucially, is not restricted to the rank one setting. Applying the Euler system machinery to these classes, Kato was able to bound the Selmer group from above, proving his divisibility, often referred to as the "easy" direction of the Main Conjecture (despite its immense technical difficulty).[33]

The reverse divisibility, $\mathrm{char}_{\Lambda}(X(E/Q_\infty)) \subseteq (L_p(E,s))$, was proven by Christopher Skinner and Eric Urban using completely different methods rooted in the theory of automorphic forms.[48] Their approach involved studying congruences between automorphic forms on the unitary group GU(2,2). By constructing an Eisenstein ideal in the Hecke algebra for this group and relating it to Selmer groups, they were able to bound the Selmer group from below, establishing the required divisibility under certain technical hypotheses (including the irreducibility of the residual Galois representation and a ramification condition at a prime dividing the conductor).[48]

Together, the works of Kato and Skinner-Urban provide a full proof of the Iwasawa Main Conjecture for GL(2) for a large class of elliptic curves.[48]

4.4. A "Master Conjecture" and the Synthesis of Modern Methods

The Iwasawa Main Conjecture can be viewed as a "master conjecture" from which the BSD conjecture can be derived. While BSD relates two numbers, $L^{(r)}(E,1)/r!$ and the algebraic invariants of the curve, the Main Conjecture relates two functions (power series) in the Iwasawa algebra, $L_p(E,s)$ and the characteristic power series of the Selmer module. By evaluating these power series at specific characters of the Galois group Γ, one can recover the classical BSD formula for curves of rank 0 and 1. This demonstrates a powerful principle in modern number theory: to understand an arithmetic phenomenon over a base field like $\mathbb{Q}$, it is often advantageous to study it over an infinite tower of fields like $\mathbb{Q}_\infty$. The richer structure of the Galois group of the tower often regularizes the arithmetic in a way that reveals deeper structural truths. The relationship between L-values and arithmetic is not a one-off phenomenon at the

point s=1, but a continuous, p-adic property that holds throughout an entire family.

The proof of the Main Conjecture is also a testament to the state of the art in number theory. It required the confluence of a vast array of modern techniques: the algebraic geometry of modular curves, algebraic K-theory, the intricate machinery of p-adic Hodge theory, the representation theory of p-adic groups, and the theory of automorphic forms on higher-rank groups. The fact that two completely independent and conceptually distinct approaches—Kato's geometric/cohomological construction of an Euler system and Skinner-Urban's analytic/automorphic method of congruences—were both required to prove the two separate divisibilities of the conjecture highlights its extraordinary depth. This successful synthesis of different mathematical worlds is a concrete and powerful validation of the philosophy of the Langlands program, which conjectures that such deep equivalences should exist.

Section 5: The Statistical Theory: A Breakthrough for a "Typical" Elliptic Curve

While the proof of the Iwasawa Main Conjecture provided a profound understanding of the BSD conjecture for a large class of curves, it did not resolve the conjecture for any specific curve of rank greater than one. In the 2010s, a revolutionary new approach emerged, pioneered by Manjul Bhargava and his collaborators. This approach shifted the focus from proving BSD for every individual curve to proving it for a "positive proportion" or a "majority" of all curves. This statistical perspective has led to some of the most dramatic progress on the conjecture to date.

5.1. Arithmetic Statistics and Ordering by Height

The field of arithmetic statistics aims to understand the distribution of arithmetic objects, such as number fields, class groups, or elliptic curves. To ask meaningful statistical questions about an infinite set like the set of all elliptic curves over Q, one must first define a way to order them. The standard method is to order curves by the *height* of their minimal Weierstrass coefficients. An elliptic curve $E: y^2 = x^3 + Ax + B$ has height $H(E) = \max(4|A|^3, 27B^2)$.[57] One can then study the properties of a "typical"

elliptic curve by analyzing the average behavior of invariants as the height tends to infinity.

Based on extensive heuristics and numerical data, it is conjectured that when ordered by height, 50% of elliptic curves have algebraic rank 0, 50% have algebraic rank 1, and a vanishing proportion (0%) have rank 2 or greater.[59] If this rank distribution conjecture is true, it would imply that 100% of elliptic curves satisfy the weak BSD conjecture.

5.2. The Bhargava-Shankar Method: Averaging Selmer Groups

Directly computing the rank for all curves up to a large height is computationally infeasible. The groundbreaking work of Bhargava and Shankar was to bypass the direct computation of the rank and instead compute the *average size* of the n-Selmer groups, Seln(E/Q), over all elliptic curves ordered by height.[61]

Their method involves a masterful application of the geometry of numbers. They established a correspondence between elements of the n-Selmer group and integral orbits of certain algebraic groups on high-dimensional vector spaces. By developing techniques to count these integral orbits in fundamental domains, they were able to compute the average size of the Selmer groups. Their key results include:

- The average size of the 2-Selmer group is 3.[58]
- The average size of the 3-Selmer group is 4.[64]
- The average size of the 4-Selmer group is 7.[65]
- The average size of the 5-Selmer group is 6.[67]

Since the rank of E(Q) is bounded by the rank of the n-Selmer group, these results had immediate and profound consequences. For example, the fact that the average size of the 2-Selmer group is 3 implies that the average rank of elliptic curves is bounded above by 1.5.[58] This provided the first-ever unconditional proof that the average rank of elliptic curves is finite, a major milestone in the field.[58]

5.3. The Role of the Parity Conjecture

A crucial ingredient in leveraging the Selmer group results to obtain information about the rank itself is the Parity Conjecture. This conjecture, which is a direct consequence of the BSD conjecture, states that the parity of the algebraic rank of an elliptic curve is determined by the sign (or root number) w(E) in the functional equation of its L-function:

(−1)rank(E(Q))=w(E)

.71 The root number
w(E) is a product of local root numbers and is, in principle, computable. The Parity Conjecture is therefore a more accessible consequence of BSD. Significant progress on this conjecture has been made by Tim and Vladimir Dokchitser, who have proven it holds for elliptic curves over Q and in many other cases, often by relating the parity of the rank to the parity of the dimension of the p-Selmer group.[14]

5.4. The Main Result of Bhargava, Skinner, and Zhang

The culmination of this line of research was a landmark 2014 paper by Manjul Bhargava, Christopher Skinner, and Wei Zhang. They brilliantly synthesized the three major threads of research discussed so far: the Bhargava-Shankar results on average Selmer sizes, the Skinner-Urban proof of the Iwasawa Main Conjecture, and the Dokchitsers' work on the Parity Conjecture.

Their strategy was to first identify families of elliptic curves for which the hypotheses of the Skinner-Urban theorem hold. For curves within these families, the Iwasawa Main Conjecture is true, which in turn implies that the BSD conjecture holds, provided the analytic rank is at most one.[60] They then used the powerful counting methods of Bhargava and Shankar to prove that these "good" families of curves have a positive density among all elliptic curves when ordered by height. By carefully combining results for different primes

p (especially p=3 and p=5) and analyzing the distribution of root numbers, they were able to prove their main theorem:

Theorem (Bhargava-Skinner-Zhang): A positive proportion (in fact, greater than 66%) of elliptic curves over Q, when ordered by height, satisfy the Birch and Swinnerton-Dyer conjecture and have a finite Tate-Shafarevich group.[57]

This result also established for the first time that a positive proportion of all elliptic

curves have proven algebraic and analytic rank zero (at least 16.5%) and a positive proportion have proven algebraic and analytic rank one (at least 20.68%).[57]

5.5. A New Synthesis and a Philosophical Shift

The work of Bhargava, Skinner, and Zhang represents a powerful new synthesis in number theory. It demonstrates how the deep, structural results of Iwasawa theory, which apply to specific (if large) classes of curves, can be used as essential input for the machinery of arithmetic statistics to yield sweeping conclusions about "most" curves. The proof is a beautiful interplay between the algebraic and the analytic, the individual and the statistical. The Skinner-Urban theorem provides the necessary BSD-type results for certain well-behaved families, and the Bhargava-Shankar methods provide the crucial density estimates to show that these families are not arithmetically rare.

This breakthrough also marks a significant philosophical shift in the field. While the ultimate goal remains a proof of the BSD conjecture for *every* elliptic curve, the statistical results demonstrate that the conjecture is "generically true." We now know with certainty that the BSD conjecture is the norm, not the exception. This provides enormous theoretical and psychological validation for the conjecture and reframes the outstanding problem. The question is no longer "Is the BSD conjecture true?" but has become "What are the special arithmetic properties of the (at most) 34% of curves for which we cannot yet prove it?". This also clarifies the important distinction between proving that "100% of curves satisfy BSD" and proving that "all curves satisfy BSD." The former is a statistical statement that allows for a set of exceptions of measure zero, while the latter is a stronger, purely algebraic statement that allows for no exceptions whatsoever.[59] The work of Bhargava, Skinner, and Zhang brings us tantalizingly close to the first statement, while the second remains a distant, albeit central, goal.

Section 6: Frontiers: Higher Rank and Future Directions

The progress on the Birch and Swinnerton-Dyer conjecture for elliptic curves of

analytic rank at most one, and for a majority of all curves, has been nothing short of spectacular. However, the case of curves with rank two or greater remains a formidable fortress. The methods that were so successful in the rank one case break down completely, and the path forward requires the development of new ideas and deeper generalizations. This final section surveys the challenges of the higher rank case and explores the current frontiers of research, from the construction of high-rank curves to the search for new Euler systems and the discovery of unexpected patterns through computational exploration.

6.1. The Challenge of Higher Rank

The fundamental barrier to progress on higher rank elliptic curves is the failure of the Heegner point construction. As explained in Section 2, the Gross-Zagier formula relates the height of a Heegner point to the first derivative of an L-function. For an elliptic curve E/Q with analytic rank ran≥2, the L-function L(E,s) has a zero of order at least two at s=1. For any choice of imaginary quadratic field K satisfying the Heegner hypothesis, the twisted L-function L(ED,s) will also have a zero at s=1. Consequently, the derivative of the combined L-function L(E/K,s) at s=1 is zero. The Gross-Zagier formula then implies that the corresponding Heegner point has height zero, meaning it is a torsion point and provides no information about the rank of the curve.[34]

This is not merely a technical issue; it is a fundamental obstruction. At present, there is no known general, theoretical method for constructing points of infinite order on an elliptic curve of rank two or greater, nor is there a method for proving that two such constructed points are linearly independent over Z.[76] The elliptic curve

389.a1, the curve of smallest conductor with rank 2, and 5077.a1, a rank 3 curve, serve as stark reminders of this challenge.[22] While we can find their generators using computational search methods, we lack a theoretical construction analogous to Heegner points that would produce them from first principles. This is the central open problem in the field.

6.2. Constructing High-Rank Curves

Despite the theoretical difficulties, there has been significant progress in the explicit construction of elliptic curves with high rank. For many years, it was not known if there were infinitely many elliptic curves of any fixed rank $r \geq 2$. This was recently settled for rank 2 by David Zywina.

Theorem (Zywina): There are infinitely many elliptic curves $E/\mathbb{Q}$, up to isomorphism, for which the Mordell-Weil group $E(\mathbb{Q})$ has rank exactly 2.[5]

Zywina's proof involves constructing an explicit one-parameter family of elliptic curves over $\mathbb{Q}(T)$ that has rank 2. He then uses a deep result from additive combinatorics, the polynomial Szemerédi theorem of Tao and Ziegler, to show that there are infinitely many rational specializations $t \in \mathbb{Q}$ for which the resulting elliptic curve over $\mathbb{Q}$ has rank exactly 2, proven via a direct 2-descent computation.[5]

The question of whether the rank of elliptic curves over $\mathbb{Q}$ is bounded or unbounded remains a major open problem. For decades, the record for the highest-known rank stood at 28, a curve found by Noam Elkies. Very recently, in late 2024, Elkies and Zev Klagsbrun announced the discovery of a curve with rank at least 29, breaking the long-standing record and breathing new life into the debate.[79] These constructions, while not providing a general theory, serve as crucial test cases and demonstrate the extreme arithmetic complexity that elliptic curves can exhibit.

6.3. Generalized Heegner Cycles and New Euler Systems

The most ambitious and theoretically deep research program aimed at tackling the higher rank case involves generalizing the Heegner point construction. The hope is to find analogous "special cycles" on more complicated algebraic varieties that could play the role of Heegner points for higher derivatives of L-functions. This has led to the study of *generalized Heegner cycles* on varieties fibered over modular curves, such as Kuga-Sato varieties or products of an elliptic curve with a CM elliptic curve.[80]

These generalized Heegner cycles are algebraic cycles supported on fibers above CM points, defined over abelian extensions of imaginary quadratic fields. The central conjecture is that the heights of these cycles (or more generally, their images under a p-adic Abel-Jacobi map) should be related to the values of higher derivatives of Rankin L-series. For example, the height of a generalized Heegner cycle on a variety X_r might be related to the central value of the $(r+1)$-th derivative of a Rankin

L-function. If such a formula could be established, it might provide a way to construct a non-trivial Euler system for an elliptic curve of rank r+1. This research program, pursued by Darmon, Rotger, and others, is at the absolute frontier of the field, requiring a deep synthesis of the theory of automorphic forms, p-adic Hodge theory, and the arithmetic of algebraic cycles.[81]

6.4. The Role of Computation and New Phenomena

As theoretical progress on higher rank curves faces formidable obstacles, computational work continues to push the boundaries of our knowledge. The numerical verification of the strong BSD conjecture is being extended to abelian varieties of higher dimension, such as the Jacobians of genus 2 curves. The work of van Bommel, Stoll, Keller, and others has provided exact verification of the strong BSD conjecture for hundreds of abelian surfaces, including cases where the Shafarevich-Tate group is non-trivial.[16] These computations provide crucial test cases for the general theory and refine the algorithms needed to compute the various terms in the BSD formula.

In a surprising recent development, the application of machine learning techniques to the vast dataset of elliptic curves in the LMFDB has revealed a completely new phenomenon. In 2022, He, Lee, Oliver, and Pozdnyakov discovered unexpected statistical patterns in the sequences of ap coefficients, which they dubbed "murmurations".[25] They found that when averaging the

ap values over large families of curves, the resulting plots form distinct, oscillating waves that cleanly separate curves of rank 0 from curves of rank 1. This discovery, which was made possible by modern data science techniques, suggests that there are deep, underlying structural regularities in the arithmetic of elliptic curves that are not yet understood theoretically. Recent work has begun to provide theoretical explanations for these murmurations, connecting them to the properties of Hecke operators and root numbers, but the full picture is still emerging.[87] This points to a new era of computer-assisted discovery in number theory, where data-driven approaches may uncover patterns that guide future theoretical development.

6.5. Concluding Remarks

The landscape of research on elliptic curves is currently characterized by a fascinating bifurcation. On one hand, the statistical approach pioneered by Bhargava and his collaborators has achieved stunning success, proving that the BSD conjecture holds for a majority of elliptic curves without needing to resolve the conjecture for any single curve of rank greater than one. This approach leverages the power of averages and density theorems to make broad, sweeping statements. On the other hand, the structural approach, which seeks to understand the mechanics of individual curves, has been forced into ever deeper and more abstract territory to confront the challenge of higher rank. The study of generalized Heegner cycles, p-adic Rankin L-series, and new Euler systems represents a formidable but potentially revolutionary path toward a general proof of the BSD conjecture.

The future of the field likely lies in the eventual synthesis of these two approaches. Perhaps the statistical patterns of the murmurations will provide the necessary clues to construct the correct generalized cycles for higher rank curves. Conversely, a deeper understanding of the geometry of these generalized cycles might provide a theoretical explanation for the observed statistical biases. The journey to understand the arithmetic of elliptic curves, which began with simple questions about integer solutions to cubic equations, has led to the development of some of the most profound and powerful tools in modern mathematics. It has required a synthesis of complex analysis, abstract algebra, algebraic geometry, representation theory, and, increasingly, large-scale computation and data science. The Birch and Swinnerton-Dyer conjecture, elegant and simple in its statement, remains a central organizing principle in this grand endeavor, and its pursuit continues to generate some of the deepest and most beautiful mathematics of our time.

Works cited

1. Catalogue of GP/PARI Functions: Elliptic curves, accessed July 11, 2025, https://pari.math.u-bordeaux.fr/dochtml/html/Elliptic_curves.html
2. The conjecture of Birch and Swinnerton-Dyer - University of Warwick, accessed July 11, 2025, https://warwick.ac.uk/fac/sci/maths/people/staff/turcas/piii-essay.pdf
3. The BSD Conjecture: A Deep Dive - Number Analytics, accessed July 11, 2025, https://www.numberanalytics.com/blog/deep-dive-bsd-conjecture
4. Arithmetic of Elliptic Curves: Theory and Applications - Number Analytics, accessed July 11, 2025, https://www.numberanalytics.com/blog/arithmetic-elliptic-curves-theory-applications
5. There are infinitely many elliptic curves over the rationals of rank 2 - Cornell

Mathematics, accessed July 11, 2025, https://pi.math.cornell.edu/~zywina/papers/Rank2.pdf
6. Elliptic curve with LMFDB label 37.a1 (Cremona label 37a1) - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/EllipticCurve/Q/37/a/1
7. Conductor of an elliptic curve (reviewed) - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/knowledge/show/ec.conductor
8. LMFDB - The L-functions and modular forms database, accessed July 11, 2025, https://www.lmfdb.org/
9. LMFDB, the L-functions and modular forms database - MathBases, accessed July 11, 2025, https://mathbases.org/d/lmfdb
10. THE L-FUNCTIONS AND MODULAR FORMS DATABASE PROJECT - John Cremona, accessed July 11, 2025, https://johncremona.github.io/papers/lmfdb_article.pdf
11. Elliptic curves: statistics - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/EllipticCurve/stats
12. The L-functions and Modular Forms DataBase - MIT Mathematics, accessed July 11, 2025, https://math.mit.edu/~roed/writings/talks/2022_05_22.pdf
13. Birch and Swinnerton-Dyer conjecture - Wikipedia, accessed July 11, 2025, https://en.wikipedia.org/wiki/Birch_and_Swinnerton-Dyer_conjecture
14. THE p-PARITY CONJECTURE FOR ELLIPTIC CURVES WITH A p-ISOGENY, accessed July 11, 2025, https://www.imo.universite-paris-saclay.fr/~kestutis.cesnavicius/p-parity-p-isogeny.pdf
15. The current status of the Birch & Swinnerton-Dyer Conjecture - MathOverflow, accessed July 11, 2025, https://mathoverflow.net/questions/11502/the-current-status-of-the-birch-swinnerton-dyer-conjecture
16. Numerical verification of BSD - for hyperelliptics of genus 2 & 3, and ..., accessed July 11, 2025, https://people.maths.bris.ac.uk/~matyd/BSDData/R%20v%20Bommel%20-%20Numerical%20verification%20of%20BSD.pdf
17. Complete verification of strong BSD for many modular abelian ..., accessed July 11, 2025, https://www.mathe2.uni-bayreuth.de/stoll/papers/FiniteSupport.pdf
18. Regulator of an elliptic curve (reviewed) - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/knowledge/show/ec.regulator
19. Tate–Shafarevich group - Wikipedia, accessed July 11, 2025, https://en.wikipedia.org/wiki/Tate%E2%80%93Shafarevich_group
20. Elliptic curve data - 37.a1 - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/EllipticCurve/Q/data/37.a1
21. Some interesting elliptic curves over $\Q - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/EllipticCurve/Q/interesting
22. Elliptic Curves — Thematic Tutorials v9.3.beta9, accessed July 11, 2025, http://sporadic.stanford.edu/thematic_tutorials/explicit_methods_in_number_theory/elliptic_curves.html
23. Elliptic curve isogeny class with LMFDB label 5077.a (Cremona label 5077a),

accessed July 11, 2025, https://www.lmfdb.org/EllipticCurve/Q/5077.a/
24. A Spectral Hamiltonian Approach to Solving the Birch and ... - OSF, accessed July 11, 2025, https://osf.io/gnxza_v2/download/?format=pdf
25. Elliptic Curve 'Murmurations' Found With AI Take Flight | Quanta Magazine, accessed July 11, 2025, https://www.quantamagazine.org/elliptic-curve-murmurations-found-with-ai-take-flight-20240305/
26. The L-functions and Modular Forms Database (LMFDB) - MIT Mathematics, accessed July 11, 2025, https://math.mit.edu/~drew/ICMS2020.pdf
27. Elliptic curve 256.6-a1 over number field \(\Q(\sqrt{-7}) \) - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/EllipticCurve/2.0.7.1/256.6/a/1
28. Magma code - Day 4.txt, accessed July 11, 2025, https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-Magma-code-DAY4.pdf
29. Code to SageMath - LMFDB, accessed July 11, 2025, https://www.lmfdb.org/EllipticCurve/Q/197714/l/1/download/sage?label=197714.l1
30. Heegner point - Wikipedia, accessed July 11, 2025, https://en.wikipedia.org/wiki/Heegner_point
31. Heegner Points: The Key to Unlocking Elliptic Curve Mysteries - Number Analytics, accessed July 11, 2025, https://www.numberanalytics.com/blog/heegner-points-elliptic-curve-mysteries
32. Heegner points and derivatives of L-series. - EUDML, accessed July 11, 2025, https://eudml.org/doc/143341
33. @let@token Verifying the Full Birch and Swinnerton-Dyer Conjecture in Specific Cases - William Stein, accessed July 11, 2025, https://wstein.org/talks/2006-12-waterloo/bsd/bsd.pdf
34. Heegner Points on Rank Two Elliptic Curves (Preliminary Version) - William Stein, accessed July 11, 2025, https://wstein.org/misc/sagedays18_papers/stein-heegner_points_on_rank_two_elliptic_curves.pdf
35. Kolyvagin's Euler system and Ciperiani-Wiles, accessed July 11, 2025, https://www.math.ucla.edu/~ntg/Seminars/f07-kolyvagin/
36. Kolyvagin's Theorem: A Deep Dive - Number Analytics, accessed July 11, 2025, https://www.numberanalytics.com/blog/deep-dive-kolyvagin-theorem-number-theory
37. Euler systems Karl Rubin, accessed July 11, 2025, https://swc-math.github.io/notes/files/99RubinES.pdf
38. Review of “Euler Systems” by Karl Rubin, accessed July 11, 2025, https://www.math.mcgill.ca/darmon/pub/Articles/Expository/08.Rubin-Review/paper.pdf
39. What's the difference between Euler systems and Kolyvagin systems? - MathOverflow, accessed July 11, 2025, https://mathoverflow.net/questions/203215/whats-the-difference-between-euler-systems-and-kolyvagin-systems
40. finiteness of e(q) and iii(e,q) for a subclass of weil curves, accessed July 11, 2025,

https://wstein.org/papers/bib/kolyvagin-finitess_of_EQ_and_sha_for_a_subclass.pdf
41. FINITENESS OF AND FOR A SUBCLASS OF WEIL CURVES - ResearchGate, accessed July 11, 2025, https://www.researchgate.net/publication/231112762_FINITENESS_OF_AND_FOR_A_SUBCLASS_OF_WEIL_CURVES
42. Title, Abstract and References | ICTS, accessed July 11, 2025, https://www.icts.res.in/event/page/21582
43. Kolyvagin's conjecture - lccs - Columbia Math Department, accessed July 11, 2025, https://www.math.columbia.edu/~chaoli/docs/KolyvaginConjecture.html
44. PDF - American Mathematical Society, accessed July 11, 2025, https://www.ams.org/journals/bull/2002-39-03/S0273-0979-02-00939-4/S0273-0979-02-00939-4.pdf
45. Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over Q up to squares - arXiv, accessed July 11, 2025, https://arxiv.org/pdf/1711.10409
46. Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one | LMS Journal of Computation and Mathematics - Cambridge University Press, accessed July 11, 2025, https://www.cambridge.org/core/journals/lms-journal-of-computation-and-mathematics/article/proving-the-birch-and-swinnertondyer-conjecture-for-specific-elliptic-curves-of-analytic-rank-zero-and-one/A12F4BBC7DDB743A028986EA2C124786
47. Kolyvagin's Euler Systems Matemática Aplicada e Computaç˜ao - Fenix, accessed July 11, 2025, https://fenix.tecnico.ulisboa.pt/downloadFile/1970719973969956/Kolyvagins%20Euler%20Systems.pdf
48. the iwasawa main conjectures for gl2 - christopher skinner and eric urban - Columbia Math Department, accessed July 11, 2025, https://www.math.columbia.edu/~urban/eurp/MC.pdf
49. Introduction to Skinner-Urban's Work on the Iwasawa Main Conjecture for GL2, accessed July 11, 2025, http://www.mcm.ac.cn/faculty/wx/201609/W020160919378831326945.pdf
50. Main conjecture of Iwasawa theory - Wikipedia, accessed July 11, 2025, https://en.wikipedia.org/wiki/Main_conjecture_of_Iwasawa_theory
51. Mastering the Main Conjecture - Number Analytics, accessed July 11, 2025, https://www.numberanalytics.com/blog/mastering-main-conjecture-iwasawa-theory
52. p-adic Hodge theory and values of zeta functions of ... - Numdam, accessed July 11, 2025, https://www.numdam.org/article/AST_2004__295__117_0.pdf
53. An introduction to Kato's Euler systems - AJ Scholl - DPMMS, accessed July 11, 2025, https://www.dpmms.cam.ac.uk/~ajs1005/preprints/euler.pdf
54. p-adic Hodge theory and Bloch-Kato theory - Centro de Ciencias de Benasque Pedro Pascual, accessed July 11, 2025, https://www.benasque.org/2015numbers/slides/BrunoJoyal.pdf

55. INTEGRAL p-ADIC HODGE THEORY AND RAMIFICATION OF CRYSTALLINE REPRESENTATIONS, accessed July 11, 2025, https://www.comm.tcu.ac.jp/~shinh/RennesHodge/RennesHodge.pdf
56. The Iwasawa Main Conjectures for GL2 - ResearchGate, accessed July 11, 2025, https://www.researchgate.net/publication/228543726_The_Iwasawa_Main_Conjectures_for_GL2
57. A Majority of Curves Over Q Satisfy BSD - Scribd, accessed July 11, 2025, https://www.scribd.com/document/721367464/A-majority-of-curves-over-Q-satisfy-BSD
58. Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves | Annals of Mathematics, accessed July 11, 2025, https://annals.math.princeton.edu/2015/181-1/p03
59. Mathematics Items | Not Even Wrong - Columbia Math Department, accessed July 11, 2025, https://www.math.columbia.edu/~woit/wordpress/?p=7037
60. The BSD conjecture is true for most elliptic curves - Matt Baker's Math Blog, accessed July 11, 2025, https://mattbaker.blog/2014/03/10/the-bsd-conjecture-is-true-for-most-elliptic-curves/
61. Average rank of elliptic curves over function fields - MathOverflow, accessed July 11, 2025, https://mathoverflow.net/questions/157999/average-rank-of-elliptic-curves-over-function-fields
62. The average size of the 2-Selmer group of Jacobians of hyperelliptic ..., accessed July 11, 2025, https://people.math.harvard.edu/~gross/preprints/stable23.pdf
63. The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point - ResearchGate, accessed July 11, 2025, https://www.researchgate.net/publication/230609377_The_average_size_of_the_2-Selmer_group_of_Jacobians_of_hyperelliptic_curves_having_a_rational_Weierstrass_point
64. Ternary cubic forms having bounded invariants, and the existence of ..., accessed July 11, 2025, https://annals.math.princeton.edu/2015/181-2/p04
65. The average number of elements in the 4-Selmer groups of elliptic curves is 7 - Semantic search for arXiv papers with AI, accessed July 11, 2025, https://axi.lims.ac.uk/paper/1312.7333
66. The average number of elements in the 4-Selmer groups of elliptic curves is 7 - arXiv, accessed July 11, 2025, https://arxiv.org/abs/1312.7333
67. The average 5-Selmer rank of elliptic curves Arul Shankar - Boston University, accessed July 11, 2025, http://math.bu.edu/research/algebra/Fall2013/Shankar.pdf
68. The average size of the 5-Selmer group of elliptic curves is 6, and ..., accessed July 11, 2025, https://arxiv.org/abs/1312.7859
69. arxiv.org, accessed July 11, 2025, https://arxiv.org/abs/1203.0809#:~:text=Bhargava%20and%20Shankar%20prove%20that,E(Q)%20is%20bounded.
70. [1203.0809] Average rank of elliptic curves - arXiv, accessed July 11, 2025, https://arxiv.org/abs/1203.0809

71. The 2-parity conjecture for elliptic curves with isomorphic 2-torsion - ResearchGate, accessed July 11, 2025, https://www.researchgate.net/journal/Proceedings-of-the-Royal-Society-A-1471-2946/publication/363355374_The_2-parity_conjecture_for_elliptic_curves_with_isomorphic_2-torsion/links/648ca69595bbbe0c6ecd2743/The-2-parity-conjecture-for-elliptic-curves-with-isomorphic-2-torsion.pdf
72. The parity conjecture - elliptic curves - MathOverflow, accessed July 11, 2025, https://mathoverflow.net/questions/71609/the-parity-conjecture
73. The parity conjecture for elliptic curves at supersingular reduction primes | Compositio Mathematica - Cambridge University Press & Assessment, accessed July 11, 2025, https://www.cambridge.org/core/journals/compositio-mathematica/article/parity-conjecture-for-elliptic-curves-at-supersingular-reduction-primes/0E3D32365B9D4E53B008D265B1E6EEA0
74. Tim Dokchitser's home page, accessed July 11, 2025, https://people.maths.bris.ac.uk/~matyd/
75. A majority of elliptic curves over $\mathbb Q$ satisfy the Birch and ..., accessed July 11, 2025, https://www.researchgate.net/publication/263736562_A_majority_of_elliptic_curves_over_mathbb_Q_satisfy_the_Birch_and_Swinnerton-Dyer_conjecture
76. Any recent work on the BSD conjecture that you might know about? : r/mathematics - Reddit, accessed July 11, 2025, https://www.reddit.com/r/mathematics/comments/1jbhxaj/any_recent_work_on_the_bsd_conjecture_that_you/
77. There Are Infinitely Many Elliptic Curves Over the Rationals of Rank 2 - David Zywina, accessed July 11, 2025, https://www.youtube.com/watch?v=5VR_RybJeNw
78. There are infinitely many elliptic curves over the rationals of rank 2 - arXiv, accessed July 11, 2025, https://arxiv.org/html/2502.01957v1
79. New Elliptic Curve Breaks 18-Year-Old Record - Quanta Magazine, accessed July 11, 2025, https://www.quantamagazine.org/new-elliptic-curve-breaks-18-year-old-record-20241111/
80. Heegner Points and Generalised Heegner Cycles - ETH Zürich, accessed July 11, 2025, https://people.math.ethz.ch/~avego/Master_thesis-Vego.pdf
81. GENERALIZED HEEGNER CYCLES AND p-ADIC RANKIN L-SERIES - McGill University, accessed July 11, 2025, https://www.math.mcgill.ca/darmon/pub/Articles/Research/51.BDP1/duke-publisheddversion.pdf
82. GENERALISED HEEGNER CYCLES AND p-ADIC RANKIN L-SERIES, accessed July 11, 2025, https://www.math.mcgill.ca/darmon/pub/Articles/Research/51.BDP1/paper.pdf
83. Generalized heegner cycles and p-adic rankin L-series - SciSpace, accessed July 11, 2025, https://scispace.com/pdf/generalized-heegner-cycles-and-p-adic-rankin-l-series

-1m3rmm8iyo.pdf
84. Kolyvagin's Conjecture for Specific Higher Rank Elliptic Curves - William Stein, accessed July 11, 2025, https://wstein.org/papers/kolyconj2/kolyconj.pdf
85. Exact verification of the strong BSD conjecture for some absolutely simple abelian surfaces, accessed July 11, 2025, https://www.mathe2.uni-bayreuth.de/stoll/papers/BSD-ModAbSurf1.pdf
86. Complete verification of strong BSD for many modular abelian surfaces over ${\mathbf {Q}}$ | Forum of Mathematics, Sigma | Cambridge Core, accessed July 11, 2025, https://www.cambridge.org/core/product/8154162660F5F225C45787570719D85D
87. arXiv:2403.17626v1 [math.NT] 26 Mar 2024, accessed July 11, 2025, https://arxiv.org/pdf/2403.17626