REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Birch and Swinnerton-Dyer conjecture: old and new

*Óscar Rivero-Salgado
Universitat Politècnica de Catalunya
oscar.rivero@upc.edu
∗Corresponding author

Resum *(CAT)*

La conjectura de Birch i Swinnerton-Dyer (BSD) és un dels sis problemes del mil·lenni que encara no s'ha resolt. Tot i que es va formular després de diferents experiments numèrics, hi ha diverses raons teòriques i analogies amb objectes matemàtics més senzills que ens fan pensar que l'enunciat és cert. Repassarem primer algunes d'aquestes motivacions i explicarem els resultats i generalitzacions més rellevants que es coneixen. A la darrera part ens apropem al mon en el que el rang analític és dos, una situació poc treballada, i ens trobem així amb la conjectura el·líptica de Stark, molt relacionada amb BSD.

Abstract *(ENG)*

The Birch and Swinnerton-Dyer (BSD) conjecture is one of the millennium problems that has not been solved yet. Although it was formulated after different numerical experiments, there are several theoretical reasons and analogies with simpler mathematical objects that lead us to believe that it is true. We go through some of these analogies, and at the same time, we explain the most relevant results and generalizations that are currently known. At the end, we move to the rank two situation, recovering the elliptic Stark conjecture, closely related to BSD.

Keywords: *BSD, elliptic curve, L-series, modular forms, Gross–Zagier Stark conjecture.*
MSC (2010): *11G18, 14G35.*
Received: *April 17, 2017.*
Accepted: *October 28, 2018.*

Acknowledgement

The author thanks V. Rotger for his advice during the realization of this project, which is part of his bachelor thesis. He also thanks the referee for comments that contributed to improve the quality of this presentation.

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

1. Introduction

During the first half of the 1960s, mathematicians Bryan Birch and Peter Swinnerton-Dyer formulated, after having performed different numerical computations, a conjecture relating the rank of an elliptic curve over a number field with the order of vanishing of the corresponding L-series at the point $s = 1$, lying outside the region of convergence of the defining series. The conjecture asserts that the rank of the elliptic curve (also called the algebraic rank) agrees with the order of vanishing of the L-series at $s = 1$ (the analytic rank), and moreover, it gives a formula for the first non-zero coefficient in the Taylor development of this L-series. At that time, not much knowledge concerning the theory of elliptic curves was available. In the thirties, Mordell had proved the finiteness of the rank for an elliptic curve defined over $\mathbb{Q}$, and then Weil generalized the proof to the case of number fields. It was also Weil who did a more detailed study of the L-series attached to a projective variety, which allowed to have a broaden perspective of the real meaning of this analytic object. There was a lot of progress along the 20-th century, that culminated with the proof of the modularity theorem, first by Taylor and Taylor–Wiles for the case of elliptic curves over $\mathbb{Q}$ with semistable reduction, and then in the general case (but again only over $\mathbb{Q}$) by Breuil, Conrad, Diamond and Taylor. This theorem allows to attach to an elliptic curve a normalized modular form of weight two with the same L-series, which turns out to be useful in many different settings (for instance, to prove the analytic continuation and the functional equation of the L-series of the elliptic curve).

However, in spite of all this great progress in number theory, the conjecture of Birch and Swinnerton-Dyer remains unsolved and only some special cases have been proved. The most remarkable result was obtained by Gross–Zagier and Kolyvagin, who proved the conjecture in analytic rank at most one. For that, they made use of what is known as an Euler system, a compatible collection of cohomology classes along a tower of fields. In this case, it is the Euler system of Heegner points. However, Heegner points are futile in analytic rank greater than one since they are torsion. In those settings, new tools based on p-adic methods have recently been introduced and the interested reader is referred to [1, 2, 3, 7, 9] for a wider perspective.

The organization of this note is as follows. First of all, Section 2 gives a motivation for the conjecture based on the parallelism with the finiteness results available for the group of units of a number field. Our last aim in this section is to present the statement of the conjecture. Then, in Section 3 we state some of the most interesting results and generalizations of the BSD conjecture, particularly the so-called equivariant BSD. Finally, Section 4 explores some of the new insights when the analytic rank is greater than one, and in particular we recover the elliptic Stark conjecture, where the parallelism between units in number fields and points in elliptic curves is again present. For some results about elliptic curves, L-series and modular curves that we freely use along the exposition, we refer to the excellent book [4].

2. Motivation for the BSD conjecture

2.1 First analogies

There are two main reason that make the BSD conjecture specially appealing at first sight: it can be seen as a local-global principle, and at the same time, it makes a link between the algebraic side (the rank of the elliptic curve) and the analytic side (the L-function). We go more carefully through each of these points:

(i) The BSD conjecture can be understood as a local-global principle. The L-function is an analytic object obtained by gluing different pieces that are constructed just counting points over finite fields. From it, we expect to derive some properties about the global behavior (the rank of the elliptic curve over $\mathbb{Q}$ or more generally over a number field). This follows the spirit of Hasse–Minkowski theorem, which states that a homogeneous quadratic form represents 0 over $\mathbb{Q}$ if and only if it represents 0 in all the completions of the rational numbers (the real numbers $\mathbb{R}$ and the p-adic fields $\mathbb{Q}_p$, for the different rational primes p).

However, we know that the Hasse principle is not true for cubic curves, as Selmer showed with his celebrated example $3x^3 + 4y^3 + 5z^3 = 0$, so in general we cannot expect a generalization of this result. This would be something similar to expect that one can prove that a polynomial with integer coefficients is irreducible over $\mathbb{Q}$ just by knowing that is irreducible over all the finite fields $\mathbb{F}_p$. Some examples showing that this is false are the polynomials $x^4 + 1$ or $x^4 - 10x^2 + 1$ (in particular, any irreducible degree four polynomial whose Galois group over $\mathbb{Q}$ is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, or more generally any irreducible degree n polynomial whose Galois group does not contain an n-cycle). The point is that there is an ubiquitous group, the Tate–Shafarevich group, that measures the failure to the Hasse principle, and we expect that for elliptic curves this group is finite.

(ii) The BSD conjecture gives a relation between the algebraic or geometric side (the rank of the elliptic curve) and the analytic side (the L-series). This gives a connection with another remarkable conjecture, the Bloch–Kato conjecture, that also establishes a link between the rank of vanishing of an L-series and the dimension of appropriate cohomology groups. In particular, we will see that when trying to generalize the Gross–Zagier formula to analytic rank greater than one we necessarily pass through some construction of families of compatible cohomology classes, for which some *explicit reciprocity laws* connecting these classes with appropriate L-functions are available. It turns out that proving this kind of equalities is easier in the p-adic world than in the complex one.

As we have suggested, elliptic curves over a number field are not as easy to understand as one may expect at first sight, so it is natural to look for *simpler* analogies, such as the *ring of integers of a number field*. There are two main remarkable results that come from Minkowski's theorem, that asserts that a set in $\mathbb{R}^n$ which is big enough must contain a rational point: these two results are the finiteness of the class number and the finite generation of the group of units. We would like to look for analogues in the case of an elliptic curve:

(i) The analogue of the rank of the group of units is the rank of the elliptic curve. Both of them are known to be finite and in fact the proof of the Mordell–Weil theorem makes use of the classical result for number fields. This last analogy is specially relevant. We will see how the L-series of the number field encodes information about the rank of the group of units, and we expect the same for elliptic curves via the BSD conjecture.

(ii) One may think that the natural analogue of the class group is the Picard group, that can be defined for any ringed space X as the first cohomology group $H^1(X, \mathcal{O}_X^\times)$. In the case of curves, it turns out to be isomorphic to the jacobian of the curve, that for an elliptic curve is the elliptic curve itself. However, there is another object that we later present, the *Tate–Shafarevich group*, which turns out to be a more appropriate analogue. However, proving its finiteness is equally hard and again, results are limited to situation of analytic rank at most one.

2.2 The L-function of an elliptic curve

L-series are analytic functions attached to motives, which are essentially pieces of the cohomology of a variety over a field. In particular, when M is a motive over $\mathbb{Q}$ with coefficients in a field $E \subset \mathbb{C}$, we may attach to it the complex L-function $L(M,s) = \prod_p P_{M,p}(p^{-s})^{-1}$, where the product runs over all rational primes and $P_{M,p}$ is the characteristic polynomial (suitably normalized) of the Frobenius at p, Frob_p, acting on the motive M of weight w. It converges on $\Re(s) > 1 + w/2$.

The easiest example is concerned with a Dirichlet character $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$. In this case, the identification $(\mathbb{Z}/N\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/N})/\mathbb{Q})$ allows us to work from the perspective of Galois representations. In a natural way, one can construct $\rho_\chi : G_\mathbb{Q} \to \mathbb{C}^\times \simeq \mathrm{GL}_1(\mathbb{C})$ as the composition of the projection $G_\mathbb{Q} \to \mathrm{Gal}(\mathbb{Q}(e^{2\pi i/N})/\mathbb{Q})$ with the character χ. With this approach, the local factor $P_{M,p}(p^{-s})$ is nothing but the characteristic polynomial of $\rho_\chi(\mathrm{Frob}_p)$, for a choice of Frob_p. Alternatively, this local factor corresponds to the Frobenius acting on the p-torsion of $\mathbb{C}^\times$ (the multiplicative group generated by ζ_p), and it is just $1/(1-\chi(p)p^{-s})$ (as a Galois character, χ acts as $\zeta_p \mapsto \zeta_p^{\chi(p)}$). Then, we obtain the L-function

$$L(\chi,s) = \prod_{p\nmid N} \frac{1}{1-\chi(p)p^{-s}},$$

that in the particular case that χ is identically one agrees with the usual zeta-function. This function can be analytically continued to the whole complex plane (this is a classical result in complex analysis).

This same study can be done for a general number field, and then the corresponding L-function encodes information about all the primes of that number field. In particular, given a number field K and $\rho\colon G_K \to \mathrm{GL}(V)$,

$$L(\rho,s) = \prod_{\mathfrak{p}\subset\mathcal{O}_K} \frac{1}{P_{\rho,\mathfrak{p}}(\mathbb{N}_{K/\mathbb{Q}}(\mathfrak{p})^{-s})}.$$

When ρ is the trivial representation, we obtain the usual Dedekind zeta function of the number field K, ζ_K. It converges absolutely for $\Re(s) > 1$ and it extends to a meromorphic function defined for all complex numbers s and with a simple pole at $s = 1$. The following result is a wonderful analogy for BSD, since we can see how in some sense the value at $s = 1$ allows us to recover arithmetic information. This is the so-called class number formula:

$$\lim_{s\to 1}(s-1)\cdot\zeta_K(s) = \frac{2^{r_1}\cdot(2\pi)^{r_2}\cdot h_K\cdot \mathrm{Reg}_K}{w_K\cdot\sqrt{|D_K|}},$$

where we have made use of the usual conventions of writing r_1, r_2 for the number of real embeddings and half of the complex embeddings of K, respectively; h_K for the class number; Reg_K for the regulator of the number field; w_K for the number of roots of unity in K and D_K for the discriminant of $K/\mathbb{Q}$. Many cases of this result can be more deeply analyzed in the realm of class field theory.

In the case of an elliptic curve (say over $\mathbb{Q}$), the way to introduce the L-function is to consider the Galois action over the so-called Tate module. The construction we describe may seem ad-hoc but it really works in a more general framework and can be extended to more general algebraic varieties. Recall that in the number field case we have used the p-torsion of $\mathbb{C}^\times$ (the group generated by ζ_p), so now we can consider the p-torsion of an elliptic curve. Take $E/\mathbb{Q}$ an elliptic curve. When p is a prime of good reduction (the cubic curve modulo p is still non-singular), it turns out that the p-torsion over $\bar{\mathbb{Q}}$ (denoted by $E[p]$) is a finite group isomorphic to $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ which respects the action of the Galois group, so we have a

morphism $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Since this can also be done for $E[p^n]$, taking projective limits we get a representation (that we denote with the same letter) $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}_p)$. This projective limit is called the Tate module.

It is quite easy to prove (see [13, Ch. 5] for more details) that the characteristic polynomial of Frob_p acting on the p-torsion evaluated at p^{-s} is $1 - a_p(E)p^{-s} + p^{1-2s}$ for the primes of good reduction. Then,

$$L(E,s) = \prod_{p \text{ good}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \text{ bad}} \frac{1}{1 - a_p p^{-s}},$$

where the extra factors correspond to the primes of bad reduction. A priori, it may not be clear that this function could be analytically continued, and in fact this is a consequence of the work of Wiles and others towards the proof of the modularity theorem. The idea is based on the introduction of the so-called modular forms, that are functions on the upper half-plane satisfying certain transformation properties, the so-called *modular forms*. The symbol $S_2(N)$ arises for the *weight two* modular forms of level N. vanishing at infinity.

Theorem 2.1 (Modularity)**.** *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Then, there exists a modular form $f \in S_2(N)$ such that $L(E,s) = L(f,s)$.*

This means that the coefficients $a_p(E) = p + 1 - \sharp E(\mathbb{F}_p)$ agree with the Fourier coefficients of the modular form f.

Corollary 2.2. *The L-function $L(E,s)$ has an analytic continuation and an integral representation of the form*

$$(2\pi)^{-s}\Gamma(s)L(E,s) = \int_0^\infty f(it)t^{s-1}dt.$$

2.3 Curves of genus zero

Before giving our first formulation of BSD, we can try to study another analogy for curves of genus zero. In particular, let us investigate some local-global properties for conics in a different setting. Consider for instance the circle $x^2 + y^2 = 1$ and count solutions modulo a certain prime. These solutions can be parameterized following the usual method of considering lines through a fixed point of the conic. That way, we get that all the solutions are given in terms of a variable t in the form

$$(x,y) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right),$$

so the number of solutions is $p-1$ or $p+1$, since t^2+1 has either zero or two solutions modulo p depending on the residue of p modulo 4 (this works for odd p). Then, we can consider the proportion between the number of points modulo a certain prime and the size of the prime, and multiplying all the quotients we directly get

$$\prod_p \frac{p}{N_p} = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{2n-1} = \frac{\pi}{4},$$

where the last equality follows from Wallis formula. If we denote by $N_{\mathbb{R}}$ the measure of the "real solutions" (the length of the unit circle), we get a very curious result:

$$\prod_p \frac{N_p}{p} \cdot N_{\mathbb{R}} = \frac{4}{\pi} \cdot 2\pi = 8,$$

that is precisely twice the number of integer solutions of $x^2 + y^2 = 1$.

Observe that for counting the number of points over $\mathbb{F}_p$ in the case of elliptic curves, an heuristic argument (that may seem naïve at first sight) is the following. Taking the Weierstrass equation $y^2 = x^3 + Ax + B =: f(x)$, for each value of x modulo p we can obtain either that $f(x) = 0$ (one solution), that $f(x)$ is a non-zero square (two solutions) or that it is a non-square (zero solutions). Since these two last cases occur the same number of times, we expect in average $p + 1$ solutions (considering the point at infinity). The truth is that Hasse's bound is precisely $a_p = |p + 1 - \#E(\mathbb{F}_p)| < 2\sqrt{p}$, which can be seen as some kind of Riemann hypothesis for elliptic curves, since from here we may define a certain zeta function, and Hasse's bound implies that the zeros of this zeta function has real part $1/2$. Then, it makes sense again to consider the quantity

$$f(T) = \prod_{p \leq T} \frac{N_p}{p}.$$

One of the first versions preceding BSD was the following one:

Conjecture 2.3. *For each elliptic curve E over $\mathbb{Q}$, there exists a constant C such that $\lim_{T \to +\infty} f(T) = C \cdot \log(T)^r$, where r is the rank of the elliptic curve. Roughly speaking, "many points over the different $\mathbb{F}_p$ force many points over $\mathbb{Q}$".*

2.4 The BSD conjecture

At this point of the discussion, we are in conditions of presenting the extended version of the BSD conjecture. However, the reader should note that it is enough to prove that the rank of $E/\mathbb{Q}$ equals the order of vanishing at $s = 1$ of $L(E, s)$ in order to receive the prize of the Clay Mathematical Institute.

Conjecture 2.4. *Let r be the rank of $E(\mathbb{Q})$ and $P_1, \dots, P_r$ be linearly independent elements of $E(\mathbb{Q})$. Then,*

$$\lim_{s \to 1} \frac{L(E, s)}{(s-1)^r} = \left(\Omega \prod_{p \text{ bad}} c_p\right) \frac{\text{Sha}(E/\mathbb{Q}) \det(\langle P_i, P_j \rangle)}{(\#E_{\text{tors}})^2},$$

where $\Omega = \int_{E(\mathbb{R})} |\omega|$ is the integral of the canonical differential; c_p corresponds to the bad reduction prime p raised to some explicit power and $\text{Sha}(E/\mathbb{Q})$ is the order of the Tate–Shafarevich group.

This Tate–Shafarevich group is an important actor in the different versions of BSD and measures the failure to the Hasse principle. To properly introduce it, let us define it together with the n-th Selmer group, $S^{(n)}(E/\mathbb{Q})$.

$$\begin{aligned} S^{(n)}(E/\mathbb{Q}) &= \{\gamma \in H^1(\mathbb{Q}, E[n]) \mid \text{ for all } p, \gamma_p \text{ comes from } E(\mathbb{Q}_p)\} \\ &= \ker\left(H^1(\mathbb{Q}, E[n]) \to \prod_{p=2,3,\dots,\infty} H^1(\mathbb{Q}_p, E)\right), \end{aligned}$$

$$\text{Sha}(E/\mathbb{Q}) = \ker\left(H^1(\mathbb{Q}, E) \to \prod_{p=2,3,\dots,\infty} H^1(\mathbb{Q}_p, E)\right).$$

These two groups are related via the short exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \to S^{(n)}(E/\mathbb{Q}) \to \text{Sha}(E/\mathbb{Q})[n] \to 0.$$

It is conjectured that $\text{Sha}(E/\mathbb{Q})$ is finite. This group turns out to appear in many other situations and in general Selmer groups are a powerful tool very related with the Euler systems we will briefly present at the end of our discussion. They also arise in the formulation of the Iwasawa main conjecture, another milestone in number theory.

3. Results and generalizations

3.1 The Gross–Zagier, Kolyvagin theorem

Our next aim is to explore some of the known results around BSD conjecture. In 1976, Coates and Wiles proved that the conjecture was true in analytic rank zero (that is, when $L(E,1) \neq 0$, the algebraic rank is zero) for elliptic curves with complex multiplication (informally, curves with many endomorphisms).

The most remarkable result about BSD was proved by Gross–Zagier and Kolyvagin.

Theorem 3.1 (Gross–Zagier, Kolyvagin)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then,*

(i) if $L(E,1) \neq 0$, then $\#E(\mathbb{Q}) < \infty$ (the algebraic rank is zero);

(ii) if $L(E,1) = 0$ and $L'(E,1) \neq 0$, then the algebraic rank of the elliptic curve is one and there is an efficient method for calculating $E(\mathbb{Q})$.

In both cases $\text{Sha}(E/\mathbb{Q})$ is finite.

The proof of this result requires the introduction of an extremely powerful tool, the so-called Heegner points. In general, for an imaginary quadratic extension K of $\mathbb{Q}$, we write H_n for the ring class field of K of conductor n. A Heegner system attached to (E,K) is a collection of points $P_n \in E(H_n)$ indexed by integers n prime to N satisfying certain (explicit) norm compatibility properties. When (E,K) satisfies the Heegner hypothesis (that is, all primes dividing the conductor of E split in $K/\mathbb{Q}$), there is a non-trivial Heegner system attached to (E,K). Let $\{P_n\}_n$ be a Heegner system and let $P_K = \text{Trace}_{H_1/K}(P_1) \in E(K)$. More generally, consider $\chi : \text{Gal}(H_n/K) \to \mathbb{C}^\times$ a primitive character of a ring class field extension of K of conductor n and let

$$P_n^\chi = \sum_{\sigma \in \text{Gal}(H_n/K)} \bar{\chi}(\sigma) P_n^\sigma \in E(H_n) \otimes \mathbb{C}.$$

The following formula provides the relation between the Heegner system $\{P_n\}$ and the special values of the complex L-series $L(E/K,s)$ and its twists.

Theorem 3.2. *Let $\langle , \rangle_n$ be the canonical Néron–Tate height on $E(H_n)$ extended by linearity to a Hermitian pairing on $E(H_n) \otimes \mathbb{C}$. Then,*

(i) $\langle P_K, P_K \rangle = * L'(E/K,1)$;

(ii) $\langle P_n^\chi, P_n^{\bar{\chi}} \rangle = * L'(E/K,\chi,1)$.

Here, $*$ means equality up to a non-zero factor that can be explicitly described.

The remarkable fact in this story is that a non-trivial Heegner system, beyond yielding lower bounds on the size of the Mordell–Weil group of E over ring class fields of K, also leads to upper bounds on the Mordell–Weil group and the Shafarevich–Tate group of E/K.

Theorem 3.3. *Let $\{P_n\}$ be a Heegner system attached to (E,K). If P_K is non-torsion, then*

(i) the Mordell–Weil group $E(K)$ is of rank one, so that P_K generates a finite-index subgroup of $E(K)$;

(ii) the Shafarevich–Tate group of E/K is finite.

With these ingredients, the proof of the theorem of Gross–Zagier and Kolyvagin is relatively easy; see [4, Ch. 10].

3.2 The equivariant BSD conjecture

As it occurs in many cases, the formulation of a stronger version of the problem can help to clarify some questions around it. Let us explain now the so-called equivariant BSD conjecture. Let $K/\mathbb{Q}$ be a finite Galois extension. Then, by the Mordell–Weil theorem $E(K)\otimes\mathbb{C}\cong\oplus V_i^{r_i}$, where $r=\sum r_i\dim(V_i)<\infty$. That is, we have decomposed a representation into the sum of irreducible representations. Consider for the sake of clarity $K=\mathbb{Q}(\sqrt{-D})$; the Galois group has just a non-trivial element, say χ. Then,

$$E(K)\otimes\mathbb{C}=V_1^{r_1}\oplus V_\chi^{r_\chi}=(E(\mathbb{Q})\otimes\mathbb{C})\oplus(E(K)^\chi\otimes\mathbb{C}),$$

where the last summand is the set of elements v in $E(K)\otimes\mathbb{C}$ such that $\bar{v}=-v$. Observe that if $P\in E(K)$, then $P+\chi(P)\in E(\mathbb{Q})$ and $P-\chi(P)\in E(K)^\chi$.

We can mimic this decomposition for the L-series and express

$$L(E/K,s)=\prod_i L(E/K,V_i,s)^{\dim(V_i)},$$

in such a way that $\operatorname{ord}_{s=1}L(E/K,s)=\sum\operatorname{ord}_{s=1}L(E/K,V_i,s)\dim(V_i)$ (this V_i in the L-function refers to the twist by a certain given representation).

Again, the simplest instance of this phenomenon is the quadratic case. There, $L(E/K,\chi,s)$ can be seen as the L-function of what is called a quadratic twist of E, an elliptic curve that is isomorphic to E not over $\mathbb{Q}$, but over the quadratic extension K. For instance, the elliptic curves $y^2=x^3-x$ and $2y^2=x^3-x$ are not isomorphic over $\mathbb{Q}$, but over $\mathbb{Q}(\sqrt{2})$. Then, if D is the discriminant of the extension, we denote by $E^D: Dy^2=x^3+Ax+B$. We give a brief explanation of why in this case $L(E/K,s)=L(E,s)L(E^D,s)$, by comparing the local factors at p, where p is a prime of good reduction.

Let n_p be the number of points of E and m_p the number of points of E^D; write $a_p=p+1-n_p$ and $b_p=p+1-m_p$. When p splits in K, $Dy^2=f(x)$ has the same number of solutions than $y^2=f(x)$. Then, $a_p=b_p$ and each of the primes contributes to the L-function of the curve over K with the same factor, that is present once both in the L-function of E and E^D.

In the inert case, it is easy to check that $n_p+m_p=2+2p$ and hence $a_p+b_p=0$. Then,

$$(1-a_pp^{-s}+p^{1-2s})(1-b_pp^{-s}+p^{1-2s})=1+2p^{1-2s}+p^{2-4s}+(-a_p^2)p^{-2s}.$$

Taking into account that when p is inert its norm is p^2, what we have is that the inverse of the local factor is $1-a_{p^2}p^{-2s}+p^{2-4s}$ and everything gets reduced to proving that $a_{p^2}=a_p^2-2p$, which can be deduced from standard properties of L-series of elliptic curves; see again [13, §5.2].

Conjecture 3.4 (Equivariant BSD). *With the previous notations,* $\operatorname{ord}_{s=1} L(E/K, V_i, s) = \dim(V_i)$.

Let us briefly comment some of the cases in which this equivariant version of BSD has been proved in analytic rank zero:

(i) ρ is the odd self-dual two-dimensional Galois representation induced from a ring class (or dihedral) character of an imaginary quadratic field; this follows from the work of Gross–Zagier and Kolyvagin;

(ii) ρ is a Dirichlet character; this follows from the work of Kato;

(iii) ρ is an odd irreducible two-dimensional Galois representation satisfying mild restrictions;

(iv) ρ is an irreducible constituent of the tensor product of two odd irreducible two dimensional Galois representations which is self-dual and satisfies some other mild restrictions.

4. Rank two and beyond

One of the challenges when working with BSD it to produce tools that allow us to obtain new results in analytic rank 2 or greater. Moreover, given a Galois representation ρ with underlying vector space V_ρ defined over a number field L, when the analytic rank of $E \otimes \rho$ is positive we have the objective of constructing non-zero elements in $E(H)^\rho_L := \sum_\phi \phi(V_\rho)$, where ϕ runs over a basis of $\operatorname{Hom}_{G_\mathbb{Q}}(V_\rho, E(H)\otimes L)$. We are going to point out some of the new directions trying to emphasize new insights that can help to a better understanding of the problem.

A great progress came with the use of p-adic methods. In 1986, Mazur, Tate and Teitelbaum published "On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer" [11]. They comment in the introduction that since the p-adic analogue of the Hasse–Weil L-function had been defined and also p-adic theories analogous to the theory of the canonical height had been introduced, "it seemed to us to be an appropriate time to embark on the project of formulating a p-adic analogue of the conjecture of Birch and Swinnerton-Dyer, and gathering numerical data in its support [...] The project has proved to be anything but routine".

The first surprising aspect is the appearance of a factor that they call p-adic multiplier, which is a simple local term not equal to any recognizable Euler factor. It can vanish at the central point and throw off the order of vanishing of the p-adic L-function at that point (exceptional case). We expect that in the exceptional case the order of vanishing of the p-adic L-function is one greater than the order of vanishing of the classical L-function. This agrees with the fact that when E has split multiplicative reduction at p, one can define in a natural way the extended Mordell–Weil group, the rank of which is one greater than the rank of the usual Mordell–Weil group. Further, we can define a p-adic height pairing on this extended Mordell–Weil group. In this case, the formulation of BSD involves the regulator of the extended Mordell–Weil group. In this setting, we can produce a conjectural relationship between the special value of the first derivative of the p-adic L-function of E and the algebraic part of the special value of the classical L-function of E. It turns out that the former quantity is the product of the latter and the factor

$$\mathcal{L}_p(E) = \log_p(q_p(E))/\operatorname{ord}_p(q_p(E)),$$

where $q_p(E)$ is the p-adic multiplicative period of E. The quantity $\mathcal{L}_p(E)$ is known as the L-invariant of E.

One of the most popular techniques to deal with these p-adic conjectures is the use of Euler systems. Roughly speaking, they are collection of compatible elements of Galois cohomology classes indexed by towers of fields. The most well-known examples are cyclotomic and elliptic units, but also Heegner points, that has been previously presented (more precisely, Heegner points are an example of *anticyclotomic* Euler system). For the study of the rank two setting, the Euler systems that are more useful are those envisaged by Kato, also known as systems of Rankin–Selberg–Garrett type. They consist on the image under étale or syntomic regulators of certain cycles occurring in the higher Chow groups (or K-groups) of modular curves. At the same time, the complex L-function is replaced by its p-adic counterpart. This p-adic L-functions are usually constructed via the interpolation of classical L-values, divided by suitable period, along a certain *interpolation region*.

There are several *explicit reciprocity laws* relating the Perrin–Riou big-logarithm (a map interpolating the dual exponential map and the Bloch–Kato logarithm) of the cohomology classes with special values of p-adic L-functions lying outside the region of non-classical interpolation. This kind of results put a link between the algebraic and analytic side, that is at the end what aims the BSD conjecture. The most *surprising* idea is that in the p-adic setting we may consider certain L-function where we do not only have the usual variable s, but a weight variable which makes the modular form f to vary in a continuous way (we move the modular form along what is called a Hida family).

We continue now by introducing the elliptic Stark conjecture. It is a more constructive alternative to BSD, allowing the efficient computation of p-adic logarithms of global points. In some sense, it can be seen as trying to unify two of the currently known constructions of global points on elliptic curves over $\mathbb{Q}$, Heegner points and the conjectural Stark–Heegner points attached to real quadratic cycles on $\mathbb{H}_p \times \mathbb{H}$. Stark's conjectures give complex analytic formulas for units in number fields (their logarithms) in term of the leading terms of Artin L-functions at $s = 0$. Let $g = \sum a_n(g)q^n$ be a cusp form of weight one, level N and odd character χ. Consider also H_g, the field cut out by an Artin representation ρ_g and $L \subset \mathbb{Q}(\zeta_n)$, the field generated by the Fourier coefficients of g. We denote by V_g the vector space underlying ρ_g. In this framework, Stark's conjecture states the following.

Conjecture 4.1 (Stark)**.** *Let g be a cuspidal newform of weight one with Fourier coefficient in L. Then, there is a modular unit $u_g \in (\mathcal{O}_{H_g}^{\times} \otimes L)^{\sigma_\infty = 1}$ (where σ_∞ stands for the complex conjugation) such that $L'(g, 0) = \log(u_g)$.*

There are some cases (the reducible one, the imaginary dihedral case), where it has been proved. The general result is still unknown to be true.

In [5], the authors formulate some kind of analogue in the realm of points in elliptic curves. The motivation for all this work came for the previous results around Katz's p-adic L-function, the Mazur–Swinnerton-Dyer p-adic L-function and in general, the various types of p-adic Rankin L-functions. Let E be an elliptic curve attached to $f \in S_2(N)$. We introduce the following notations, where χ is a Dirichlet character modulo N, with N relatively prime with a fixed p; more details can be found in [5]:

(i) $M_k(Np, \chi)$ is the space of classical modular forms of weight k, level Np and character χ;

(ii) $M_k^{(p)}(N, \chi)$ is the corresponding space of p-adic modular forms;

(iii) $M_k^{\mathrm{oc}}(N, \chi)$ is the subspace of overconvergent modular forms, a p-adic Banach space where the Hecke operator U_p acts completely continuously. It satisfies $M_k(Np, \chi) \subset M_k^{\mathrm{oc}}(N, \chi) \subset M_k^{(p)}(N, \chi)$.

Coleman's theorem asserts that when h is overconvergent and ordinary of weight ≥ 2, then it is classical;

(iv) $d = q\,d/dq$ is the Atkin–Serre d operator on p-adic modular forms;

(v) when $f \in M_2^{\mathrm{oc}}(N)$, then $F := d^{-1}f \in M_0^{\mathrm{oc}}(N)$, where the d^{-1} refers to the limit of d^t when t tends p-adically to -1;

(vi) $e_{\mathrm{ord}} := \lim_n U_p^{n!}$ is Hida's ordinary projection.

Let $\gamma \in M_k(Np, \chi)^\vee$ and $h \in M_k(N, \chi)$. We define the so-called p-adic iterated integral of f and h along γ as $\int_\gamma f \cdot h := \gamma(e_{\mathrm{ord}}(F \times h)) \in \mathbb{C}_p$. Our aim would be to give an arithmetic interpretation for $\int_{\gamma_{g_\alpha}} f \cdot h$ as $\gamma_{g_\alpha} \in M_1(Np, \chi)^\vee[g_\alpha]$, where this notation refers to elements having the same system of Hecke eigenvalues as g_α. This *integral* can be recast as a special value of a *triple product* p-adic L-function. For the sake of simplicity we must do some assumptions:

(i) certain local signs in the functional equation for $L(E, V_{gh}, s)$ are 1, and in particular $\mathrm{ord}_{s=1} L(E, V_{gh}, s)$ is even;

(ii) $V_{gh} = V_1 \oplus V_2 \oplus W$, where $\mathrm{ord}_{s=1} L(E, V_1, s) = \mathrm{ord}_{s=1} L(E, V_2, s) = 1$ and $L(E, W, 1) \neq 0$. BSD predicts that V_1 and V_2 occur in $E(H_{gh}) \otimes L$ with multiplicity one;

(iii) the geometric Frobenius acts on V_1 (V_2) with eigenvalue $\alpha_g\alpha_h$ ($\alpha_g\beta_h$). Here, α_g and β_g (resp. α_h and β_h) stand for the roots of the p-th Hecke polynomial of the modular form.

Conjecture 4.2 (Elliptic Stark)**.** *Under the above conditions,*

$$\int_{\gamma_{g_\alpha}} f \cdot h = \frac{\log_{E,p}(P_1)\log_{E,p}(P_2)}{\log_p u_{g_\alpha}},$$

where $P_j \in V_j$-isotypic component of $E(H_{gh}) \otimes L$ and $\sigma_p P_1 = \alpha_g\alpha_h \cdot P_1$, $\sigma_p P_2 = \alpha_g\beta_h \cdot P_2$. Further, u_{g_α} is a Stark unit in the $\mathrm{Ad}^0(V_g)$-isotypical part of $(\mathcal{O}_{H_g}^\times) \otimes L$ and $\sigma_p u_{g_\alpha} = (\alpha_g/\beta_g) \cdot u_{g_\alpha}$ (that is coherent with the fact that the Frobenius must act in the left hand side trivially).

The result has been proved by Darmon, Lauder and Rotger when g and h are theta series attached to the same imaginary quadratic field K and the prime p splits in K. In that setting, P_1 and P_2 are expressed in terms of Heegner points and u_{g_α} in terms of elliptic units. The assumption that p is split is crucial for the use of both Katz's p-adic Kronecker limit formula and also for the p-adic Gross–Zagier formula of Bertolini, Darmon and Prasanna.

This conjecture is adapted in [6] to express it in the setting of units in number fields, where some of the self-duality assumptions can be relaxed. In particular, the conjecture is rephrased in terms of the special value $L_p(g \otimes h, 1)$, where g and h are two weight one modular forms and $L_p(g \otimes h, s)$ is the Hida–Rankin p-adic L-function attached to the convolution of two modular forms. This value is expected to encode information about units and p-units in the field cut out by the Galois representation attached to $g \otimes h$. In [12], this conjecture is proved when g and h are self-dual, and there is a further study of the question via the Euler system of Beilinson–Flach elements constructed in [2, 3, 10]. The setting of points in elliptic curves is treated in [8] using the families of cohomology classes of [9].

As a way of finishing this survey about the conjecture of Birch and Swinnerton-Dyer, we would like to emphasize the idea that mathematicians have not still envisaged a successful approach to the problem useful for its general proof, but many interesting ideas not only for this area but for many others have emerged in the last years. In particular, those ideas concerning Euler systems and p-adic methods have been successfully applied to many other instances, such as the study of the Iwasawa main conjecture for elliptic curves.

References

[1] M. Bertolini, F. Castella, H. Darmon, S. Dasgupta, K. Prasanna, and V. Rotger. "p-adic L-functions and Euler systems: a tale in two trilogies", *Automorphic forms and Galois representations*, Vol. 1, LMS Lecture Notes **414** Cambridge University Press (2014) 52–102.

[2] M. Bertolini, H. Darmon, and V. Rotger, "Beilinson–Flach elements and Euler systems I: syntomic regulators and p-adic Rankin L-series", *J. Algebraic Geometry* **24** (2015), 355–378.

[3] M. Bertolini, H. Darmon, and V. Rotger, "Beilinson–Flach elements and Euler systems II: p-adic families and the Birch and Swinnerton-Dyer conjecture", *J. Algebraic Geometry* **24** (2015), 569–604.

[4] H. Darmon. "Rational points on modular elliptic curves", American Mathematical Society, 2004.

[5] H. Darmon, A. Lauder, and V. Rotger, "Stark points and p-adic iterated integrals attached to modular forms of weight one", *Forum of Mathematics, Pi* **3** (2015), 95 pages.

[6] H. Darmon, A. Lauder, and V. Rotger, "Gross-Stark units and p-adic iterated integrals attached to modular forms of weight one", *Ann. Math. Québec* **40** (2016), 325–354.

[7] H. Darmon and V. Rotger, "Diagonal cycles and Euler systems I: a p-adic Gross-Zagier formula", *Annales Scientifiques de l'Ecole Normale Supérieure* **47**(4) (2014), 779–832.

[8] H. Darmon and V. Rotger, "Elliptic curves of rank two and generalised Kato classes", accepted at *Research in Math. Sciences*, special issue in memory of Robert Coleman, (2016).

[9] H. Darmon and V. Rotger, "Diagonal cycles and Euler systems II: the Birch and Swinnerton-Dyer conjecture for Hasse-Weil-Artin L-series", *Journal of the American Mathematical Society* **30**(3) (2017), 601–672.

[10] G. Kings, D. Loeffler, and S.L. Zerbes, "Rankin–Eisenstein classes and explicit reciprocity laws", *Cambridge J. Math* **5**(1) (2017), 1–122.

[11] B. Mazur, J. Tate, and J. Teitelbaum, "On p-adic analogues of the conjecture of Birch and Swinnerton-Dyer", *Inventiones Matematicae* **84** (1986), 1–49.

[12] O. Rivero and V. Rotger, "Derived Beilinson–Flach elements and the arithmetic of the adjoint of a modular form", preprint available at Arxiv.

[13] J. Silvermann, "The arithmetic of elliptic curves", *Graduate Texts in Mathematics* (Springer), 1986.