A Survey of Results Concerning the Birch and Swinnerton-Dyer Conjecture over Function Fields

Jennifer Balakrishnan

February 23, 2004

Abstract

Seen by many to be the most important open problem in number theory, the Birch and Swinnerton-Dyer conjecture has enjoyed increased prominence in recent years. We look at its instantiation over function fields and trace through recent progress made in this area, primarily following the work of Ulmer in [Ulm02] and [Ulm04].

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ in Weierstrass normal form $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Z}$. It is a well-known theorem of Mordell that the group of rational points on E is a finitely generated abelian group $E(\mathbb{Q})$. Thus $E(\mathbb{Q})$ has a natural decomposition as $E(\mathbb{Q}) \approx \mathbb{Z}^r \oplus E(\mathbb{Q})_{\text{tors}}$, where $E(\mathbb{Q})_{\text{tors}}$ is a finite abelian group and r, the rank of the curve, is a nonnegative integer.

Now define the following quantities:

$$\begin{aligned} \Delta &:= \text{discriminant of } E, \\ N_p &:= \text{number of solutions of } y^2 \equiv x^3 + ax + b \bmod p, \\ a_p &:= p - N_p. \end{aligned}$$

Then consider the Euler product

$$L^*(E, s) = \prod_{p \nmid \Delta} (1 - a_p p^{-s} + p^{1-2s})^{-1}.$$

L^*, as a function of a complex variable s, converges for $\text{Re}(s) > \frac{3}{2}$ and has a holomorphic continuation to the whole complex plane [BCDT01]. It is a conjecture of Birch and Swinnerton-Dyer that the Taylor expansion of $L^*(E, s)$ at $s = 1$ is of the form

$$L^*(E, s) = c^*(s - 1)^r + \text{higher order terms},$$

where $c^* \neq 0$ and $r = \text{rank}(E(\mathbb{Q}))$. If we consider $L(E, s)$, the L-series of E, which accounts for the Euler factors at primes $p \mid 2\Delta$, the refined Birch and Swinnerton-Dyer conjecture further predicts that $L(E, s) \sim c(s-1)^r$ with the leading coefficient c equivalent to an expression involving certain invariants associated to E.

Though its formulation over $\mathbb{Q}$ is what the Clay Mathematics Institute [Wil00] is interested in, the Birch and Swinnerton-Dyer conjecture has p-adic analogues due to Mazur, Tate, and Teitelbaum and can be stated for general abelian varieties, as well as over arbitrary number fields and function fields. Indeed, in recent years much progress has been made toward the Birch and Swinnerton-Dyer conjecture over function fields, and currently more is known about the conjecture over function fields than its counterpart over number fields.

The paper is structured as follows: we begin with a brief introduction in Section 2 to function fields, highlighting various differences between function fields and number fields. In Section 3 we look at the analogues of the various quantities involved with the Birch and Swinnerton-Dyer conjecture, leading to the statement of the problem. We discuss progress made toward a Gross-Zagier formula for function fields in Section 4 and examine the recent geometric non-vanishing results of Ulmer in Section 4.3. In Section 5, we take a look at the rank conjecture over function fields and survey Ulmer's results in [Ulm02], which prove the Birch and Swinnerton-Dyer conjecture for certain curves of high rank.

2 Function fields

We begin with a brief introduction to some concepts central to the theory of arithmetic over function fields. For more details, the reader is encouraged to see [Sti93] or [Ros02].

A function field F/K of one variable over an arbitrary field K is an extension field $F \supset K$ with F a finite algebraic extension of $K(x)$ where $x \in F$ is an element that is transcendental over K. Perhaps the simplest example of a function field is the rational function field: F/K is said to be rational if $F = K(x)$, where $x \in F$ is transcendental over K. Any nonzero element $z \in K(x)$ can be uniquely represented as a product

$$z = a \cdot \prod_i p_i(x)^{n_i},$$

where a is a nonzero element of K, $p_i(x) \in K[x]$ are monic, pairwise distinct irreducible polynomials, and $n_i \in \mathbb{Z}$.

A valuation ring of a function field F/K is a ring $\mathcal{O} \subset F$ such that

- $K \nsubseteq \mathcal{O} \nsubseteq F$, and
- given $z \in F$, $z \in \mathcal{O}$ or $z^{-1} \in \mathcal{O}$.

A place P of a function field F/K is the maximal ideal of some valuation ring $\mathcal{O} \subset F/K$. A prime element of P is an element $t \in P$ such that $P = t\mathcal{O}$.

Arithmetic over function fields can prove to be quite different than over number fields. For instance, recall that finite fields and fields of characteristic 0 are perfect. However, consider a function field of degree 1 over a finite field, i.e., a finite algebraic extension of $\mathbb{F}_p(t)$. The function field $\mathbb{F}_p(t)$ is readily seen to have an inseparable extension of degree p and thus is not perfect. Furthermore, as we shall see in Section 3 below, there is an important distinction between elliptic curves over number fields and function fields.

3 The Birch and Swinnerton-Dyer conjecture over function fields

3.1 Elliptic curves over function fields

Take $\mathcal{C}$ to be a smooth, geometrically connected, projective curve over a finite field $\mathbb{F}_q$ and let $F = \mathbb{F}_q(\mathcal{C})$, which is a function field in the sense of Section 2. We can define an elliptic curve E over F by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_i \in F.$$

The discriminant Δ is defined in terms of the coefficients a_i, as one would expect over number fields, as are the c-invariants and the j-invariant (see, for example, [Sil92]).

However, as we alluded to earlier, there is an important distinction between elliptic curves over number fields and function fields. We say E is constant if we can choose a Weierstrass equation for E with all $a_i \in \mathbb{F}_q$. This, however, is the boring case, and so we move on to isotrivial E, those curves that become isomorphic to a constant curve when considered over a finite extension of F. This condition is equivalent to $j(E) \in \mathbb{F}_q$. The most interesting case, as we shall see in section (5), is that of non-isotrivial curves, those with $j(E) \notin \mathbb{F}_q$.

The conductor $\mathfrak{n}$ is an effective divisor, i.e., is a linear combination of places, and is divisible only by places of $\mathcal{C}$ where E has bad reduction. Furthermore,

$$v \mid \mathfrak{n} \text{ with order } \begin{cases} 1 & \text{where } E \text{ has multiplicative reduction,} \\ \geq 2 & \text{where } E \text{ has additive reduction and,} \\ 2 & \text{at places of additive reduction if char(F)} > 3. \end{cases} \tag{3.1}$$

Our notion of rank carries over, as the Mordell-Weil theorem holds for E/F; that is, $E(F)$ is a finitely generated abelian group. The proof of Mordell-Weil over function fields is analogous to the well-known formulation over number fields, involving Selmer groups and height bounds.

We can define the L-function $L(E/F,s)$ of E to be the Euler product

$$\prod_{v\nmid\mathfrak{n}}(1-a_v{q_v}^{-s}+{q_v}^{1-2s})^{-1}\times\prod_{v|\mathfrak{n}}\begin{cases}(1-{q_v}^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction at } v,\\ (1+{q_v}^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction at } v,\\ 1 & \text{if } E \text{ has additive reduction at } v,\end{cases} \tag{3.2}$$

where q_v is the cardinality of the residue field $\mathbb{F}_v$ at v and $a_v = q_v + 1 - |E(\mathbb{F}_v)|$. L converges absolutely when $\mathrm{Re}(s) > \frac{3}{2}$ and has a meromorphic continuation to the s plane (more details, via Grothendieck's analysis of L-functions, can be found in [Mil80]).

3.2 The conjecture as it stands today

With this in mind, the Birch and Swinnerton-Dyer conjecture over function fields reads as it does over number fields:

Conjecture 3.1 (Birch, Swinnerton-Dyer). *If E is an elliptic curve over a function field F, then the algebraic and analytic ranks associated to E are the same:*

$$r = \mathrm{Rank}(E(F)) = \mathrm{ord}_{s=1}\, L(E/F,s). \tag{3.3}$$

The refined conjecture as well bears striking similarity to its analogue over number fields:

Conjecture 3.2 (Refined BSD). *the leading coefficient in the expansion of $L(E/F,s)$ about $s=1$ is equal to*

$$\frac{1}{r}L^{(r)}(E/F,1) = \frac{|Ш|R\tau}{|E(F)_{tors}|^2},$$

where Ш is the Shafarevich-Tate group, R is a regulator associated to the heights of a generating set for $E(F)$, τ a Tamagawa number that serves as an analogue of a period, and $E(F)_{\mathrm{tors}}$ the torsion points of $E(F)$. As these individual objects themselves have little bearing on the results described in this paper, the interested reader is referred to [Tat95].

The function field analogue of the Birch and Swinnerton-Dyer conjecture first appeared in the article of Tate [Tat95], where it was proven that

$$\mathrm{Rank}(E(F)) \leq \mathrm{ord}_{s=1}\, L(E/F,s). \tag{3.4}$$

Via results of Artin, Tate [Tat95] and Milne [Mil75], it is also known that the refined Birch and Swinnerton-Dyer conjecture, i.e., concerning the value of the leading coefficient of $L(E/F,s)$, holds true if any of the following equivalent conditions are satisfied:

- Equality in (3.4)

- Finiteness of the l-primary part of Ш for any one prime l (with no restrictions on l, in particular $l = p$ is valid)
- Finiteness of Ш

Two ideas play a key role in these results, and in the results to follow. The first of these is a lifting to the unique elliptic surface $\mathcal{E} \longrightarrow \mathcal{C}$ associated to E, where $\mathcal{E}$ is a smooth, proper surface over $\mathbb{F}_q$ with generic fiber E/F that admits a flat and relatively minimal morphism to $\mathcal{C}$. Also important is Grothendieck's analysis of L-functions, key to our cohomological understanding of the ζ-function of $\mathcal{E}$ and the L-function of E.

While the full Birch and Swinnerton-Dyer conjecture over function fields has not been resolved, much progress has been made in this direction. A survey of the literature will show that the conjecture holds for the following:

- Given a finite extension K of F, if the conjecture is true for E/K, it is also true for E/F.
- Via results of Tate [Tat95], the conjecture holds for constant E.
- Looking at the elliptic surface $\mathcal{E}$, the conjecture is known to be true when $\mathcal{E}$ is rational, $K3$ [ASD73], or dominated by a product of curves [Tat94]
- Recent results of Ulmer [Ulm03], together with a function field analogue of the Gross-Zagier formula, can be used to prove the conjecture for elliptic curves of analytic rank at most 1 over function fields of characteristic greater than 3.
- Ulmer has also constructed a family of elliptic curves of arbitrarily high rank for which the Birch and Swinnerton-Dyer conjecture holds, and thus over function fields, the Birch and Swinnerton-Dyer conjecture is known for specific curves whose ranks tend to infinity.

4 The Gross-Zagier theorem over function fields

We shall focus a large portion of the paper on these last two results, namely that of Ulmer in [Ulm], [Ulm03], and [Ulm02]. As the former results stem from an attempt to prove the Gross-Zagier formula over function fields, we first revisit some concepts necessary to an understanding of the Gross-Zagier formula.

4.1 Modularity

We begin with the situation for elliptic curves over $\mathbb{Q}$. An elliptic curve over $\mathbb{Q}$ with conductor N is said to be modular if one of the two equivalent formulations of modularity hold:

1. (Analytic modularity) There exists a modular form $f \in \Gamma_0(N)$ of weight two such that $L(E, \chi, s) = L(f, \chi, s)$ for all Dirichlet characters χ.

2. (Geometric modularity) E can be parametrized by a modular curve $X_0(N)$ by means of a non-constant morphism, i.e., $X_0(N) \longrightarrow E$.

We wish to examine the function field analogues of the above criteria for modularity.

4.1.1 Analytic modularity

We begin with some notation. Let $\mathcal{C}$ be a smooth, proper, geometrically connected curve over $\mathbb{F}_{p^n} = \mathbb{F}_q$ and set $F = \mathbb{F}_q(\mathcal{C})$. Denote by $\mathbb{A}_F$ the adèle ring of F and $\mathcal{O}_F \subset \mathbb{A}_F$ the subring of everywhere integral adèles. We can define automorphic forms on this space, namely the functions on $\mathrm{GL}_2(\mathbb{A}_F)$ invariant under left translations by $\mathrm{GL}_2(F)$ and under right translations by an open subgroup $K \subset \mathrm{GL}_2(\mathcal{O}_F)$ of finite index. As functions on the double coset space $\mathrm{GL}_2(F)\backslash \mathrm{GL}_2(\mathbb{A}_F)/K$, they take values in any field of characteristic 0. For our purposes, this field is $\overline{\mathbb{Q}}$, and we embed $\overline{\mathbb{Q}} \to \mathbb{C}$ and $\overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_l (l \neq p)$.

K here plays the role of a congruence subgroup, and its most useful analogues are those akin to $\Gamma_0(\mathfrak{m})$ or $\Gamma_1(\mathfrak{m})$, where $\mathfrak{m}$, like the classical conductor, is an effective divisor on $\mathcal{C}$. Now given an automorphic form f and an idèle class character

$$\psi : \mathbb{A}^\times / F^\times \longrightarrow \overline{\mathbb{Q}}_l{}^\times,$$

we say that f has central character ψ if $f(zg) = \psi(z)f(g)$ for all $z \in Z(\mathrm{GL}_2(\mathbb{A}_F)) \cong \mathbb{A}_F{}^\times$ and all $g \in \mathrm{GL}_2(\mathbb{A}_F)$. This central character is our analogue of weight and so given $k \in \mathbb{Z}^+$, $\psi(z) =\mid z \mid^{-k}$ (of adèlic norm $\mid \cdot \mid$), f becomes our analogue of a weight k modular form.

Since we now have an analogue of modular forms, the next natural question would be if we could view them as functions acting on the upper half plane. The answer, fortunately is yes, and the construction proceeds as follows: fix a place ∞ of F and let $K = \Gamma_0(\infty\mathfrak{n}), \mathfrak{n}$ prime to ∞. Then our automorphic form f can be thought of as a function acting on a finite number of copies of the homogeneous space $\mathrm{PGL}_2(F_\infty)/\Gamma_0(\infty)$, with structure as an oriented tree. As in the classical case, these functions are invariant under certain congruence subgroups, finite index subgroups of $\mathrm{GL}_2(A) \subset \mathrm{GL}_2(F_\infty)$, where the subring $A \subset F$ is the set of functions regular outside ∞.

We shall see that much of the classical theory carries over. For one, our automorphic forms have Fourier expansions, with coefficients indexed by effective divisors on $\mathcal{C}$. We also have a notion of Hecke operators, also indexed by effective divisors on $\mathcal{C}$, and thus we have the expected correspondence between Fourier coefficients of eigenforms and eigenvalues of Hecke operators. Our space of modular forms has a subspace of cusp forms, and fixing "level" K and "weight" ψ, the space is finite-dimensional. Further associated to f is the complex-valued L-function $L(f, s)$, and if f happens to be a cuspidal eigenform, its L-function has an Euler product and an analytic continuation to an entire function of s, and can be written in terms of a functional equation.

For more details on the constructions in this section, the reader is encouraged to see Weil's [Wei71]. We skip to perhaps what is the most important result in [Wei71], namely, that which connects L-functions to modularity. The theorem describes suitable analyticity conditions that would make a Dirichlet series the L-function of an automorphic form on GL_2. Of these conditions, the most important is that the Dirichlet series in question has sufficiently many twists by finite order characters satisfying functional equations.

Via results of Grothendieck and Deligne, one finds that indeed, such is the case. Given an elliptic curve E over F, Grothendieck showed that the Dirichlet series $L(E, s)$ is meromorphic, with its twists satisfying certain functional equations. It remained to be shown that these were the functional equations described by Weil, but this was settled by Deligne in [Del73]. The automorphic form f_E attached to E is chraracterized by the equations $L(E, \chi, s) = L(f_E, \chi, s)$ for all finite order idèle class characters χ. f_E is an eigenform for the Hecke operators, and if E is non-isotrivial, f_E is a cusp form. Furthermore, it satisfies the necessary level and weight analogues: given $\mathfrak{m}$ the conductor of E, it has level $\Gamma_0(\mathfrak{m})$ and it has central character $|\cdot|^{-2}$. This f_E is thus the desired function field analogue of the classical modular form in 1.

4.1.2 Geometric modularity and Drinfeld modules

As before, let $\mathcal{C}$ be a smooth, proper, geometrically connected curve over $\mathbb{F}_{p^n} = \mathbb{F}_q$ and set $F = \mathbb{F}_q(\mathcal{C})$. Our main object of interest in our study of geometric modularity is that of the Drinfeld module [Dri74]. We begin with some notation. Let A be the ring of elements of F that are regular away from a fixed place ∞ in F. Take F_∞ to be the completion of F at ∞ and C the completion of an algebraic closure of F_∞. For example, when $F = \mathbb{F}_q(t)$ and∞ is the usual $t = \infty$, then $A = \mathbb{F}_q[t]$. Now let k be a ring of characteristic p with a homomorphism $A \longrightarrow k$, and denote by $k\{\tau\}$ the ring of non-commutative polynomials in τ, such that $\tau a = a^p \tau$. There is a natural inclusion $\mathbf{e} : k \to k\{\tau\}$ with left inverse $D : k\{\tau\} \longrightarrow k$ such that $D(\sum a_n \tau^n) = a_0$. For an arbitrary k-algebra R, the additive group of R can be turned into a $k\{\tau\}$-module by setting $(\sum a_n \tau^n)(x) = \sum a_n x^{p^n}$.

A Drinfeld module over k is then a ring homomorphism $\phi : A \longrightarrow k\{\tau\}$ with image not in k such that the composition $D \circ \phi : A \longrightarrow k$ is the homomorphism mentioned above. We define the characteristic of ϕ to be the kernel of the mapping $A \longrightarrow k$, which turns out to be a prime ideal of A. To simplify notation, let ϕ_a denote the image of $a \in A$ (as opposed to $\phi(a)$). Supposing our ring A to be $\mathbb{F}_q[t]$, then ϕ is solely determined by ϕ_t, where $\phi_t \in \{k\{\tau\}\}$, with degree > 0 and constant term the image of t under the mapping $A \longrightarrow k$.

Further properties of Drinfeld modules are as follows: given a k-algebra and a Drinfeld module ϕ, the k-algebra can be turned into an A-algebra by the Drinfeld module acting on it such that $a \cdot x = \phi_a(x)$. The map $a \mapsto \phi_a$ is always an injection, and there exists a positive integer r such that $p^{\deg_\tau(\phi_a)} = |\ a\ |_\infty^{\ r} = \#(A/a)^r$. This r is called the rank of the Drinfeld module. Given two Drinfeld modules ϕ and

ϕ', we can define a homomorphism $u : \phi \longrightarrow \phi'$ to be an element $u \in k\{\tau\}$ with $u\phi_a = \phi'_a u$ for all $a \in A$. A nonzero homomorphism is said to be an isogeny, and isogenous Drinfeld modules must have the same rank and characteristic.

With this background material established, we can now concentrate on rank 2 Drinfeld modules, which bear many similarities to elliptic curves. Throughout the following discussion, we shall assume that these Drinfeld modules are over schemes of characteristic p.

First, we can construct "level $\mathfrak{n}$ structure" on a Drinfeld module, given an effective divisor $\mathfrak{n}$ on $\mathcal{C}$ that is relatively prime to ∞ (i.e., a nonzero ideal of A). From here, there is a notion of a moduli space $Y_0(\mathfrak{n})$ that parametrizes rank 2 Drinfeld modules having level $\mathfrak{n}$ structure and thus a point on the moduli space is represented by a pair ϕ and ϕ' and a cyclic n-isogeny? $Y_0(\mathfrak{n})$ is smooth and affine over F and its completion, adding "cusp" points, yields a smooth, proper curve $X_0(\mathfrak{n})$. As with elliptic curves, these cusps involve certain degeneracies of the Drinfeld module. Furthermore, many objects associated to the classical modular curve $X_0(\mathfrak{n})$ carry over to our Drinfeld-module-analogue: e.g., Hecke correspondences and Atkin-Lehner involutions (for more details, see [Dri74] and [DH87]).

Now consider the Drinfeld upper half plane $\Omega = \mathbb{P}^1(C) \setminus \mathbb{P}^1(F_\infty)$, where C is the completion of an algebraic closure of F_∞. Drinfeld [Dri74] constructed the isomorphism

$$Y_0(\mathfrak{n})(C) \cong \mathrm{GL}_2(F) \setminus \left(\mathrm{GL}_2(\mathbb{A}_F^f) \times \Omega\right) / \Gamma_0(\mathfrak{n})^f,$$

where the exponent ^{f} denotes "finiteness": for example, $\mathbb{A}_F^f$ is the set of adèles with the component at infinity removed, i.e., "finite" adèles. There is, a priori, a map from Ω to $PGL_2(F_\infty)/\Gamma_0(\infty)$ (the so-called building map). With this map, one gets a relation between the C points of $Y_0(\mathfrak{n})$ and the double coset space where the automorphic forms live. Via a cohomological arugment, Drinfeld formulated a reciprocity theorem, namely that if f is a level $\Gamma_0(\mathfrak{n}\infty)$ eigenform that is special at ∞ (i.e., E has split multiplication at ∞), then there exists a factor A_f of the Jacobian $J_0(\mathfrak{n})$ of $X_0(\mathfrak{n})$ with $L(f, \chi, s) = L(A_f, \chi, s)$, for all finite order idèle class characters χ of F, where A_f is well-defined up to isogeny.

If the eigenvalues of the Hecke operator on f are integers, A_f is an elliptic curve. If f is a newform, then the conductor of E is $n\infty$ and is split multiplicative at ∞. It is this case that interests us: let E be an elliptic curve over F with level $\mathfrak{m} = n\infty$ that is split multiplicative at ∞. Recall from our earlier discussion in section 4.1.1, Deligne's results furnished us with a weight 2, level $\mathfrak{m}$ automorphic form f_E on GL_2 over F that is special at ∞. We saw that Drinfeld constructed a class of isogenous elliptic curves A_{f_E} in the Jacobian of $X_0(\mathfrak{n})$, such that the following L-functions were equal:

$$L(E, \chi, s) = L(f_E, \chi, s) = L(A_{f_E}, \chi, s).$$

Zarhin [Zar74] and Moret-Bailly [MB85] then showed that the associated L-function determines the isogeny class of a given abelian variety A. The consequence is a non-trivial modular parametrization $X_0(\mathfrak{n}) \longrightarrow E$, as E must be in the class

A_{f_E}. Finally, Gekeler and Reversat [GR96] constructed an analytic parametrization $X_0(\mathfrak{n})(C) \longrightarrow E(C)$, the function field analogue of the classical elliptic curve parametrization.

4.2 Gross-Zagier formula and Heegner points

Armed with the function field analogue of modularity, concerted efforts have been made over the last 10 years to generalize Heegner points, the Gross-Zagier formula, and the work of Kolyvagin. We provide a brief historical overview of these results.

Brown began in [Bro94] by generalizing Heegner points. With this construction, in the spirit of Kolyvagin [Kol90], he attempted to show that if a certain point P_K is not torsion, then $Ш(E)$ is finite and the rank of $E(K)$ is 1, thus proving the Birch and Swinnerton-Dyer conjecture for E over K. Unfortunately, Brown's paper contained many inaccuracies and it is Ulmer's opinion [Ulm04] that his results are not completely proven.

Rück and Tipp [RT00] successfully constructed a function field analogue of the Gross-Zagier formula. However, its usefulness (insofar as it can be applied to the Birch and Swinnerton-Dyer conjecture) does not seem to be promising, although under certain restrictive hypothesis it is known to have implications. Likewise, with the work of Pàl [PÓ0] and Longhi [Lon02]: both successfully made function field analogues of the Bertolini-Darmon [BD98] construction of Heegner points, but their results do not immediately yield much in the direction of resolving the Birch and Swinnerton-Dyer conjecture over function fields.

4.3 Geometric non-vanishing

Much like those before him, Ulmer has been working on a Gross-Zagier formula and Heegner point construction for elliptic curves over function fields. Yet he believes that a mere function field analogue of the Gross-Zagier formula analogue ultimately yields the Birch and Swinnerton-Dyer conjecture with "parasitic hypotheses" [Ulm04]. For instance, the Heegner point construction relies on a Drinfeld modular parametrization, which in turn necessitates the elliptic curve having split multiplication at a place that does not immediately seem to have any relevance to the Birch and Swinnerton-Dyer conjectures.

As an alternative approach, Ulmer has recently proven a geometric non-vanishing result [Ulm03], that, coupled with a version of the Gross-Zagier formula, proves the Birch and Swinnerton-Dyer conjecture for rank 1 elliptic curves, without any sort of parasitic hypotheses. Namely, given an elliptic curve E over a function field F of characteristic greater than 3, if $\operatorname{ord}_{s=1} L(E/F, s) \leq 1$, then the Birch and Swinnerton-Dyer conjecture holds for E.

We proceed to outline the statement of the result on geometric non-vanishing. We begin with an elliptic curve E over F with analytic rank $\operatorname{ord}_{s=1} L(E/F, s) \leq 1$. As the Birch and Swinnerton-Dyer conjecture is known to hold for rank 0 elliptic curves via Tate's results, we can assume that $\operatorname{ord}_{s=1} L(E/F, s) = 1$. Furthermore,

supposing that E is non-isotrivial, we have that $j(E) \notin \mathbb{F}_q$, which implies that E has a pole at some place of F and is thus potentially multiplicative at that place. We can easily find a finite extension F' of F such that E is split multiplicative at that place, and as proving BSD over a finite extension implies BSD for the base field, it suffices to consider E over F'. However, to use Heegner points, F' has to be such that $\operatorname{ord}_{s=1} L(E/F', s)$, which *a priori* is greater than or equal to 1, must be 1. This then relies on the non-vanishing of a twist of the L-function, in this case, $L(E/F', s)/L(E/F, s)$. Furthermore, a similar non-vanishing result is needed when considering the Gross-Zagier formula. We want a quadratic extension K/F' chosen in light of the Heegner hypotheses, with $\operatorname{ord}_{s=1} L(E/K, s) = \operatorname{ord}_{s=1} L(E/F', s) = 1$. This, in turn, necessitates a non-vanishing result concerning quadratic twists of $L(E/F', s)$ by characters satisfying certain local conditions. Both non-vanishing results are settled by Ulmer in the following theorem[1]:

Theorem 4.1. *Let E be a non-constant elliptic curve over a function field F of characteristic $p > 3$. Then there exists a finite separable extension F' of F and a quadratic extension K of F' such that the following conditions are satisfied:*

1. *E is semistable over F', i.e., its conductor is square-free.*
2. *E has split multiplicative reduction at some place of F' which we call ∞.*
3. *K/F' satisfies the Heegner hypotheses with respect to E and ∞. In other words, K/F' is split at every place $v \neq \infty$ dividing the conductor of E and it is not split at ∞.*
4. *$\operatorname{ord}_{s=1} L(E/K, s)$ is odd and at most $\operatorname{ord}_{s=1} L(E/F, s) + 1$. In particular, if $\operatorname{ord}_{s=1} L(E/F, s) = 1$, then $\operatorname{ord}_{s=1} L(E/K, s) = \operatorname{ord}_{s=1} L(E/F', s) = 1$*

With an appropriate formulation of the Gross-Zagier formula (see [Ulm]), the above result proves the Birch and Swinnerton-Dyer conjecture for elliptic curves of analytic rank 1. Item (1) is needed for the Gross-Zagier formula. Item (2) gives us a Drinfeld modular parametrization of E over F' via item (3), we have a Heegner point over K. The Gross-Zagier formula, along with item (4) ensures that the Heegner point does not have torsion, which implies that Rank $E(K) \geq 1$. Thus this result yields the Birch and Swinnerton-Dyer conjecture for E over K, and as K was a finite extension of F, the implication holds for E over F as well.

5 Ranks over function fields

While the Birch and Swinnerton-Dyer conjecture is known to hold for analytic rank ≤ 1 elliptic curves over function fields as well as number fields, the situation over

[1]This result is actually a consequence of a more general non-vanishing theorem that Ulmer proved for motivic L-functions, i.e., those attached to Galois representations. However, as much of this work relies on the difficult monodromy results of Katz [Kat02], we shall stop here in our exposition and refer the interested reader to [Ulm03].

function fields is slightly more interesting, in that the conjecture has also been verified for curves of arbitrarily high rank. Indeed, the following result of Ulmer also settles the rank conjecture (i.e., that there exist curves of arbitrarily high rank) for elliptic curves over function fields:

Theorem 5.1. *Let p be a prime, n a positive integer, and $d|(p^n+1)$. Let q be a power of p and let E be the elliptic curve over $\mathbb{F}_q(t)$ defined by*

$$y^2 + xy = x^3 - t^d.$$

Then the j-invariant of E is not in $\mathbb{F}_q$, the conjecture of Birch and Swinnerton-Dyer holds for E, and the rank of $E(\mathbb{F}_q(t))$ is

$$\sum_{\substack{e|d \\ e\nmid 6}} \frac{\phi(e)}{o_e(q)} + \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } 4 \nmid (q-1) \\ 1 & \text{if } 2 \mid d \text{ and } 4 \mid (q-1) \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \\ 1 & \text{if } 3 \mid d \text{ and } 3 \nmid (q-1) \\ 2 & \text{if } 3 \mid d \text{ and } 3 \mid (q-1). \end{cases} \tag{5.1}$$

Here $\phi(e)$ is the cardinality of $(\mathbb{Z}/e\mathbb{Z})^\times$ and $o_e(q)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$

Ulmer's proof is, not surprisingly, both geometric and arithmetic in nature. On the geometric side, an elliptic surface $\mathcal{E} \longrightarrow \mathbb{P}^1$ is constructed over $\mathbb{F}_p$ with generic fiber E/K, where $K = \mathbb{F}_p(t)$. We are interested in $\mathcal{E}$, since the rank of its Néron-Severi group gives us information about the rank of the Mordell-Weil group of E. From the work of Shioda [Shi86], it is known that a map can be defined between $\mathcal{E}$ and the Fermat surface F_d in $\mathbb{P}^3$, $F_d = x_0^d + x_1^d + x_2^d + x_3^d = 0$. This, in turn, induces a key birational isomorphism between $\mathcal{E}$ and a quotient of the Fermat surface.

On the arithmetic side, it is known that the Birch and Swinnerton-Dyer conjecture for E is equivalent to the Tate conjecture[2] for $\mathcal{E}$. Fortunately for us, the Tate conjecture is known for Fermat surfaces, and hence for $\mathcal{E}$. The birational map mentioned above helps us express the zeta function of $\mathcal{E}$ in terms of the zeta function of F_d, which was explicitly calculated by Weil in terms of Gauss sums. From this calculation, we can deduce that the zeta function of $\mathcal{E}$ has a pole of large order at $s = 1$ and hence conclude that $E(K)$ has high rank.

It is important to note that the elliptic curves above are all non-isotrivial (see section (3.1). An earlier construction of Shafarevich and Tate, in [TS67], had yielded elliptic curves of arbitrarily high rank as well. This was done by taking a supersingular elliptic curve E_0 defined over $K = \mathbb{F}_p$ (but also thought of as a curve E over K in the usual way) and finding quadratic extensions L/K with the Jacobian of the curve over $\mathbb{F}_p$ having a large number of factors that were isogenous to E_0 over $\mathbb{F}_p$. This, then, meant that the quadratic twist of E by L had large rank, but all such curves found by this method were isotrivial, i.e., were isomorphic to curves over $\mathbb{F}_p$ after a finite extension. As there is no analogous property of isotriviality over $\mathbb{Q}$, it was not clear if this set of examples lent any credence to the rank conjecture over

[2] A conjecture on cycles and poles of zeta functions: see [Tat65] for more details.

$\mathbb{Q}$. Nevertheless, as per the results of Ulmer in [Ulm02], it does seem slightly more possible now for a number field analogue to be constructed, thereby proving the rank conjecture[3].

References

[ASD73] M. Artin and P. Swinnerton-Dyer, *The Shafarevich-Tate conjecture for pencils of elliptic curves on K3 surfaces*, Invent. Math. **20** (1973), 249–266.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises*, no. 4, 843–939.

[BD98] M. Bertolini and H. Darmon, *Heegner points, p-adic L-functions, and the Cerednik-Drinfeld uniformization*, Invent. Math. **131** (1998), 453–491.

[Bro94] M. Brown, *On a conjecture of Tate for elliptic surfaces over finite fields*, Proc. London Math. Soc. (3) **69** (1994), 489–514.

[Del73] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one varaible, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[DH87] P. Deligne and D. Husemoller, *Survey of drinfeld modules*, Current trends in arithemtical algebraic geometry (Arcata, CA, 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 25–91.

[Dri74] V. G. Drinfeld, *Elliptic modules*, Mat. Sb. (N.S.) **94 (136)** (1974), 594–627, 656.

[GR96] E.-U. Gekeler and M. Reversat, *Jacobians of drinfeld modular curves*, J. Reine Angew. Math. **476** (1996), 27–93.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

[Kat02] N. Katz, *Twisted L-functions and monodromy*, Annals of Mathematics Studies, vol. 150, Princeton University Press, Princeton, 2002.

[Kol90] V. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, 1990, pp. 435–483.

[Lon02] I. Longhi, *Non-Archimedean integration and elliptic curves over function fields*, J. Number Theory **94** (2002), 375–404.

[3]Over $\mathbb{Q}$, the record as it stands today is algebraic rank 24 (see [MM00]) analytic rank 3 (see [GZ86]).

[MB85] L. Moret-Bailly, *Pinceaux de variétés abéliennes*, Astérique **no. 129,266** (1985), 31–34.

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), 517–533.

[Mil80] ———, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980. MR 81j:14002

[MM00] R. Martin and W McMillen, *An elliptic curve over $\mathbb{Q}$ with rank at least 24*, Number Theory Listserver (2000).

[PÓ0] A. Pál, *Drinfeld modular curves, heegner points and interpolation of special values*, Columbia University Ph.D. thesis (2000).

[Ros02] M. Rosen, *Number theory in function fields*, Springer, New York, 2002.

[RT00] H.-G. Rück and U. Tipp, *Heegner points and L-series of automorphic cusp forms of drinfeld type*, Doc. Math. **5** (2000), 365–444 (electronic).

[Shi86] T. Shioda, *An explicit algorithm for computing the picard number of certain algebraic surfaces*, Amer. J. Math **108** (1986), 415–432.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Springer-Verlag, Berlin, 1993.

[Tat65] J. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry (O. F. G. Schilling, ed.), Harper and Row, New York, 1965, pp. 93–110.

[Tat94] ———, *Conjectures on algebraic cycles in l-adic cohomology*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 71–83.

[Tat95] ———, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440.

[TS67] J. Tate and I. Shafarevich, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), 770–773.

[Ulm] D. Ulmer, *Automorphic forms on* GL(2) *over function fields and Gross-Zagier theorems*, In preparation.

[Ulm02] ———, *Elliptic curves with large rank over function fields*, Ann. of Math. (2) **155** (2002), 295–315.

[Ulm03] ———, *Geometric non-vanishing*, preprint (2003).

[Ulm04] ———, *Elliptic curves and analogies between number fields and function fields*, Heegner points and Rankin L-series (MSRI) Publications 48, Cambridge Univ. Press, New York, 2004, pp. ??–??

[Wei71] A. Weil, *Dirichlet series and automorphic L-forms*, Lecture Notes in Math., vol 189, Springer, New York, 1971.

[Wil00] A. J. Wiles, *The Birch and Swinnerton-Dyer Conjecture*, `http://www.claymath.org/prize_problems/birchsd.htm`.

[Zar74] Y. Zarhin, *A finiteness theorem for isogenies of abelian varieties over function fields of finite characteristic (Russian)*, Funkcional. Anal. i Priložen **8** (1974), 31–34.