ELLIPTIC CURVES AND ANALOGIES BETWEEN NUMBER FIELDS AND FUNCTION FIELDS

DOUGLAS ULMER

Abstract. The well-known analogies between number fields and function fields have led to the transposition of many problems from one domain to the other. In this paper, we will discuss traffic of this sort, in both directions, in the theory of elliptic curves. In the first part of the paper, we consider various works on Heegner points and Gross-Zagier formulas in the function field context; these works lead to a complete proof of the conjecture of Birch and Swinnerton-Dyer for elliptic curves of analytic rank at most 1 over function fields of characteristic > 3. In the second part of the paper, we will review the fact that the rank conjecture for elliptic curves over function fields is now known to be true, and that the curves which prove this have asymptotically maximal rank for their conductors. The fact that these curves meet rank bounds suggests a number of interesting problems on elliptic curves over number fields, cyclotomic fields, and function fields over number fields. These problems are discussed in the last four sections of the paper.

1. Introduction

The purpose of this paper is to discuss some work on elliptic curves over function fields inspired by the Gross-Zagier theorem and some new ideas about ranks of elliptic curves from the function field case which I hope will inspire work over number fields.

We begin in Section 2 by reviewing the statement of and current state of knowledge on the conjecture of Birch and Swinnerton-Dyer for elliptic curves over function fields. Then in Section 3 we discuss various works by Rück and Tipp, Pál, and Longhi on function field analogues of the Gross-Zagier formula and some related work by Brown. We also explain how suitably general Gross-Zagier formulas together with my "geometric non-vanishing" results lead to a theorem of the form: the Birch and Swinnerton-Dyer conjecture for elliptic curves over function fields of curves over finite fields of characteristic > 3 holds for elliptic curves with analytic rank at most 1.

In Sections 4 and 5 we move beyond rank one and explain that the rank conjecture holds for elliptic curves over function fields: there are (non-isotrivial) elliptic curves with Mordell-Weil group of arbitrarily large rank. Moreover, these curves meet an asymptotic bound due to Brumer for the rank in terms of the conductor. So in the function field case, we know precisely the asymptotic growth of ranks of elliptic curves ordered by the size of their conductors. In fact, there are two bounds, one arithmetic, the other geometric, and both are sharp.

Date: May 22, 2003.

This paper is based upon work supported by the National Science Foundation under Grant No. DMS0070839.

The rest of the paper is devoted to explaining some interesting problems suggested by the existence and sharpness of these two types of rank bounds. In Section 6 we make a conjecture which says roughly that Mestre's bound on the ranks of elliptic curves over $\mathbb{Q}$ and suitable generalizations of it over number fields are asymptotically sharp. Next, we note that the Mestre bound and even more so the Brumer bound are (or rather can be reformulated as) algebraic statements. For example, the Brumer bound can be interpreted as a statement about the eigenvalues of Frobenius on étale cohomology. It is therefore natural to ask for an algebraic proof; reformulating the bounds into statements that might admit an algebraic proof leads to some interesting questions which are explained in Section 7.

Finally, in Sections 8 and 9 we discuss possible rank bounds over cyclotomic fields and over function fields over number fields. More precisely, we discuss pairs of ranks bounds, one "arithmetic" the other "geometric," for pairs of fields like $\mathbb{Q}^{p-\mathrm{cyc}}/\mathbb{Q}$ or $\overline{\mathbb{Q}}(\mathcal{C})/\mathbb{Q}(\mathcal{C})$ where $\mathcal{C}$ is a curve over $\mathbb{Q}$. In both cases, one rank bound is known (arithmetic in the first case, geometric in the second) and the other bound has yet to be considered.

Acknowledgements. It is a pleasure to thank Guatam Chinta, Henri Darmon, Mihran Papikian, Joe Silverman, Dinesh Thakur, Adrian Vasiu and the referee for their comments, corrections, and references to the literature.

2. Review of the Birch and Swinnerton-Dyer conjecture over function fields

We assume that the reader is familiar with elliptic curves over number fields, but perhaps not over function fields, and so in this preliminary section we set up some background and review the Birch and Swinnerton-Dyer conjecture. For many more details, examples, etc., we refer to [Ulmb].

Let $\mathcal{C}$ be a smooth, geometrically connected, projective curve over a finite field $\mathbb{F}_q$ and set $F = \mathbb{F}_q(\mathcal{C})$. Let E be an elliptic curve over F, i.e., a curve of genus one defined as usual by an affine Weierstrass equation

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

($a_i \in F$) with the point at infinity $[0, 1, 0]$ as origin; the discriminant Δ and j-invariant are given by the usual formulas (see, e.g., [Tat72]) and we of course assume that $\Delta \neq 0$. We say that E is *constant* if it is defined over $\mathbb{F}_q$, i.e., if it is possible to choose the Weierstrass model so that the $a_i \in \mathbb{F}_q$. Equivalently, E is constant if there exists an elliptic curve E_0 defined over $\mathbb{F}_q$ such that $E \cong E_0 \times_{\operatorname{Spec} \mathbb{F}_q} \operatorname{Spec} F$. In this case we say that E is based on E_0. We say that E is *isotrivial* if it becomes isomorphic to a constant curve after a finite extension of F; this is easily seen to be equivalent to the condition $j(E) \in \mathbb{F}_q$. Finally, we say that E is *non-isotrivial* if $j(E) \notin \mathbb{F}_q$.

Let $\mathfrak{n}$ be the conductor of E. This is an effective divisor on $\mathcal{C}$ which is divisible only by the places where E has bad reduction. More precisely, v divides $\mathfrak{n}$ to order 1 at places where E has multiplicative reduction and to order at least 2 at places where E has additive reduction and to order exactly 2 at these places if the characteristic of F is > 3. The reduction, exponent of conductor, and minimal model of E at places of F can be computed by Tate's algorithm [Tat72].

The Mordell-Weil theorem holds for E, namely $E(F)$ is a finitely generated abelian group. This can be proven in a manner entirely analogous to the proof over

number fields, using Selmer groups and heights, or by more geometric methods; see [Nér52]. Also, both the rank conjecture (that for a fixed F, the rank of $E(F)$ can be arbitrarily large) and the torsion conjecture (that there is a bound on the order of the torsion subgroup of $E(F)$ depending only on the genus of F) are known to be true in this context. For the rank conjecture, see [Ulm02] and Section 4 below. The torsion conjecture was proven by Levin [Lev68], who showed that there is an explicit bound of the form $O(\sqrt{g}+1)$ for the order of the torsion subgroup of a non-isotrivial elliptic curve over F, where g is the genus of F. More recently, Thakur [Tha02] proved a variant bounding the order of torsion in terms of the "gonality" of $\mathcal{C}$, i.e., the smallest degree of a non-constant map to $\mathbb{P}^1$.

The L-function of E is defined by the Euler product

$$L(E/F,s) = \prod_{v \not| \mathfrak{n}} \left(1 - a_v q_v^{-s} + q_v^{1-2s}\right)^{-1} \times \prod_{v|\mathfrak{n}} \begin{cases} (1-q_v^{-s})^{-1} & \text{if } E \text{ has split multiplicative reduction at } v \\ (1+q_v^{-s})^{-1} & \text{if } E \text{ has non-split multiplicative reduction at } v \\ 1 & \text{if } E \text{ has additive reduction at } v. \end{cases}$$

Here q_v is the cardinality of the residue field $\mathbb{F}_v$ at v and the number of points on the reduced curve is $\#E(\mathbb{F}_v) = q_v + 1 - a_v$. The product converges absolutely in the half-plane $\Re s > 3/2$, has a meromorphic continuation to the s plane, and satisfies a functional equation for $s \mapsto 2-s$. If E is not constant, then $L(E/F,s)$ is a polynomial in s of degree $4g-4+\deg \mathfrak{n}$ and thus an entire function of s. (All this comes from Grothendieck's analysis of L-functions. See the last section of [Mil80] for more details.)

The Birch and Swinnerton-Dyer conjecture in this context asserts that

$$\operatorname{Rank} E(F) \stackrel{?}{=} \operatorname{ord}_{s=1} L(E/F,s)$$

and, setting $r = \operatorname{ord}_{s=1} L(E/F,s)$, that the leading coefficient is

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

where Ш is the Tate-Shafarevitch group, R is a regulator constructed from heights of a set of generators of $E(F)$, and τ is a certain Tamagawa number (an analogue of a period). We will not enter into the details of the definitions of these objects since they will play little role in what follows; see [Tat66b] for more details.

Much more is known about this conjecture in the function field case than in the number field case. Indeed, we have

$$\operatorname{Rank} E(F) \leq \operatorname{ord}_{s=1} L(E/F,s) \tag{2.1}$$

and the following assertions are equivalent:

(1) Equality holds in 2.1.
(2) The ℓ primary part of Ш is finite for any one prime ℓ ($\ell = p$ is allowed).
(3) Ш is finite.

Moreover, if these equivalent conditions are satisfied, then the refined conjecture on the leading coefficient of the L-series is true. The "prime-to-p" part of this was proven by Artin and Tate [Tat66b]. More precisely, they showed that equality holds in 2.1 if and only if the ℓ primary part of Ш is finite for any one prime $\ell \neq p$ if and only if the ℓ primary part of Ш is finite for every $\ell \neq p$, and that if these

conditions hold, the refined formula is correct up to a power of p. Milne proved the stronger statement above in [Mil75] for $p \neq 2$; due to later improvements in p-adic cohomology, his argument applies essentially verbatim to the case $p = 2$ as well.

These results were obtained by considering the elliptic surface $\mathcal{E} \to \mathcal{C}$ attached to E, which can be characterized as the unique smooth, proper surface over $\mathbb{F}_q$ admitting a flat and relatively minimal morphism to $\mathcal{C}$, with generic fiber E/F. Another key ingredient is Grothendieck's analysis of L-functions, which gives a cohomological interpretation of the ζ-function of $\mathcal{E}$ and the L-function of E.

Equality in 2.1, and therefore the full Birch and Swinnerton-Dyer conjecture, is known to hold in several cases (but certainly not the general case!): If it holds for E/K where K is a finite extension of F, then it holds for E/F (this is elementary); it holds for constant, and thus isotrivial, E (this follow from [Tat66a]); and it holds for several cases most easily described in terms of $\mathcal{E}$, namely if $\mathcal{E}$ is a rational surface (elementary), a $K3$ surface [ASD73], or if $\mathcal{E}$ is dominated by a product of curves (see [Tat94]). The rational and $K3$ cases are essentially those where the base field F is $\mathbb{F}_q(t)$ and the coefficients a_i in the defining Weierstrass equation of E have small degree in t.

3. Function field analogues of the Gross-Zagier theorem

In this section we will give some background on modularity and Heegner points and then discuss various works on Gross-Zagier formulas in the function field context. Our treatment will be very sketchy, just giving the main lines of the arguments, but we will give precise references where the reader may find the complete story. Throughout, we fix a smooth, proper, geometrically connected curve $\mathcal{C}$ over a finite field $\mathbb{F}_q$ of characteristic p and we set $F = \mathbb{F}_q(\mathcal{C})$.

3.1. **Two versions of modularity.** Recall that for elliptic curves over $\mathbb{Q}$ there are two (not at all trivially!) equivalent statements expressing the property that an elliptic curve E of conductor N is modular:

(1) There exists a modular form f (holomorphic of weight 2 and level $\Gamma_0(N)$) such that $L(E, \chi, s) = L(f, \chi, s)$ for all Dirichlet characters χ.
(2) There exists a non-constant morphism $X_0(N) \to E$ (defined over $\mathbb{Q}$).

(We note that over $\mathbb{Q}$, the equalities $L(E, \chi, s) = L(f, \chi, s)$ in (1) are implied by the *a priori* weaker statement that $L(E, s) = L(f, s)$. But this implication fails over higher degree number fields and over function fields and it is the stronger assertion that we need.)

In the next two subsections we will explain the analogues of these two statements in the function field context. In this case, the relationship between the two statements is a little more complicated than in the classical case. For example, the relevant automorphic forms are complex valued and thus are not functions or sections of line bundles on the analogue of $X_0(\mathfrak{n})$, which is a curve over F. Nevertheless, analogues of both modularity statements are theorems in the function field case.

3.2. **Analytic modularity.** We begin with (1). Let $\mathbb{A}_F$ be the adèle ring of F and $\mathcal{O}_F \subset \mathbb{A}_F$ the subring of everywhere integral adèles. Then for us, automorphic forms on GL_2 over F are functions on $\mathrm{GL}_2(\mathbb{A}_F)$ which are invariant under left

translations by $\mathrm{GL}_2(F)$ and under right translations by a finite index subgroup K of $\mathrm{GL}_2(\mathcal{O}_F)$. In other words, they are functions on the double coset space

$$\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A}_F)/K. \tag{3.2.1}$$

These functions may take values in any field of characteristic zero; to fix ideas, we take them with values in $\overline{\mathbb{Q}}$ and we fix embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and into $\overline{\mathbb{Q}}_\ell$ for some $\ell \neq p$. The subgroup K is the analogue of the level in the classical setting and the most interesting case is when K is one of the analogues $\Gamma_0(\mathfrak{m})$ or $\Gamma_1(\mathfrak{m})$ of the Hecke congruence subgroups where $\mathfrak{m}$ is an effective divisor on $\mathcal{C}$. If $\psi : \mathbb{A}^\times/F^\times \to \overline{\mathbb{Q}}_\ell{}^\times$ is an idèle class character and f is an automorphic form, we say 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 $g \in \mathrm{GL}_2(\mathbb{A}_F)$. The central character plays the role of weight: When k is a positive integer and $\psi(z) = |z|^{-k}$ (where $|\cdot|$ is the adèlic norm), f is analogous to a classical modular form of weight k. The basic reference for this point of view is [Wei71]; see Chapter III for definitions and first properties. For a more representation-theoretic point of view, see [JL70].

If we single out a place ∞ of F and assume that $K = \Gamma_0(\infty\mathfrak{n})$ where $\mathfrak{n}$ is prime to ∞, then there is an analogue of the description of classical modular forms as functions on the upper half plane. Namely, an automorphic form f may be viewed as a function (or a section of line bundle if the ∞ component of ψ is non-trivial) on a finite number of copies of the homogeneous space $\mathrm{PGL}_2(F_\infty)/\Gamma_0(\infty)$ which has the structure of an oriented tree. (Compare with $\mathrm{PGL}_2(\mathbb{R})/O_2(\mathbb{R}) \cong \mathbb{H}$.) The corresponding functions are invariant under certain finite index subgroups of $\mathrm{GL}_2(A) \subset \mathrm{GL}_2(F_\infty)$ where $A \subset F$ is the ring of functions regular outside ∞. The various copies of the tree are indexed by a generalized ideal class group of A. This point of view is most natural when $F = \mathbb{F}_q(t)$ and ∞ is the standard place $t = \infty$, in which case there is just one copy of the tree and this description is fairly canonical. In the general case, there are several copies of the tree and choices must be made to identify automorphic forms with functions on trees. Using this description (or suitable Hecke operators) one may define the notion of a form being "harmonic" or "special" at ∞. Namely, sum of the values over edges with a fixed terminus should be zero. This is an analogue of being holomorphic. See [DH87, Chap. 5], [GR96, Chap. 4], or [vdPR97, Chap. 2] for details.

Automorphic forms have Fourier expansions, with coefficients naturally indexed by effective divisors on $\mathcal{C}$. There are Hecke operators, also indexed by effective divisors on $\mathcal{C}$ and the usual connection between eigenvalues of Hecke operators and Fourier coefficients of eigenforms holds. There is a notion of cusp form and for a fixed K and ψ the space of cusp forms is finite dimensional. An automorphic form f gives rise to an L-function $L(f, s)$, which is a complex valued function of a complex variable s. If f is a cuspidal eigenform, this L-function has an Euler product, an analytic continuation to an entire function of s, and satisfies a functional equation. See [Wei71] for all of this except the finite dimensionality, which follows easily from reduction theory. See [Ser80, Chap. II] for the finite dimensionality when $F = \mathbb{F}_q(t)$ and [HLW80] for an explicit dimension formula in the general case.

The main theorem of [Wei71] is a "converse" theorem which says roughly that a Dirichlet series with a suitable analytic properties is the L-function of an automorphic form on GL_2. (The function field case is Theorem 3 of Chapter VII.) The most important requirement is that sufficiently many of the twists of the given Dirichlet

series by finite order characters should satisfy functional equations. This result was also obtained by representation theoretic methods in [JL70]. Also, see [Li84] for an improved version, along the lines of [Wei71].

Now let E be an elliptic curve over F. By Grothendieck's analysis of L-functions, we know that the Dirichlet series $L(E,s)$ is meromorphic (entire if E is non-isotrivial) and its twists satisfy functional equations. In [Del73, 9.5-9.7], Deligne verified the hypotheses of Weil's converse theorem. The main point is to check that the functional equations given by Grothendieck's theory are the same as those required by Weil. The form f_E associated to E is characterized by the equalities $L(E,\chi,s) = L(f_E,\chi,s)$ for all finite order idèle class characters χ. It is an eigenform for the Hecke operators and is a cusp form if E is non-isotrivial. Its level is $\Gamma_0(\mathfrak{m})$ where $\mathfrak{m}$ is the conductor of E and it has central character $|\cdot|^{-2}$ (i.e., is analogous to a form of weight 2). If E has split multiplication at ∞, then f_E is special at ∞. The construction of f_E from E is the function field analogue of (1) above.

3.3. **Geometric modularity.** We now turn to Drinfeld modules and (2). There is a vast literature on Drinfeld modules and we will barely scratch the surface. The primary reference is [Dri74] and there are valuable surveys in [DH87] and [GvdPRG97].

Fix a place ∞ of F and define A to be the ring of elements of F regular away from ∞. Let F_∞ denote the completion of F at ∞ and C the completion of the algebraic closure of F_∞. The standard example is when $F = \mathbb{F}_q(t)$, ∞ is the standard place $t = \infty$, and $A = \mathbb{F}_q[t]$.

Let k be a ring of characteristic p equipped with a homomorphism $A \to k$. Let $k\{\tau\}$ be the ring of non-commutative polynomials in τ, with commutation relation $\tau a = a^p \tau$. There is a natural inclusion $\epsilon : k \hookrightarrow k\{\tau\}$ with left inverse $D : k\{\tau\} \to k$ defined by $D(\sum_n a_n \tau^n) = a_0$. If R is any k-algebra, we may make the additive group of R into a module over $k\{\tau\}$ by defining $(\sum_n a_n \tau^n)(x) = \sum_n a_n x^{p^n}$.

A Drinfeld module over k (or elliptic module as Drinfeld called them) is a ring homomorphism $\phi : A \to k\{\tau\}$ whose image is not contained in k and such that $D \circ \phi : A \to k$ is the given homomorphism. The characteristic of ϕ is by definition the kernel of the homomorphism $A \to k$, which is a prime ideal of A. It is convenient to denote the image of $a \in A$ by ϕ_a rather than $\phi(a)$. If $A = \mathbb{F}_q[t]$ then ϕ is determined by ϕ_t, which can be any element of $k\{\tau\}$ of positive degree with constant term equal to the image of t under $A \to k$. For a general A and k equipped with $A \to k$ there may not exist any Drinfeld modules and if they do exist, they may not be easy to find. As above, a Drinfeld module ϕ turns any k-algebra into an A-module by the rule $a \cdot x = \phi_a(x)$.

It turns out that $a \mapsto \phi_a$ is always injective and there exists a positive integer r, the rank of ϕ, such that $p^{\deg_\tau(\phi_a)} = |a|_\infty^r = \#(A/a)^r$. If ϕ and ϕ' are Drinfeld modules over k, a homomorphism $u : \phi \to \phi'$ is by definition an element $u \in k\{\tau\}$ such that $u\phi_a = \phi'_a u$ for all $a \in A$ and an isogeny is a non-zero homomorphism. Isogenous Drinfeld modules have the same rank and characteristic. See [Dri74, §2] or [DH87, Chap. 1].

We will only consider Drinfeld modules of rank 2. These objects are in many ways analogous to elliptic curves. For example, if k is an algebraically closed field

and $\mathfrak{p} \subset A$ is a prime ideal, then we have an isomorphism of A-modules

$$\phi[\mathfrak{p}](k) := \{x \in k | \phi_a(x) = 0 \text{ for all } a \in \mathfrak{p}\} \cong (A/\mathfrak{p})^e$$

where $0 \leq e \leq 2$ and $e = 2$ if the characteristic of ϕ is relatively prime to $\mathfrak{p}$. A second analogy occurs with endomorphism rings: $\mathrm{End}(\phi)$, the ring of endomorphisms of ϕ, is isomorphic as A-module to either A, an A-order in an "imaginary" quadratic extension K of F, or an A-order in a quaternion algebra over F. Here "imaginary" means that the place ∞ of F does not split in K and an A-order in a division algebra D over F is an A-subalgebra R which is projective of rank 4 as A-module. The quaternion case can occur only if the characteristic of ϕ is non-zero, in which case the quaternion algebra is ramified precisely at ∞ and the characteristic of ϕ. A third analogy is the analytic description of Drinfeld modules over C: giving a Drinfeld module of rank 2 over C up to isomorphism is equivalent to giving a rank 2 A-lattice in C up to homothety by elements of $C^\times$. If ϕ corresponds to the lattice Λ, there is a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & C & \xrightarrow{\exp_\Lambda} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \phi_a} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & C & \xrightarrow{\exp_\Lambda} & C & \longrightarrow & 0 \end{array}$$

where $\exp_\Lambda : C \to C$ is the Drinfeld exponential associated to Λ. See [Dri74, §§2-3] or [DH87, Chaps. 1-2].

There is a natural generalization of all of the above to Drinfeld modules over schemes of characteristic p. Given an effective divisor $\mathfrak{n}$ on $\mathcal{C}$ relatively prime to ∞ (or equivalently, a non-zero ideal of A), there is a notion of "level $\mathfrak{n}$ structure" on a Drinfeld module. Using this notion, one may construct a moduli space $Y_0(\mathfrak{n})$ (a scheme if $\mathfrak{n}$ is non-trivial and a stack if $\mathfrak{n}$ is trivial) parameterizing Drinfeld modules of rank 2 with level $\mathfrak{n}$ structure, or equivalently, pairs of rank 2 Drinfeld modules connected by a "cyclic $\mathfrak{n}$-isogeny" $u : \phi \to \phi'$. (The notions of level $\mathfrak{n}$ structure and cyclic isogeny are somewhat subtle and a significant advance over the naive notions. Analogues of Drinfeld's notions were used in [KM85] to completely analyze the reduction of classical modular curves at primes dividing the level.) The curve $Y_0(\mathfrak{n})$ is smooth and affine over F and may be completed to a smooth, proper curve $X_0(\mathfrak{n})$. The added points ("cusps") can be interpreted in terms of certain degenerations of Drinfeld modules. The curve $X_0(\mathfrak{n})$ carries many of the structures familiar from the classical case, such as Hecke correspondences (indexed by effective divisors on $\mathcal{C}$) and Atkin-Lehner involutions. See [Dri74, §5] and [DH87, Chap. 1, §6]. The construction of the moduli space (or stack) is done very carefully in [Lau96, Chap. 1] and the interpretation of the cusps is given in [vdPT97].

The analytic description of Drinfeld modules over C yields an analytic description of the C points of $Y_0(\mathfrak{n})$. Namely, let Ω denote the Drinfeld upper half plane: $\Omega = \mathbb{P}^1(C) \setminus P^1(F_\infty)$. Then $Y_0(\mathfrak{n})(C)$ is isomorphic (as rigid analytic space) to a union of quotients of Ω by finite index subgroups of $\mathrm{GL}_2(A)$. The components of $Y_0(\mathfrak{n})(C)$ are indexed by a generalized ideal class group of A. More adelically, we have an isomorphism

$$Y_0(\mathfrak{n}) \cong \mathrm{GL}_2(F) \backslash \left(GL_2(\mathbb{A}_F^f) \times \Omega \right) / \Gamma_0(\mathfrak{n})^f$$

where $\mathbb{A}_F^f$ denotes the "finite adèles" of F, namely the adèles with the component at ∞ removed, and similarly with $\Gamma_0(\mathfrak{n})^f$. See [Dri74, §6] or [DH87, Chap. 3].

This description reveals a close connection between $Y_0(\mathfrak{n})$ and the description of automorphic forms as functions on trees (cf. 3.2.1). Namely, there is a map between the Drinfeld upper half plane Ω and a geometric realization of the tree $\mathrm{PGL}_2(F_\infty)/\Gamma_0(\infty)$. Using this, Drinfeld was able to analyze the étale cohomology of $X_0(\mathfrak{n})$ as a module for $\mathrm{Gal}(\overline{F}/F)$ and the Hecke operators, in terms of automorphic forms of level $\Gamma_0(\mathfrak{n}\infty)$ which are special at ∞. (Drinfeld used an *ad hoc* definition of étale cohomology; for a more modern treatment, see [vdPR97].) This leads to one form of the Drinfeld reciprocity theorem: if f is an eigenform of level $\Gamma_0(\mathfrak{n}\infty)$ which is special at ∞, then there exists a factor A_f of the Jacobian $J_0(\mathfrak{n})$ of $X_0(\mathfrak{n})$, well-defined up to isogeny, such that

$$L(A_f, \chi, s) = \prod_{\sigma:\mathbb{Q}(f)\hookrightarrow\mathbb{C}} L(f^\sigma, \chi, s)$$

for all finite order idèle class characters χ of F. Here the product is over all embeddings of the number field generated by the Fourier coefficients of f into $\mathbb{C}$. If the Hecke eigenvalues of f are rational integers, then A_f is an elliptic curve, and if f is a new, then E has conductor $\mathfrak{n}\infty$ and is split multiplicative at ∞. See [Dri74, §§10-11], [DH87, Chaps. 4-5], and [GR96, Chap. 8].

So, starting with an elliptic curve E over F of level $\mathfrak{m} = \mathfrak{n}\infty$ which is split multiplicative at ∞, Deligne's theorem gives us an automorphic form f_E on GL_2 over F of level $\mathfrak{m}$ which is special at ∞ and which has integer Hecke eigenvalues. From f_E, Drinfeld's construction gives us an isogeny class of elliptic curves A_{f_E} appearing in the Jacobian of $X_0(\mathfrak{n})$. Moreover, we have equalities of L-functions:

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

But Zarhin proved that the L-function of an abelian variety A over a function field (by which we mean the collection of all twists $L(A, \chi, s)$) determines its isogeny class. See [Zar74] for the case $p > 2$ and [MB85, XXI.2] for a different proof that works in all characteristics. This means that E is in the class A_{f_E} and therefore we have a non-trivial modular parameterization $X_0(\mathfrak{n}) \to E$.

In [GR96, Chap. 9] Gekeler and Reversat completed this picture by giving a beautiful analytic construction of $J_0(N)(C)$ and of the analytic parameterization $X_0(\mathfrak{n})(C) \to E(C)$. This is the analogue of the classical parameterization of an elliptic curve by modular functions. Recently, Papikian has studied the degrees of Drinfeld modular parameterizations and proved the analogue of the degree conjecture. See [Pap02] and forthcoming publications.

3.4. **Heegner points and Brown's work.** It was clear to the experts from the beginning that Heegner points, the Gross-Zagier formula, and Kolyvagin's work could all be extended to the function field case, using the Drinfeld modular parameterization, although people were reluctant to do so. The first efforts in this direction were made by Brown in [Bro94].

Fix as usual F, ∞, A, and $\mathfrak{n}$, so we have the Drinfeld modular curve $X_0(\mathfrak{n})$. Let K/F be an imaginary quadratic extension and let B be an A-order in K. A Drinfeld-Heegner point with order B (or Heegner point for short) is by definition a point on $X_0(\mathfrak{n})$ corresponding to a pair $\phi \to \phi'$ connected by a cyclic $\mathfrak{n}$ isogeny such that $\mathrm{End}(\phi) = \mathrm{End}(\phi') = B$. These will exist if and only if there exists a

proper ideal $\mathfrak{n}'$ of B (i.e., one such that $\{b \in K | b\mathfrak{n}' \subset \mathfrak{n}'\} = B$) with $B/\mathfrak{n}' \cong A/\mathfrak{n}$. The simplest situation is when every prime dividing $\mathfrak{n}$ splits in K and B is the maximal A-order in K, i.e., the integral closure of A in K. Assuming B has such an ideal $\mathfrak{n}'$, we may construct Heegner points using the analytic description of Drinfeld modules over C as follows. If $\mathfrak{a} \subset B$ is a non-zero proper ideal then the pair of Drinfeld modules ϕ and ϕ' corresponding to the lattices $\mathfrak{n}'\mathfrak{a}$ and $\mathfrak{a}$ in $K \hookrightarrow C$ satisfy $\mathrm{End}(\phi) = \mathrm{End}(\phi') = B$ and they are connected by a cyclic $\mathfrak{n}$-isogeny. The corresponding point turns out to depend only on B, $\mathfrak{n}'$, and the class of $\mathfrak{a}$ in $\mathrm{Pic}(B)$ and it is defined over the ring class field extension K_B/K corresponding to B by class field theory. The theory of complex multiplication of Drinfeld modules implies that $\mathrm{Gal}(K_B/K) \cong \mathrm{Pic}(B)$ acts on the Heegner points through its natural action on the class of $\mathfrak{a}$. Applying an Atkin-Lehner involution to a Heegner point is related to changing the choice of ideal $\mathfrak{n}'$ over $\mathfrak{n}$. All of this is discussed in [Bro94, §2] in the context where $A = \mathbb{F}_q[t]$.

Taking the trace from K_B to K of a Heegner point and subtracting a suitable multiple of a cusp, we get a K-rational divisor of degree 0, and so a point $J_0(\mathfrak{n})(K)$. We write Q_K for the point so constructed when K is an imaginary quadratic extension of F in which every prime dividing $\mathfrak{n}$ splits and B is the maximal A-order in K. The point Q_K is well-defined, independently of the other choices ($\mathfrak{n}'$ and $\mathfrak{a}$), up to a torsion point of $J_0(\mathfrak{n})(K)$. If E is an elliptic curve over F of level $\mathfrak{n}\infty$ with split multiplicative reduction at ∞, then using the modular parameterization discussed above one obtains a point $P_K \in E(K)$, well-defined up to torsion.

Brown purports to prove, by methods analogous to those of Kolyvagin [Kol90], that if P_K is non-torsion, then the Tate-Shafarevitch group of E is finite and the rank of $E(K)$ is one. (He gives an explicit annihilator of the ℓ-primary part of $Ш$ for infinitely many ℓ.) As we have seen, this implies that the Birch and Swinnerton-Dyer conjecture holds for E over K.

Unfortunately, Brown's paper is marred by a number of errors, some rather glaring. For example, the statement of the main theorem is not in fact what is proved and it is easily seen to be false if taken literally. Also, he makes the strange hypothesis that q, the number of elements in the finite ground field, is not a square. The source of this turns out to be a misunderstanding of quadratic reciprocity in the proof of his Corollary 3.4. In my opinion, although something like what Brown claims can be proved by the methods in his paper, a thorough revision is needed before his theorem can be said to have been proven.

There is another difficulty, namely that Brown's theorem does not give a very direct approach to the Birch and Swinnerton-Dyer conjecture. This is because it is rather difficult to compute the modular parameterization and thus the Heegner point, and so the hypotheses of Brown's theorem are hard to verify. (The difficulty comes from the fact that non-archimedean integration seems to be of exponential complexity in the desired degree of accuracy, in contrast to archimedean integration which is polynomial time.) On the other hand it is quite easy to check whether the L-function of E vanishes to order 0 or 1, these being the only cases where one expects Heegner points to be of help. In fact the computation of the entire L-function of E is straightforward and (at least over the rational function field) can be made efficient using the existence of an automorphic form corresponding to E. See [TR92]. This situation is the opposite of that in the classical situation; cf. the remarks of Birch near the end of §4 of his article in this volume [Bir04].

In light of this difficulty, a more direct and straightforward approach to the Birch and Swinnerton-Dyer conjecture for elliptic curves of rank ≤ 1 is called for. My interest in function field analogues of Gross-Zagier came about from an effort to understand Brown's paper and to find a better approach to BSD in this context.

3.5. **Gross-Zagier formulas.** Let us now state what the analogue of the Gross-Zagier formula [GZ86] should be in the function field context. Let E be an elliptic curve over F of conductor $\mathfrak{n}\infty$ and with split multiplicative reduction at ∞. Then for every imaginary quadratic extension K of F satisfying the Heegner hypotheses (namely that every prime dividing $\mathfrak{n}$ is split in K), we have a point $P_K \in E(K)$ defined using Heegner points on $X_0(\mathfrak{n})$ and the modular parameterization. The desired formula is then

$$L'(E/K,1) = a\langle P_K, P_K\rangle \tag{3.5.1}$$

where $\langle,\rangle$ is the Néron-Tate canonical height on E and a is an explicit non-zero constant. Because equality of analytic and algebraic ranks implies the refined BSD conjecture, the exact value of a is not important for us.

The left hand side of this formula is also a special value of the L-function of an automorphic form (namely, the f such that $L(E,\chi,s) = L(f,\chi,s)$) and Equation 3.5.1 is a special case of a more general formula which applies to automorphic forms without the assumption that their Hecke eigenvalues are integers. Let S be the vector space of complex valued cuspidal automorphic forms on GL_2 over F which have level $\Gamma_0(\mathfrak{n}\infty)$, central character $|\cdot|^{-2}$, and which are special at ∞. (As discussed in Subsection 3.2, this is the analogue of $S_2(\Gamma_0(N))$.) Then we have a Petersson inner product

$$(\ ,\ ) : S \times S \to \mathbb{C}$$

which is positive definite Hermitian. For $f \in S$, let $L_K(f,s)$ be the L-function of the base change of f to a form on GL_2 over K. (This form can be shown to exist using a Rankin-Selberg integral representation and Weil's converse theorem.) Then the function $f \mapsto L'_K(f,1)$ is a linear map $S \to \mathbb{C}$ and so there exists a unique element $h_K \in S$ such that

$$(f, h_K) = L'_K(f,1)$$

for all $f \in S$.

For $h \in S$, let $c(h,\mathfrak{m})$ be the $\mathfrak{m}$-th Fourier coefficient of h. Then a formal Hecke algebra argument, as in the classical case, shows that the desired Gross-Zagier formula 3.5.1 (and its more general version mentioned above) follows from the following equalities between Fourier coefficients and heights on $J_0(\mathfrak{n})$:

$$c(h_K,\mathfrak{m}) = a\langle Q_K, T_{\mathfrak{m}} Q_K\rangle \tag{3.5.2}$$

for all effective divisors $\mathfrak{m}$ prime to $\mathfrak{n}\infty$. Here $T_{\mathfrak{m}}$ is the Hecke operator on $J_0(\mathfrak{n})$ indexed by $\mathfrak{m}$ and $\langle,\rangle$ is the canonical height pairing on $J_0(\mathfrak{n})$.

From now on, by "Gross-Zagier formula" we will mean the sequence of equalities 3.5.2.

3.6. **Rück-Tipp.** Rück and Tipp were the first to write down a function field analogue of the Gross-Zagier formula [RT00]. They work over $F = \mathbb{F}_q(t)$ with q odd, and ∞ the standard place at infinity $t = \infty$ (so their ∞ has degree 1). They assume that $\mathfrak{n}$ is square free and that $K = F(\sqrt{D})$ where D is an *irreducible* polynomial in $\mathbb{F}_q[t]$. Under these hypotheses, they checked the equalities 3.5.2 for

all $\mathfrak{m}$ prime to $\mathfrak{n}\infty$, which yields the formula 3.5.1. This gives some instances of the conjecture of Birch and Swinnerton-Dyer, under very restrictive hypotheses.

Their paper follows the method of Gross and Zagier [GZ86] quite closely (which is not to say that the analogies are always obvious or easy to implement!). They use the Rankin-Selberg method and a holomorphic projection operator to compute the Fourier coefficients of h_K. The height pairing is decomposed as a sum of local terms and, at finite places, the local pairing is given as an intersection number, which can be computed by counting isogenies between Drinfeld modules over a finite field. The local height pairing at ∞ is also an intersection number and one might hope to use a moduli interpretation of the points on the fibre at ∞ to calculate the local height. But to my knowledge, no one knows how to do this. Instead, Rück and Tipp compute the local height pairing using Green's functions on the Drinfeld upper half plane. This is a very analytic way of computing a rational number, but it matches well with the computations on the analytic side of the formula.

3.7. **Pál and Longhi.** Pál and Longhi worked (independently) on function field analogues of the Bertolini-Darmon [BD98] p-adic construction of Heegner points. Both work over a general function field F of odd characteristic. Let E be an elliptic curve over F with conductor $\mathfrak{n}\infty$ and which is split multiplicative at ∞. Let K be a quadratic extension in which ∞ is inert and which satisfies the Heegner hypotheses with respect to E. Also let H_n be the ring class field of K of conductor ∞^n and set $G = \varprojlim \mathrm{Gal}(H_n/K)$.

Pál [Pál00] used "Gross-Heegner" points, as in Bertolini-Darmon (following Gross [Gro87]), to construct an element $\mathcal{L}(E/K)$ in the completed group ring $\mathbb{Z}[[G]]$ which interpolates suitably normalized special values $L(E/K,\chi,1)$ for finite order characters χ of G. It turns out that $\mathcal{L}(E/K)$ lies in the augmentation ideal I of $\mathbb{Z}[[G]]$ and so defines an element $\mathcal{L}'(E/K)$ in $I/I^2 \cong \mathcal{O}_{K_\infty}^\times/\mathcal{O}_{F_\infty}^\times \cong \mathcal{O}_{K_\infty,1}^\times$. (Here F_∞ and K_∞ are the completions at ∞ and $\mathcal{O}_{K_\infty,1}^\times$ denotes the 1-units in $\mathcal{O}_{K_\infty}$.) Since E is split multiplicative at ∞, we have a Tate parameterization $K_\infty^\times \to E(K_\infty)$ and Pál shows that the image of $\mathcal{L}'(E/K)$ in $E(K_\infty)$ is a global point. More precisely, if E is a "strong Weil curve," then Pál's point is $P_K - \overline{P}_K$ where P_K is the Heegner point discussed above and $\overline{P}_K$ is its "complex conjugate." It follows that if $\mathcal{L}'(E/K)$ is non-zero, then the Heegner point is of infinite order and so $\mathrm{Rank}_{\mathbb{Z}} E(K)$ is at least one. One interesting difference between Pál's work and [BD98] is that in the latter, there are 2 distinguished places, namely ∞, which is related to the classical modular parameterization, and p, which is related to the Tate parameterization. In Pál's work, the role of both of these primes is played by the prime ∞ of F. This means that his result is applicable in more situations than the naive analogy would predict—E need only have split multiplicative reduction at one place of F.

Longhi [Lon02] also gives an ∞-adic construction of a Heegner point. Whereas Pál follows [BD98], Longhi's point of view is closer to that of [BD01]. His ∞-adic L-element $\mathcal{L}(E/K)$ is constructed using ∞-adic integrals, following the approach of Schneider [Sch84] and a multiplicative version of Teitelbaum's Poisson formula [Tei91]. Unfortunately, there is as yet no connection between his ∞-adic $\mathcal{L}(E/K)$ and special values of L-functions.

Both of these works have the advantage of avoiding intricate height computations on Drinfeld modular curves, as in [GZ86]. (Pál's work uses heights of the much

simpler variety considered in [Gro87].) On the other hand, they do not yet have any direct application to the conjecture of Birch and Swinnerton-Dyer, because presently we have no direct link between the ∞-adic L-derivative $\mathcal{L}'(E/K)$ and the classical L-derivative $L'(E/K,1)$.

3.8. **My work on BSD for rank 1.** My interest in this area has been less in analogues of the Gross-Zagier formula or Kolyvagin's work over function fields *per se*, and more in their applications to the Birch and Swinnerton-Dyer conjecture itself. The problem with a raw Gross-Zagier formula is that it only gives the BSD conjecture with parasitic hypotheses. For example, to have a Drinfeld modular parameterization, and thus Heegner points, the elliptic curve must have split multiplicative reduction at some place and the existence of such a place presumably has nothing to do with the truth of the conjecture. Recently, I have proven a non-vanishing result which when combined with a suitable Gross-Zagier formula leads to a clean, general statement about Birch and Swinnerton-Dyer: "If E is an elliptic curve over a function field F of characteristic > 3 and $\operatorname{ord}_{s=1} L(E/F,s) \leq 1$, then the Birch and Swinnerton-Dyer conjecture holds for E." In the remainder of this section I will describe the non-vanishing result, and then give the statement and status of the Gross-Zagier formula I have in mind.

Thus, let E be an elliptic curve over F with $\operatorname{ord}_{s=1} L(E/F,s) \leq 1$; for purposes of BSD we may as well assume that $\operatorname{ord}_{s=1} L(E/F,s) = 1$ and that E is non-isotrivial. Because $j(E) \notin \mathbb{F}_q$, it has a pole at some place of F, i.e., E is potentially multiplicative there. Certainly we can find a finite extension F' of F such that E has a place of split multiplicative reduction and it will suffice to prove BSD for E over F'. But, to do this with Heegner points, we must be able to choose F' so that $\operatorname{ord}_{s=1} L(E/F',s)$, which is *a priori* ≥ 1, is equal to 1. This amounts to a non-vanishing statement for a (possibly non-abelian) twist of $L(E/F,s)$, namely $L(E/F',s)/L(E/F,s)$. Having done this, a similar issue comes up in the application of a Gross-Zagier formula, namely, we must find a quadratic extension K/F' satisfying the Heegner hypotheses such that $\operatorname{ord}_{s=1} L(E/K,s) = \operatorname{ord}_{s=1} L(E/F',s) = 1$. This amounts to a non-vanishing statement for quadratic twists of $L(E/F',s)$ by characters satisfying certain local conditions. This issue also comes up in the applications of the classical Gross-Zagier formula and is dealt with by automorphic methods. Recently, I have proven a very general non-vanishing theorem for motivic L-functions over function fields using algebro-geometric methods which when applied to elliptic curves yields the following result:

Theorem 3.8.1. [Ulm03] *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 $\operatorname{ord}_{s=1} L(E/K,s) = \operatorname{ord}_{s=1} L(E/F',s) = 1$.*

This result, plus a suitable Gross-Zagier formula, yields the desired theorem. Indeed, by point (2), E admits a Drinfeld modular parameterization over F' and

by point (3) we will have a Heegner defined over K. Point (4) (plus GZ!) guarantees that the Heegner point will be non-torsion and so we have $\operatorname{Rank} E(K) \geq 1$. As we have seen, this implies BSD for E over K and thus also over F. Point (1) is included as it makes the needed GZ formula a little more tractable. Also, although it is not stated in the theorem, it is possible to specify whether the place ∞ of F' is inert or ramified in K and this too can be used to simplifly the Gross-Zagier calculation.

Thus, the Gross-Zagier formula we need is in the following context: the base field F' is arbitrary but the level $\mathfrak{n}$ is square-free and we may assume that ∞ is inert (or ramified) in K. It would perhaps be unwise to write too much about a result which is not completely written and refereed, so I will just say a few words. The proof follows closely the strategy of Gross and Zagier, with a few simplifications due to Zhang [Zha01]. One computes the analytic side of 3.5.2 using the Rankin-Selberg method and a holomorphic projection and the height side is treated using intersection theory at the finite places and Green's functions at ∞. Because we work over an arbitrary function field, our proofs are necessarily adelic. Also, in the analytic part we emphasize the geometric view of automorphic forms, namely that they are functions on a moduli space of rank 2 vector bundles on $\mathcal{C}$. The full details will appear in [Ulma].

4. Ranks over function fields

We now move beyond rank 1 and consider the rank conjecture for elliptic curves over function fields. Recall from Section 2 the notions of constant, isotrivial, and non-isotrivial for elliptic curves over function fields. Our purpose in this section is to explain constructions of isotrivial and non-isotrivial elliptic curves over $\mathbb{F}_p(t)$ whose Mordell-Weil groups have arbitrarily large rank. These curves turn out to have asymptotically maximal rank, in a sense which we will explain in Section 5.

4.1. **The Shafarevitch-Tate construction.** First, note that if E is a constant elliptic curve over $F = \mathbb{F}_q(\mathcal{C})$ based on E_0, then $E(F) \cong \operatorname{Mor}_{\mathbb{F}_q}(\mathcal{C}, E_0)$ (morphisms defined over $\mathbb{F}_q$) and the torsion subgroup of $E(F)$ corresponds to constant morphisms. Since a morphism $\mathcal{C} \to E$ is determined up to translation by the induced map of Jacobians, we have $E(F)/tor \cong \operatorname{Hom}_{\mathbb{F}_q}(J(\mathcal{C}), E)$ where $J(\mathcal{C})$ denotes the Jacobian of $\mathcal{C}$.

The idea of Shafarevitch and Tate [TS67] was to take E_0 to be supersingular and to find a curve $\mathcal{C}$ over $\mathbb{F}_p$ which is hyperelliptic and such that $J(\mathcal{C})$ has a large number of factors isogenous to E_0. If E denotes the constant curve over $\mathbb{F}_p(t)$ based on E_0, then it is clear that $E(\mathbb{F}_p(t))$ has rank 0. On the other hand, over the quadratic extension $F = \mathbb{F}_p(\mathcal{C})$, $E(F)/tor \cong \operatorname{Hom}_{\mathbb{F}_q}(J(\mathcal{C}), E_0)$ has large rank. Thus if we let E' be the twist of E by the quadratic extension $F/\mathbb{F}_q(t)$, then $E'(\mathbb{F}_q(t))$ has large rank. Note that E' is visibly isotrivial.

To find such curves $\mathcal{C}$, Tate and Shafarevitch considered quotients of the Fermat curve of degree $p^n + 1$ with n odd. The zeta functions of Fermat curves can be computed in terms of Gauss sums, and in the case of degree of the form $p^n + 1$, the relevant Gauss sums are easy to make explicit. This allows one to show that the Jacobian is isogenous to a product of supersingular elliptic curves over $\overline{\mathbb{F}}_p$ and has a supersingular elliptic curve as isogeny factor to high multiplicity over $\mathbb{F}_p$.

We remark that the number of factors of $J(\mathcal{C})$ which are isogenous to E_0 may go up under extension of the ground field, and so the rank of E' may also go up.

In fact, the rank of the Shafarevitch-Tate curves goes up considerably: if the rank of $E'(\mathbb{F}_p(t))$ is r, then the rank of $E'(\overline{\mathbb{F}}_p(t))$ is of the order $2\log_p(r)r$.

It has been suggested by Rubin and Silverberg that one might be able to carry out a similar construction over $\mathbb{Q}(t)$, i.e., one might try to find hyperelliptic curves $\mathcal{C}$ defined over $\mathbb{Q}$ whose Jacobians have as isogeny factor a large number of copies of some elliptic curve. The obvious analogue of the construction above would then produce elliptic curves over $\mathbb{Q}(t)$ of large rank. In [RS01] they use this idea to find many elliptic curves of rank ≥ 3. Unfortunately, it is not at all evident that curves $\mathcal{C}$ such that $J(\mathcal{C})$ has an elliptic isogeny factor to high multiplicity exist, even over $\mathbb{C}$.

Back to the function field case: We note that isotrivial elliptic curves are very special and seem to have no analogue over $\mathbb{Q}$. Thus the relevance of the Shafarevitch-Tate construction to the rank question over $\mathbb{Q}$ is not clear. In the next subsection we explain a construction of *non-isotrivial* elliptic curves over $\mathbb{F}_p(t)$ of arbitrarily large rank.

4.2. **Non-isotrivial elliptic curves of large rank.** In [Shi86], Shioda showed that one could often compute the Picard number of a surface which is dominated by a Fermat surface. He applied this to write down elliptic curves over $\overline{\mathbb{F}}_p(t)$ (with $p \equiv 3 \mod 4$) of arbitrarily large rank, using supersingular Fermat surfaces (i.e., those whose degrees divide p^n+1 for some n). I was able to use the idea of looking at quotients of Fermat surfaces and a different method of computing the rank to show the existence of elliptic curves over $\mathbb{F}_p(t)$ (any p) with arbitrarily large rank. Here is the precise statement:

Theorem 4.2.1. [Ulm02] *Let p be a prime, n a positive integer, and d a divisor of 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

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

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

In particular, if we take $d = p^n+1$ and $q = p$, then the rank of E over $\mathbb{F}_p(t)$ is at least $(p^n-1)/2n$. On the other hand, if we take $d = p^n+1$ and q to be a power of p^{2n}, then the rank of E over $\mathbb{F}_q(t)$ is $d-1 = p^n$ if $6 \nmid d$ and $d-3 = p^n-2$ if $6|d$. Note that the rank may increase significantly after extension of $\mathbb{F}_q$.

Here is a sketch of the proof: by old work of Artin and Tate [Tat66b], the conjecture of Birch and Swinnerton-Dyer of E is equivalent to the Tate conjecture for the elliptic surface $\mathcal{E} \to \mathbb{P}^1$ over $\mathbb{F}_q$ attached to E. (The relevant Tate conjecture is that $-\operatorname{ord}_{s=1}\zeta(\mathcal{E},s) = \operatorname{Rank}_{\mathbb{Z}} NS(\mathcal{E})$ where $NS(\mathcal{E})$ denotes the Néron-Severi group of $\mathcal{E}$.) The equation of E was chosen so that $\mathcal{E}$ is dominated by the Fermat surface *of the same degree d*. (The fact that the equation of E has 4 monomials is essentially enough to guarantee that $\mathcal{E}$ is dominated by some Fermat surface; getting the degree right requires more.) Since the Tate conjecture is known for

Fermat surfaces, this implies it also for $\mathcal{E}$ (and thus BSD for E). Next, a detailed analysis of the geometry of the rational map $F_d \dashrightarrow \mathcal{E}$ allows one to calculate the zeta function of $\mathcal{E}$ in terms of that of F_d, i.e., in terms of Gauss and Jacobi sums. Finally, because d is a divisor of $p^n + 1$, the relevant Gauss sums are all supersingular (as in the Shafarevitch-Tate case) and can be made explicit. This gives the order of pole of $\zeta(\mathcal{E}, s)$ at $s = 1$ and thus the order of zero of $L(E/\mathbb{F}_q(t), s)$ at $s = 1$, and thus the rank.

We note that the proof does not explicitly construct any points, although it does suggest a method to do so. Namely, using the large automorphism group of the Fermat surface, one can write down curves which span $NS(F_d)$ and use these and the geometry of the map $F_d \dashrightarrow \mathcal{E}$ to get a spanning set for $NS(\mathcal{E})$ and thus a spanning set for $E(\mathbb{F}_q(t))$. It looks like an interesting problem to make this explicit, and to consider the heights of generators of $E(\mathbb{F}_q(t))$ and its Mordell-Weil lattice.

4.3. **Another approach to high rank curves.** The two main parts of the argument of Subsection 4.2 could be summarized as follows: (i) one can deduce the Tate conjecture for $\mathcal{E}$ and thus the BSD conjecture for E from the existence of a dominant rational map from the Fermat surface F_d to the elliptic surface $\mathcal{E}$ attached to E; and (ii) a detailed analysis of the geometry of the map $F_d \dashrightarrow \mathcal{E}$ allows one to compute the zeta function of $\mathcal{E}$ and thus the L-function of E, showing that it has a large order zero at $s = 1$.

Ideas of Darmon give an alternative approach to the second part of this argument (showing that the L-function has a large order zero at $s = 1$) and may lead (subject to further development of Gross-Zagier formulas in the function field case) to an alternative approach to the first part of the argument (the proof of BSD). Darmon's idea is quite general and leads to the construction of many elliptic curves over function fields of large rank (more precisely, provably of large analytic rank and conjecturally of large algebraic rank.) Here we will treat only the special case of the curve considered in Subsection 4.2 and we refer to his article in this volume [Dar04] for details of the general picture.

Let $q = p^n$ (p any prime), $d = q + 1$, and define $F = \mathbb{F}_q(u)$, $K = \mathbb{F}_{q^2}(u)$, and $H = \mathbb{F}_{q^2}(t)$ where $u = t^d$. Then H is Galois over F with dihedral Galois group. Indeed $\mathrm{Gal}(H/K)$ is cyclic of order d and because $q \equiv -1 \mod d$, the non-trivial element of $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$ acts on $\mathrm{Gal}(H/K)$ by inversion. Let E be the elliptic curve over F defined by the equation

$$y^2 + xy = x^3 - u.$$

Over H, this is the curve discussed in Subsection 4.2.

The L-function of E over H factors into a product of twisted L-functions over K:

$$L(E/H, s) = \prod_{\chi \in \hat{G}} L(E/K, \chi, s)$$

where the product is over the d characters of $G = \mathrm{Gal}(H/K)$. Because H/F is a dihedral extension and E is defined over F, we have the equality $L(E/K, \chi, s) = L(E/K, \chi^{-1}, s)$. Thus the functional equation

$$\begin{aligned} L(E/K, \chi, s) &= W(E/K, \chi,)q^{sd_{E,\chi}} L(E/K, \chi^{-1}, 2 - s) \\ &= W(E/K, \chi)q^{sd_{E,\chi}} L(E/K, \chi, 2 - s) \end{aligned}$$

(where $W(E/K,\chi)$ is the "root number" and $d_{E,\chi}$ is the degree of $L(E/K,\chi,s)$ as a polynomial in q^{-2s}) may force a zero of $L(E/K,\chi,s)$ at the critical point $s=1$. This is indeed what happens: A careful analysis shows that $W(E/K,\chi)$ is $+1$ if χ is trivial or of order exactly 6 and it is -1 in all other cases. Along the way, one also finds that $d_{E,\chi}$ is 0 if χ is trivial or of order exactly 6 and is 1 in all other cases. Thus $L(E/K,\chi,s)$ is equal to 1 if χ is trivial or of order exactly 6 and is equal to $(1-q^{-2s})$ and vanishes to order 1 at $s=1$ if χ is non-trivial and not of order exactly 6. We conclude that $\operatorname{ord}_{s=1} L(E/H,s)$ is $d-3$ if 6 divides d and $d-1$ if not.

Of course one also wants to compute the L-function of E over $H_0=\mathbb{F}_p(t)$. In this case, the L-function again factors into a product of twists, but the twists are by certain, generally non-abelian, representations of the Galois group of the Galois closure of $\mathbb{F}_p(t)$ over $\mathbb{F}_p(u)$. (The Galois closure is H and the Galois group is the semidirect product of $\operatorname{Gal}(H/K)$ with $\operatorname{Gal}(\mathbb{F}_{q^2}(u)/\mathbb{F}_p(u))$. See [Ulm03, §3] for more on this type of situation.) We will not go into the details, but simply note that in order to compute the L-function $L(E/H_0,s)$ along the lines above, one needs to know the root numbers $W(E/\mathbb{F}_r(u),\chi)$ where $r=p^{o_e}$, o_e is the order of p in $\mathbb{Z}/e\mathbb{Z}$, and e is the order of the character χ. It turns out that each of the twisted L-functions has a simple zero at $s=1$.

This calculation of $L(E/H,s)$ and $L(E/\mathbb{F}_p(t),s)$ seems to be of roughly the same difficulty as the geometric one in [Ulm02] because the "careful analysis" of the root numbers $W(E/K,\chi)$ and $W(E/\mathbb{F}_r(u),\chi)$ is somewhat involved, especially if one wants to include the cases $p=2$ or 3. (I have only checked that the answer agrees with that in [Ulm02] when $p>3$.) Calculation of the root numbers requires knowing the local representations of decompostion groups on the Tate module at places of bad reduction and eventually boils down to analysing some Gauss sums. The Shafarevitch-Tate lemma on supersingular Gauss sums (Lemma 8.3 of [Ulm02]) is a key ingredient.

Regarding the problem of verifying the BSD conjecture for E/H, note that K/F may be viewed as an "imaginary" quadratic extension, and H/K is the ring class extension of conductor $\mathfrak{n}=(0)(\infty)$. Because most of the twisted L-functions $L(E/K,\chi,s)$ vanish simply, we might expect to constuct points in $(E(H)\otimes\mathbb{C})^\chi$ using Heegner points and show that they are non-trivial using a Gross-Zagier formula. But the relevant Gross-Zagier formula here would involve Shimura curve analogs of Drinfeld modular curves (since the extension K/F does not satisfy the usual Heegner hypotheses) and such a formula remains to be proven. Perhaps Darmon's construction will provide some motivation for the brave soul who decides to take on the Gross-Zagier formula in this context! On the other hand, Darmon's paper has examples of curves where Heegner points on standard Drinfeld modular curves should be enough to produce high rank elliptic curves over $\mathbb{F}_p(t)$.

5. Rank bounds

We now return to a general function field $F=\mathbb{F}_q(\mathcal{C})$ and a general non-isotrivial elliptic curve E over F. Recall that the conductor $\mathfrak{n}$ of E is an effective divisor on $\mathcal{C}$ which is supported precisely at the places where E has bad reduction.

It is natural to ask how quickly the ranks of elliptic curves over F can grow in terms of their conductors. As discussed in Section 2, we have the inequality

$$\operatorname{Rank}_{\mathbb{Z}} E(F) \le \operatorname{ord}_{s=1} L(E/F,s).$$

Also, one knows that that $L(E/F,s)$ is a polynomial in q^{-s} of degree $4g-4+\deg \mathfrak{n}$ where g is the genus of $\mathcal{C}$. (This comes from Grothendieck's cohomological expression for the L-function and the Grothendieck-Ogg-Shafarevitch Euler characteristic formula.) Thus we have a bound

$$\text{Rank}_{\mathbb{Z}}\, E(F) \leq \text{ord}_{s=1}\, L(E/F,s) \leq 4g-4+\deg \mathfrak{n}. \tag{5.1}$$

This bound is geometric in the sense that it does not involve the size of the finite field $\mathbb{F}_q$; the same bound holds for $\text{Rank}_{\mathbb{Z}}\, E(\overline{\mathbb{F}}_q(\mathcal{C}))$. On the other hand, as we have seen above, the rank can change significantly after extension of $\mathbb{F}_q$. It is thus natural to ask for a more arithmetic bound, i.e., one which is sensitive to q.

Such a bound was proven by Brumer [Bru92], using Weil's "explicit formula" technique, along the lines of Mestre's bound for the rank of an elliptic curve over $\mathbb{Q}$. Brumer's result is

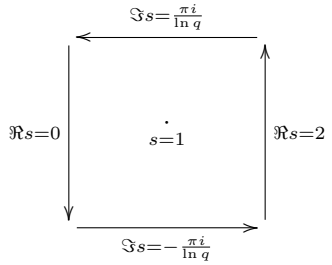
$$\text{Rank}_{\mathbb{Z}}\, E(F) \leq \text{ord}_{s=1}\, L(E/F,s) \leq \frac{4g-4+\deg(\mathfrak{n})}{2\log_q \deg(\mathfrak{n})} + C\frac{\deg(\mathfrak{n})}{(\log_q \deg(\mathfrak{n}))^2} \tag{5.2}$$

Note that this bound is visibly sensitive to q and is an improvement on the geometric bound when $\deg \mathfrak{n}$ is large compared to q.

Here is a sketch of Brumer's proof: let $\Lambda(s) = q^{Ds/2}L(E/F,s)$ where $D = 4g-4+\deg \mathfrak{n}$. Then $\Lambda(s)$ is a Laurent polynomial in $q^{-s/2}$ and so is periodic in s with period $4\pi i/\ln q$; moreover, we have the functional equation $\Lambda(s) = \pm\Lambda(2-s)$. Our task is to estimate the order of vanishing at $s=1$ of Λ or equivalently, the residue at $s=1$ of the logarithmic derivative Λ'/Λ with respect to s. Let us consider the line integral

$$I = \oint \Phi d\log\Lambda = \oint \Phi \frac{\Lambda'}{\Lambda}\, ds$$

where Φ is a suitable test function to be chosen later and the contour of integration is



(Note that $d\log\Lambda$ is periodic with period $2\pi i/\ln q$. Also, we would have to shift the contour slightly if $L(E/F,s)$ has a zero at $1\pm \pi i/\ln q$.) We assume that $\Phi(s)$ is non-negative on the line $\Re s = 1$. By the Riemann hypothesis for $L(E/F,s)$, all the zeroes of $\Lambda(s)$ lie on this line and so

$$\Phi(1)\,\text{ord}_{s=1}\, L(E/F,s) = \Phi(1)\,\text{Res}_{s=1}\, \frac{\Lambda'}{\Lambda} \leq \sum_{\rho} \Phi(\rho) = I$$

where ρ runs over the zeroes of $L(E/F,s)$ inside the contour of integration counted with multiplicities. Now we assume in addition that Φ is a Laurent polynomial in q^{-s} (so periodic with period $2\pi i/\ln q$) and that it satisfies the functional equation

$\Phi(s) = \Phi(2-s)$. Using the functional equation and periodicity of the integrand, the integral I is equal to

$$2\int_{2-\pi i/\ln q}^{2+\pi i/\ln q} \Phi \frac{\Lambda'}{\Lambda}\, ds. \tag{5.3}$$

Now the integration takes place entirely in the region of convergence of the Euler product defining $L(E/F,s)$ and so we can expand the integrand in a series and estimate the terms using the Riemann hypothesis for curves over finite fields. Finally, Brumer makes a clever choice of test function Φ which yields the desired estimate. (More precisely, he considers a sequence of test functions satisfying the hypotheses which when restricted to $\Re s = 1$ converge to the Dirac delta function at $s=1$—up to a change of variable, this is essentially the Fejér kernel—and then chooses Φ to be a suitable element of this sequence.)

Note the strongly analytic character of this proof. For example, it does not use the fact that there is massive cancellation in the series for $L(E/F,s)$ so that the L-function is really a polynomial in q^{-s} of degree D!

Let E_n be the curve of Theorem 4.2.1 with $d = p^n + 1$. Then it turns out that the degree of the conductor of E_n is $p^n + 2$ if $6|d$ and $p^n + 4$ if $6 \nmid d$. One sees immediately that the geometric bound is sharp when q is a power of p^{2n} and the main term of the arithmetic bound is met when $q = p$. Thus both the geometric and arithmetic bounds give excellent control on ranks.

The rest of this paper is devoted to considering various questions which arise naturally by analogy from the existence and sharpness of these two types of bounds, geometric and arithmetic.

6. Ranks over number fields

We now turn to analogous situations, starting with the case where the ground field F is either $\mathbb{Q}$ or a number field. Throughout, we assume that the L-series of elliptic curves have good analytic properties, namely analytic continuation, boundedness in vertical strips, and the standard functional equation. (This is of course now known for elliptic curves over $\mathbb{Q}$ by the work of Wiles and others, but is still open for a general number field F.) We also assume the conjecture of Birch and Swinnerton-Dyer so that "rank" can be taken to mean either analytic rank ($\operatorname{ord}_{s=1} L(E/F,s)$) or algebraic rank ($\operatorname{Rank}_{\mathbb{Z}} E(F)$); alternatively the reader may interpret each question or conjecture involving an unqualified "rank" to be two statements, one about analytic rank, the other about algebraic rank.

The Brumer bound discussed in the last section was modeled on work of Mestre [Mes86], who proved, along lines quite similar to those sketched above, a bound on analytic ranks of the following form:

$$\operatorname{ord}_{s=1} L(E/\mathbb{Q},s) = O\left(\frac{\log N}{\log\log N}\right) \tag{6.1}$$

where E is an elliptic curve over $\mathbb{Q}$ of conductor N. To see the analogy, note that the degree functon on divisors is a kind of logarithm and so $\deg \mathfrak{n}$ is an analogue of $\log N$. To obtain this bound, Mestre assumes the Generalized Riemann Hypothesis for $L(E/\mathbb{Q},s)$ and he actually proves a more general statement about orders of vanishing for L-series of modular forms. Assuming good analytic properties and the generalized Riemann hypothesis, his argument extends readily to elliptic curves

over number fields; in this case N should be replaced with the norm from F to $\mathbb{Q}$ of the conductor of E times the absolute value of the discriminant of F.

There is some evidence that the Mestre bound should be asymptotically sharp. First of all, it gives excellent results for small N. Secondly, in the function field case, the analogous bound is sharp. Moreover, the proof of the bound in the function field case does not use strongly any special features of that situation, such as the fact that the L-function is really a polynomial. Motivated by these facts, I make the following conjecture about the sharpness of the Mestre bound.

Conjecture 6.1. *Fix a number field F and for each positive integer N, define $r_F(N)$ by*

$$r_F(N) = \max\{\mathrm{Rank}_{\mathbb{Z}}(E(F)) | E/F \text{ with } Norm_{F/\mathbb{Q}}(\mathfrak{n}_E) = N\}$$

where the maximum is taken over all elliptic curves E over F with conductor $\mathfrak{n}_E$ satisfying $Norm_{F/\mathbb{Q}}(\mathfrak{n}) = N$; if there are no such curves, we set $r_F(N) = 0$. Then we have

$$\limsup_N \frac{r_F(N)}{\log N/\log\log N} > 0$$

By the generalization of the Mestre bound to number fields, the limit in the conjecture is finite.

If E is an elliptic curve over $\mathbb{Q}$, let $N_{\mathbb{Q}}(E)$ be its conductor and let $N_F(E)$ be the norm from F to $\mathbb{Q}$ of the conductor of E viewed as elliptic curve over F. Then there is a constant C depending only on F such that

$$1 \le \frac{N_{\mathbb{Q}}(E)^{[F:\mathbb{Q}]}}{N_F(E)} \le C$$

for all elliptic curves E over $\mathbb{Q}$. Indeed, if N is an integer, then $\mathrm{Norm}_{F/\mathbb{Q}}(N) = N^{[F:\mathbb{Q}]}$ and since the conductor of E over F is a divisor of $N_{\mathbb{Q}}(E)$ (viewed as an ideal of F), we have $1 \le N_{\mathbb{Q}}(E)^{[F:\mathbb{Q}]}/N_F(E)$. Since $N_{\mathbb{Q}}(F)$ divided by the conductor of E over F is divisible only by ramified primes and these occur with bounded exponents [BK94], there is a constant C such that $N_{\mathbb{Q}}(E)^{[F:\mathbb{Q}]}/N_F(E) \le C$. These inequalities show that a sequence of elliptic curves proving the conjecture over $\mathbb{Q}$ also proves the conjecture for a general number field F.

Finally, let us remark that there are experts who are skeptical about this conjecture. Certain probabilistic models predict that the denominator should be replaced by its square root, i.e., that the correct bound is

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}, s) \stackrel{?}{=} O\left(\left(\frac{\log N}{\log\log N}\right)^{1/2}\right).$$

On the other hand, certain random matrix models suggest that the Mestre bound is sharp. See the list of problems for the workshop on random matrices and L-functions at AIM, May 2001 (`http://aimath.org`) for more on this question.

7. Algebraic rank bounds

The Mestre and Brumer bounds are analytic in both statement and proof. It is interesting to ask whether they can be made more algebraic. For example, the Brumer bound is equivalent to a statement about the possible multiplicity of q as an eigenvalue of Frobenius on $H^1(\mathcal{C}, \mathcal{F})$ for a suitable sheaf $\mathcal{F}$, namely $R^1\pi_*\mathbb{Q}_\ell$

where $\pi : \mathcal{E} \to \mathcal{C}$ is the elliptic surface attached to E/F. It seems that statements like this might admit more algebraic proofs.

There is one situation where such algebraic proofs are available. Namely, consider an elliptic curve E over a number field or a function field F such that E has an F-rational 2-isogeny $\phi : E \to E'$. Then the Selmer group for multiplication by 2 sits in an exact sequence

$$\mathrm{Sel}(\phi) \to \mathrm{Sel}(2) \to \mathrm{Sel}(\check{\phi})$$

where $\check{\phi} : E' \to E$ is the dual isogeny. The orders of the groups $\mathrm{Sel}(\phi)$ and $\mathrm{Sel}(\check{\phi})$ can be crudely and easily estimated in terms of $\omega(N)$, the number of primes dividing the conductor N of E, and a constant depending only on F which involves the size of its class group and unit group. This yields a bound on the rank of the form

$$\mathrm{Rank}_{\mathbb{Z}} E(F) \leq C + 2\omega(N).$$

Note that this bound deserves to be called arithmetic because, for example, in the function field case $F = \mathbb{F}_q(\mathcal{C})$, $\omega(N)$ is sensitive to $\mathbb{F}_q$ since primes dividing N may split after extension of $\mathbb{F}_q$. Note also that it is compatible with the Mestre and Brumer bounds, since $\omega(N) = O(\log N/\log\log N)$ [HW79, p. 355] in the number field case and $\omega(N) = O(\deg N/\log\deg N)$ in the function field case.

It is tempting to guess that a similar bound (i.e., $\mathrm{Rank}\, E(F) = O(\omega(N))$) might be true in general, but there are several reason for skepticism. First of all, the estimation of the Selmer group above breaks down when there is no F-rational 2-isogeny. In this case, one usually passes to an extension field F' where such an isogeny exists. But then the "constant" C involves the units and class groups of F' and these vary with E since F' does. Given our current state of knowledge about the size of class groups, the bounds we obtain are not as good as the Mestre/Brumer bounds. This suggests that what is needed is a way to calculate or at least estimate the size of a Selmer group $\mathrm{Sel}(\ell)$ without passing to an extension where the multiplication by ℓ isogeny factors.

The second reason for skepticism is that such a bound would imply, for example, that there is a universal bound on the ranks of elliptic curves over $\mathbb{Q}$ of prime conductor. Although we have little information on the set of such curves (for example, it is not even known that this set is infinite), the experts seem to be skeptical about the existence of such a bound. One fact is that there is an elliptic curve over $\mathbb{Q}$ with prime conductor and rank 10 [Mes86], and so the constant in a bound of $O(\omega(N))$ would have to be at least 10, which does not seem very plausible. Also, in [BS96], Brumer and Silverman make a conjecture which contradicts an $O(\omega(N))$ bound—their conjecture implies that there should be elliptic curves with conductor divisible only by 2, 3, and one other prime and with arbitrarily large rank. There is no substantial evidence one way or the other for their conjecture, so some caution is necessary.

Lastly, wild ramification may have some role to play. Indeed, for $p = 2$ or 3 the curves of Section 4 have conductor which is divisible only by two primes ($t = 0$ and $t = \infty$) and yet their ranks are unbounded.

Despite all these reasons for skepticism about a bound of the form $\mathrm{Rank}_{\mathbb{Z}} E(F) \leq O(\omega(N))$, it is interesting to ask about the possibility of estimating ranks or Selmer groups directly, i.e., without reducing to isogenies of prime degree. It seems to me that there is some hope of doing this in the function field case, at least in the simplest context of a semistable elliptic curve over the rational function field.

In this case, ideas from étale cohomology (e.g., [Mil80, pp. 211-214]) allow one to express a cohomology group closely related to the Selmer group as a product of local factors where the factors are indexed by the places of bad reduction of the elliptic curve.

Another approach over function fields is via p-descent. In this case, there is always a rational p-isogeny, namely Frobenius, but, in contrast to an ℓ-descent, the places of (good) supersingular reduction play a role more like places of bad reduction for ℓ-descents. This means that the output of a p-descent does not *a priori* give a bound for the rank purely in terms of the conductor and invariants of the ground field. More work will be required here to yield interesting results. See [Vol90] and [Ulm91] for foundational work on p-descents in characteristic p.

8. Arithmetic and geometric bounds I: cyclotomic fields

We now turn to some questions motivated by the existence of a *pair* of bounds, one geometric, one arithmetic. Let $\mathbb{Q}_n \subset \mathbb{Q}(\mu_{p^{n+1}})$ be the subfield with $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ equal to $\mathbb{Z}/p^n\mathbb{Z}$ and set $\mathbb{Q}^{p\text{-cyc}} = \cup_{n\geq 0}\mathbb{Q}_n$. This is the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. As is well-known, the extension $\mathbb{Q}^{p\text{-cyc}}/\mathbb{Q}$ may be thought of as an analogue of the extension $\overline{\mathbb{F}}_q(\mathcal{C})/\mathbb{F}_q(\mathcal{C})$, and this analogy, noted by Weil [Wei79, p. 298], was developed by Iwasawa into a very fruitful branch of modern number theory. There has also been some traffic in the other direction, e.g., [MW83]. Let us consider the rank bounds of Section 5 in this light.

Mazur [Maz72], in analogy with Iwasawa's work, asked about the behavior of the Mordell-Weil and Tate-Shafarevitch groups of an elliptic curve (or abelian variety) defined over $\mathbb{Q}$ as one ascends the cyclotomic tower. For example, he conjectured that if E is an elliptic curve with good, ordinary reduction at p, then $E(\mathbb{Q}^{p\text{-cyc}})$ should be finitely generated. This turns out to be equivalent to the assertion that $\mathrm{Rank}_{\mathbb{Z}}\, E(\mathbb{Q}_n)$ is bounded as $n \to \infty$, i.e., it stabilizes at some finite n.

Today, by work of Rohrlich [Roh84], Kato [Kat00], Rubin [Rub98], and others, this is known to hold even without the assumption that E has ordinary reduction at p. (But we do continue to assume that E has good reduction, i.e., that p does not divide the conductor of E.)

Rohrlich proved the analytic version of this assertion, namely that the analytic rank $\mathrm{ord}_{s=1}\, L(E/\mathbb{Q}_n, s)$ is bounded as $n \to \infty$. (Rohrlich's paper is actually about the L-functions of modular forms, but by the work of Wiles and his school, it applies to elliptic curves.) Note that

$$L(E/\mathbb{Q}_n, s) = \prod_{\chi} L(E/\mathbb{Q}, \chi, s)$$

where χ ranges over characters of $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. So Rohrlich's theorem is that for any finite order character χ of $\mathrm{Gal}(\mathbb{Q}^{p\text{-cyc}}/\mathbb{Q})$ of sufficiently high conductor, $L(E/\mathbb{Q}, \chi, 1) \neq 0$. He proves this by considering the average of special values for conjugate characters $L(E/\mathbb{Q}, \chi^\sigma, 1)$ as σ varies over a suitable Galois group and showing that this average tends to 1 as the conductor of χ goes to infinity. Since $L(E/\mathbb{Q}, \chi^\sigma, 1) \neq 0$ if and only if $L(E/\mathbb{Q}, \chi, 1) \neq 0$, this implies $L(E/\mathbb{Q}, \chi, 1) \neq 0$.

Work of Rubin, Rubin-Wiles, and Coates-Wiles in the CM case and work of Kato in the non-CM case (see [Rub98, §8.1] and the references there) allows us to translate this analytic result into an algebraic result. Namely, these authors show that $L(E/\mathbb{Q}, \chi, 1) \neq 0$ implies that $(E(\mathbb{Q}_n) \otimes \mathbb{C})^\chi = 0$ where χ is a character of

$\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$. This, together with Rohrlich's theorem implies that the rank of $E(\mathbb{Q}_n)$ stabilizes for large n.

Thus for an elliptic curve E over $\mathbb{Q}$ with good reduction at p, $\mathrm{Rank}_{\mathbb{Z}} E(\mathbb{Q}^{p\text{-cyc}})$ is finite and we may ask for a bound. Since there are only finitely many E of a given conductor, there is a bound purely in terms of p and N. The question then is what is the shape of this bound. For a fixed p, the results of Section 5 might lead one to guess that $\mathrm{Rank}_{\mathbb{Z}} E(\mathbb{Q}^{p\text{-cyc}}) = O(\log N)$ (where the constant of course depends on p), but this is nothing more than a guess.

Rohrlich mentions briefly the issue of an effective bound for the smallest q such that $L(E/\mathbb{Q},\chi,1) \neq 0$ for all χ of conductor $p^n > q$. He obtains a bound of the form $q = CN^{170}$. Combined with the Mestre bound 6.1, this implies that $\mathrm{ord}_{s=1} L(E/\mathbb{Q}_n, s)$ is bounded for all n by a polynomial in N (which of course depends on p). This bound has recently been improved by Chinta [Chi02]. He points out that his Theorem 3 (or his Proposition 1 combined with Rohrlich's arguments) implies the following: If p is an odd prime where E has good reduction, then for every $\epsilon > 0$ there exist constants C_ϵ and e_ϵ such that

$$\mathrm{ord}_{s=1} L(E/\mathbb{Q}_n, s) \leq C_\epsilon p^{e_\epsilon} N^{1+\epsilon}$$

for all n. The exponent e_ϵ may be taken to be linear in $1/\epsilon$. This is of course a weaker bound than the guess $O(\log N)$; it might be interesting to try to establish the stronger bound on average. We remark that Chinta also shows the remarkable result that there exists an n_0 depending on E but *independent of* p such that $L(E/\mathbb{Q},\chi,1) \neq 0$ for all χ of conductor p^n, $n > n_0$.

9. Arithmetic and geometric bounds II: function fields over number fields

Let K be a number field and $\mathcal{C}$ a smooth, proper, geometrically connected curve over K. Let E be a non-isotrivial elliptic curve over $F = K(\mathcal{C})$ (i.e., $j(E) \notin K$). It is known that $E(F)$ is finitely generated [Nér52].

This finite generation, as well as a bound on the rank, can be obtained by considering the elliptic surface $\pi : \mathcal{E} \to \mathcal{C}$ attached to E/F. As in Section 2, $\mathcal{E}$ is the unique elliptic surface over $\mathcal{C}$ which is smooth and proper over K, with π flat, relatively minimal, and with generic fiber E/F. There is a close conection between the Mordell-Weil group $E(F)$ and the Néron-Severi group $NS(\mathcal{E})$. Using this, the cycle class map $NS(\mathcal{E}) \to H^2(\mathcal{E} \times \overline{K}, \mathbb{Q}_\ell)$ and an Euler characteristic formula, one obtains the same bound as in the positive characteristic case, namely:

$$\mathrm{Rank}_{\mathbb{Z}} E(F) \leq 4g - 4 + \deg \mathfrak{n} \tag{9.1}$$

where g is the genus of $\mathcal{C}$ and $\mathfrak{n}$ is the conductor of E.

This bound is geometric in that the number field K does not appear on the right hand side. In particular, the bound continues to hold if we replace K by $\overline{K}$:

$$\mathrm{Rank}_{\mathbb{Z}} E(\overline{K}(\mathcal{C})) \leq 4g - 4 + \deg \mathfrak{n}.$$

Using Hodge theory, this bound can be improved to $4g - 4 + \deg \mathfrak{n} - 2p_g$ where p_g is the geometric genus of $\mathcal{E}$, but this is again a geometric bound. It is reasonable to ask if there is a more arithmetic bound, improving 9.1.

There is some evidence that such a bound exists. Silverman [Sil00] considered the following situation: Let E be an elliptic curve over $F = K(t)$ and define $N^*(E)$ to be the degree of the part of the conductor of E which is prime to 0 and ∞.

Alternatively, $N^*(E)$ is the sum of the number of points $t \in \overline{K}^\times$ where E has multiplicative reduction and twice the number of points $t \in \overline{K}^\times$ where E has additive reduction. Clearly $0 \leq \deg \mathfrak{n} - N^*(E) \leq 4$ and so the bound 9.1 gives $\mathrm{Rank}_{\mathbb{Z}} E(F) \leq N^*(E)$.

Now define E_n as the elliptic curve defined by the equation of E with t replaced by t^n. This is the base change of E by the the field homomorphism $K(t) \to K(t)$, $t \mapsto t^n$. Clearly $N^*(E_n) = nN^*(E)$ and so the geometric bound 9.1 gives $\mathrm{Rank}_{\mathbb{Z}} E_n(F) \leq nN^*(E)$.

Assuming the Tate conjecture (namely the equality $-\mathrm{ord}_{s=2} L(H^2(\mathcal{E}), s) = \mathrm{Rank}_{\mathbb{Z}} NS(\mathcal{E})$), Silverman proves by an analytic method that

$$\mathrm{Rank}_{\mathbb{Z}} E_n(F) \leq d_K(n) N^*(E)$$

where

$$d_K(n) = \sum_{d|n} \frac{\phi(d)}{[K(\mu_d) : K]}.$$

So, when $\mu_d \subset K$, $d_K(n) = n$ whereas if $K \cap \mathbb{Q}(\mu_n) = \mathbb{Q}$, then $d_K(n)$ is the number of divisors of n. Thus Silverman's theorem gives an arithmetic bound for ranks of a very special class of elliptic curves over function fields over number fields. I believe that there should be a much more general theorem in this direction.

There has been recent further work in this direction. Namely, Silverman [Sil03] has proven an interesting arithmetic bound on ranks of elliptic curves over unramified, abelian towers, assuming the Tate conjecture. In the special case where the base curve is itself elliptic and the tower is defined by the multiplication by n isogenies, he obtains a very strong bound, stronger than what is conjectured below. (See his Theorem 2.)

Silverman also formulates a beautiful and precise conjecture along the lines suggested above. Namely, he conjectures that there is an absolute constant C such that for every non-isotrivial elliptic curve over $F = K(\mathcal{C})$ with conductor $\mathfrak{n}$,

$$\mathrm{Rank}\, E(F) \overset{?}{\leq} C \frac{4g - 4 + \deg \mathfrak{n}}{\log \deg \mathfrak{n}} \log |2\mathrm{Disc}(K/\mathbb{Q})|.$$

This conjecture is yet another instance of the fruitful interplay between function fields and number fields.

References

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

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

[BD01] ———, *The p-adic L-functions of modular elliptic curves*, Mathematics unlimited—2001 and beyond, Springer, Berlin, 2001, pp. 109–170.

[Bir04] B. Birch, *Heegner points: the beginnings*, Heegner points and Rankin L-series (MSRI Publications 48), Cambridge Univ. Press, New York, 2004, pp. ???–???

[BK94] A. Brumer and K. Kramer, *The conductor of an abelian variety*, Compositio Math. **92** (1994), 227–248.

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

[Bru92] A. Brumer, *The average rank of elliptic curves. I*, Invent. Math. **109** (1992), 445–472.

[BS96] A. Brumer and J. H. Silverman, *The number of elliptic curves over* $\mathbf{Q}$ *with conductor* N, Manuscripta Math. **91** (1996), 95–102.

[Chi02] G. Chinta, *Analytic ranks of elliptic curves over cyclotomic fields*, J. Reine Angew. Math. **544** (2002), 13–24.

[Dar04] H. Darmon, *Heegner points and elliptic curves of large rank over function fields*, Heegner points and Rankin L-series (MSRI Publications 48), Cambridge Univ. Press, New York, 2004, pp. ???–???

[Del73] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 501–597. Lecture Notes in Math., Vol. 349.

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

[Dri74] V. G. Drinfel′d, *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.

[Gro87] B. H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187.

[GvdPRG97] E.-U. Gekeler, M. van der Put, M. Reversat, and J. Van Geel (eds.), *Drinfeld modules, modular schemes and applications*, River Edge, NJ, World Scientific Publishing Co. Inc., 1997.

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

[HLW80] G. Harder, W. Li, and J. R. Weisinger, *Dimensions of spaces of cusp forms over function fields*, J. Reine Angew. Math. **319** (1980), 73–103.

[HW79] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979.

[JL70] H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Springer-Verlag, Berlin, 1970, Lecture Notes in Mathematics, Vol. 114.

[Kat00] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, preprint, 2000.

[KM85] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

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

[Lau96] G. Laumon, *Cohomology of Drinfeld modular varieties. Part I*, Cambridge Studies in Advanced Mathematics, vol. 41, Cambridge University Press, Cambridge, 1996, Geometry, counting of points and local harmonic analysis.

[Lev68] M. Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456–462.

[Li84] W. Li, *A criterion on automorphic forms for* GL_1 *and* GL_2 *over global fields*, Seminar on number theory, Paris 1982–83 (Paris, 1982/1983), Progr. Math., vol. 51, Birkhäuser Boston, Boston, MA, 1984, pp. 161–172.

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

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.

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

[Mes86] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), 517–533, See also the addendum available at `http://www.jmilne.org/math/`.

[Mil80] ———, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[MW83] B. Mazur and A. Wiles, *Analogies between function fields and number fields*, Amer. J. Math. **105** (1983), 507–521.

[Nér52] A. Néron, *Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166.

[Pál00] A. Pál, *Drinfeld modular curves, Heegner points and interpolation of special values*, Ph.D. thesis, Columbia University, 2000.

[Pap02] M. Papikian, *On the degree of modular parametrizations over function fields*, J. Number Theory **97** (2002), no. 2, 317–349.

[Roh84] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), 409–423.

[RS01] K. Rubin and A. Silverberg, *Rank frequencies for quadratic twists of elliptic curves*, Experiment. Math. **10** (2001), 559–569.

[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).

[Rub98] K. Rubin, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), Cambridge Univ. Press, Cambridge, 1998, pp. 351–367.

[Sch84] P. Schneider, *Rigid-analytic L-transforms*, Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983), Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 216–230.

[Ser80] J.-P. Serre, *Trees*, Springer-Verlag, Berlin, 1980, Translated from the French by John Stillwell.

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

[Sil00] J. H. Silverman, *A bound for the Mordell-Weil rank of an elliptic surface after a cyclic base extension*, J. Algebraic Geom. **9** (2000), 301–308.

[Sil03] ———, *The rank of elliptic surfaces in unramified abelian towers*, preprint, 2003.

[Tat66a] J. T. Tate, *Endomorphisms of abelian varieties over finite fields*, Invent. Math. **2** (1966), 134–144.

[Tat66b] ———, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Exp. No. 306, Vol. 9, Soc. Math. France, Paris, 1995, pp. 415–440.

[Tat72] ———, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

[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.

[Tei91] J. T. Teitelbaum, *The Poisson kernel for Drinfel′d modular curves*, J. Amer. Math. Soc. **4** (1991), 491–511.

[Tha02] D. S. Thakur, *Elliptic curves in function field arithmetic*, Currents trends in number theory (Allahabad, 2000), Hindustan Book Agency, New Delhi, 2002, pp. 215–238.

[TR92] K.-S. Tan and D. Rockmore, *Computation of L-series for elliptic curves over function fields*, J. Reine Angew. Math. **424** (1992), 107–135.

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

[Ulma] D. L. Ulmer, *Automorphic forms on* GL_2 *over function fields and Gross-Zagier theorems*, In preparation.

[Ulmb] ———, *Survey of elliptic curves over function fields*, In preparation.

[Ulm91] ———, *p-descent in characteristic p*, Duke Math. J. **62** (1991), 237–265.

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

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

[vdPR97] M. van der Put and M. Reversat, *Automorphic forms and Drinfeld's reciprocity law*, Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996), World Sci. Publishing, River Edge, NJ, 1997, pp. 188–223.

[vdPT97] M. van der Put and J. Top, *Algebraic compactification and modular interpretation*, Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996), World Sci. Publishing, River Edge, NJ, 1997, pp. 141–166.

[Vol90] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990), 247–258.

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

[Wei79] ———, *Scientific works. Collected papers. Vol. I (1926–1951)*, Springer-Verlag, New York, 1979.

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

[Zha01] S.-W. Zhang, *Gross-Zagier formula for* GL_2, Asian J. Math. **5** (2001), 183–290.

Department of Mathematics, University of Arizona, Tucson, AZ 85721
E-mail address: ulmer@math.arizona.edu