L-FUNCTIONS WITH LARGE ANALYTIC RANK AND ABELIAN VARIETIES WITH LARGE ALGEBRAIC RANK OVER FUNCTION FIELDS

DOUGLAS ULMER

1. Introduction

The goal of this paper is to explain how a simple but apparently new fact of linear algebra together with the cohomological interpretation of L-functions allows one to produce many examples of L-functions over function fields vanishing to high order at the center point of their functional equation. Conjectures of Birch and Swinnerton-Dyer, Bloch, and Beilinson relate the orders of vanishing of some of these L-functions to Mordell-Weil groups and other groups of algebraic cycles. For certain abelian varieties of high analytic rank, we are also able to prove the conjecture of Birch and Swinnerton-Dyer thus establishing the existence of large Mordell-Weil groups in those cases.

In the rest of this section we state the main results of the paper.

1.1. **Theorem.** *For every prime number p, every positive integer g, and every integer R, there exist absolutely simple, non-isotrivial abelian varieties J of dimension g over $\mathbb{F}_p(t)$ such that $\operatorname{ord}_{s=1} L(J/\mathbb{F}_p(t), s) \geq R$. For all p and g there are examples of such J for which the conjecture of Birch and Swinnerton-Dyer holds and so the rank of the finitely generated abelian group $J(\mathbb{F}_p(t))$ is at least R.*

The precise meaning of non-isotrivial and a stronger property enjoyed by J are explained in Section 5.3.

Our examples are completely explicit: We produce hyperelliptic curves whose Jacobians have the properties asserted in the theorem. For example, if p does not divide $(2g+2)(2g+1)$ then the Jacobian of the curve with affine equation $y^2 = x^{2g+2} + x^{2g+1} + t^{p^n+1}$ over $\mathbb{F}_p(t)$ is absolutely simple, non-isotrivial, and has Mordell-Weil group of rank $\geq p^n/2n$ over $\mathbb{F}_p(t)$. This curve and similar examples for other pairs (p, g) meet asymptotic upper bounds on ranks explained in Section 11.

We can also produce high analytic ranks for L-functions of cohomology groups of higher degree:

1.2. **Theorem.** *For every prime number $p > 2$, every odd positive integer k, and every integer R, there exist infinitely many integers g such that there exist absolutely simple, non-isotrivial abelian varieties J of dimension g over $\mathbb{F}_p(t)$ with*

$$\operatorname{ord}_{s=(k+1)/2} L(H^k(J)_{prim}, s) \geq R.$$

Date: July 17, 2006.

2000 *Mathematics Subject Classification.* Primary 11G40, 14G05; Secondary 11G05, 11G10, 11G30, 14G10, 14G25, 14K12, 14K15.

This paper is based upon work partially supported by the National Science Foundation under Grant No. DMS 0400877.

Here $L(H^k(J)_{prim}, s)$ is the L-function associated to the primitive part of the k-th ℓ-adic cohomology group of J. See Section 8.1 for details. A conjecture (or rather "recurring fantasy") of Bloch [Blo84] predicts that the order of vanishing appearing in the theorem is equal to the rank of a group of homologically trivial cycles of codimension k on J modulo rational equivalence. Producing the predicted cycles, even in specific examples, looks like an interesting but difficult problem.

We also obtain new results on elliptic curves. In [Ulm02] large ranks were obtained by considering a specific elliptic curve over various rational extensions of the base field. The following result shows that this is a very general phenomenon.

1.3. **Theorem.** *Let $\mathbb{F}_q$ be the field with q elements, q a power of p, and let E be any elliptic curve defined over $F = \mathbb{F}_q(v)$ such that the j-invariant of E does not lie in $\mathbb{F}_q$. Then there exists a power r of q such that for every integer R there are extensions of F of the form $K = \mathbb{F}_r(t)$ such that $\operatorname{ord}_{s=1} L(E/K, s) \geq R$.*

Regarding isotrivial elliptic curves, our method also gives a new proof of a result of Tate and Shafarevitch:

1.4. **Theorem.** *Let E_0 be a supersingular elliptic curve over $\mathbb{F}_p$ and let $E = E_0 \times_{\operatorname{Spec} \mathbb{F}_p} \operatorname{Spec} \mathbb{F}_p(t)$. Then for every integer R there exist quadratic twists E' of E over $\mathbb{F}_p(t)$ such that the rank of $E'(\mathbb{F}_p(t))$ is $\geq R$.*

1.5. The key result of linear algebra and its implications for L-functions already appeared in our previous work [Ulm05] on non-vanishing of L-functions. (In that context, it was something of a technicality, but here it returns in a more appealing guise.) For the convenience of the reader, we give a brief review of the linear algebra from a somewhat different point of view and a more general application to L-functions in Sections 2 through 4. We then prove the results stated above in Sections 5 through 10. In Section 11 we discuss an upper bound on ranks in terms of conductors and then note that the results of Section 7 show that the main term of the bound is sharp.

Our analytic rank results are all based on an understanding of the behavior of L-functions in towers of function fields, the simplest and most important example being the tower $\mathbb{F}_q(t^{1/d})$ where d runs over integers prime to p, the characteristic of $\mathbb{F}_q$. That ranks of L-functions should often be unbounded in towers became apparent while considering a question of Ellenberg on towers over finite fields versus towers over number fields. In a companion [Ulmer] to this paper, we explain Ellenberg's question and ultimately answer it in the negative by giving several examples of abelian varieties which have ranks over $\mathbb{F}_q(t^{1/d})$ bounded independently of d.

1.6. It is a pleasure to thank Jordan Ellenberg for his stimulating questions about ranks of elliptic curves as well as Brian Conrey, Bill McCallum, Dinesh Thakur, and especially Bjorn Poonen for their help.

2. Linear algebra

2.1. Proposition. *Let V be a finite-dimensional vector space with subspaces W_i indexed by $i \in \mathbb{Z}/a\mathbb{Z}$ such that $V = \oplus_{i \in \mathbb{Z}/a\mathbb{Z}} W_i$. Let $\phi : V \to V$ be an invertible linear transformation such that $\phi(W_i) = W_{i+1}$ for all $i \in \mathbb{Z}/a\mathbb{Z}$. Suppose that V admits a non-degenerate, ϕ-invariant bilinear form $\langle , \rangle$ which is either symmetric (in which case we set $\epsilon = 1$) or skew-symmetric (in which case $\epsilon = -1$). Suppose that a is even and $\langle , \rangle$ induces an isomorphism $W_{a/2} \cong W_0^*$ (the dual vector space*

of W_0). Suppose also that $N = \dim W_0$ is odd. Then the polynomial $1-\epsilon T^a$ divides $\det(1-\phi T|V)$.

The proof of Proposition 2.1 is given in Subsections 2.2 through 2.5 below.

2.2. Lemma. *Let V be a finite-dimensional vector space with subspaces W_i indexed by $i \in \mathbb{Z}/a\mathbb{Z}$ such that $V = \oplus_{i\in\mathbb{Z}/a\mathbb{Z}} W_i$. Let $\phi : V \to V$ be a linear transformation such that $\phi(W_i) \subset W_{i+1}$ for all $i \in \mathbb{Z}/a\mathbb{Z}$. Then*

$$\det(1-\phi T|V) = \det(1-\phi^a T^a|W_0) \tag{2.2.1}$$

Proof. We argue by induction on the dimension of W_0. If $W_0 = \{0\}$ then ϕ is nilpotent and both sides of 2.2.1 are 1. We may assume that the ground field is algebraically closed and so if $W_0 \neq \{0\}$ then ϕ^a has an eigenvector $v \in W_0$ with eigenvalue λ. Let W_i' be the span of $\phi^i v$ and $V' = \oplus W_i'$. A simple computation shows that

$$\det(1-\phi T|V') = 1-\lambda T^a = \det(1-\phi^a T^a|W_0').$$

Since characteristic polynomials are multiplicative in short exact sequences, we may replace V with V/V' and W_i with W_i/W_i' and finish by induction on the dimension of W_0. □

2.3. Lemma. *Under the hypotheses of Proposition 2.1, if λ is an eigenvalue of ϕ^a on W_0 then so is λ^{-1}.*

Proof. First we note that since $\phi^a : W_0 \to W_0$ factors as

$$W_0 \xrightarrow{\phi^{a/2}} W_{a/2} \xrightarrow{\phi^a} W_{a/2} \xrightarrow{\phi^{-a/2}} W_0$$

the eigenvalues of ϕ^a on W_0 are the same as the eigenvalues of ϕ^a on $W_{a/2}$. On the other hand, the pairing $\langle , \rangle$ induces a duality between W_0 and $W_{a/2}$ for which ϕ^a is orthogonal (i.e., for all $v \in W_0$, $w \in W_{a/2}$, $\langle \phi^a v, w\rangle = \langle v, \phi^{-a} w\rangle$) and so the eigenvalues of ϕ^a on W_0 are the inverses of the eigenvalues of ϕ^a on $W_{a/2}$. □

2.4. Lemma. *Under the hypotheses of Proposition 2.1, the determinant of $\phi^a : W_0 \to W_0$ is ϵ^N.*

Proof. The pairing $\langle , \rangle$ induces a pairing on $W = \bigwedge^N W_0 \oplus \bigwedge^N W_{a/2}$ which we again denote by $\langle , \rangle$. The sign of this pairing is ϵ^N, i.e., $\langle v, w\rangle = \epsilon^N \langle w, v\rangle$ for all $v, w \in W$. Let $h : W \to W$ be induced by $\bigwedge^N \phi^{a/2}$ and note that h exchanges the subspaces $\bigwedge^N W_0$ and $\bigwedge^N W_{a/2}$. Choose $v \in \bigwedge^N W_0$ and $w \in \bigwedge^N W_{a/2}$ such that $\langle v, w\rangle = 1$. Then

$$\det(\phi^a|W_0) = \langle h^2 v, w\rangle = \langle hv, h^{-1} w\rangle = \langle w, v\rangle = \epsilon^N \langle v, w\rangle = \epsilon^N.$$

□

2.5. Proposition 2.1 is an easy consequence of the lemmas. Indeed, Lemmas 2.3 and 2.4 imply that ϵ is an eigenvalue of ϕ^a on W_0, i.e., that $1-\epsilon T$ divides $\det(1-\phi^a T|W_0)$ and then Lemma 2.2 implies that $1-\epsilon T^a$ divides $\det(1-\phi T|V)$. This completes the proof of Proposition 2.1.

2.6. *Remarks.*

(1) Under the hypotheses of Proposition 2.1, $\epsilon\phi^a$ is the asymmetry (in the sense of [CT02]) of the pairing $(w, w') = \langle w, \phi^{-a/2}w'\rangle$ on W_0. This provides another way to see that $\epsilon\phi^a$ has determinant 1 and is conjugate to its inverse.
(2) With hypotheses as in Proposition 2.1 except with N even, we do not get any consequences for the eigenvalues of ϕ except what is forced by Lemma 2.3. See [Ulm05, 7.1.12] for a more precise version of this remark.

On the other hand, combining Lemma 2.2 with well-known facts about orthogonal transformations yields the following variant, whose proof will be left to the reader.

2.7. Proposition. *Let V be a finite-dimensional vector space with subspaces W_i indexed by $i \in \mathbb{Z}/a\mathbb{Z}$ such that $V = \oplus_{i\in\mathbb{Z}/a\mathbb{Z}} W_i$. Let $\phi : V \to V$ be an invertible linear transformation such that $\phi(W_i) = W_{i+1}$ for all $i \in \mathbb{Z}/a\mathbb{Z}$. Suppose that V admits a ϕ-invariant bilinear form $\langle , \rangle$ such that $\langle , \rangle$ restricted to W_0 is non-degenerate and symmetric. If $N = \dim W_0$ is odd and $\epsilon = \det(\phi^a|W_0)$, then $1-\epsilon T^a$ divides $\det(1-\phi T|V)$. If $N = \dim W_0$ is even and $\det(\phi^a|W_0) = -1$, then $1 - T^{2a}$ divides $\det(1-\phi T|V)$.*

3. Group theory

We review some simple facts about the representation theory of an extension of a finite abelian group by a cyclic group. Fix an algebraically closed field k of characteristic zero. In the applications, k will be $\overline{\mathbb{Q}}_\ell$.

3.1. Let H be a finite abelian group and let $\phi : H \to H$ be an automorphism of H. Let C be the cyclic subgroup of $\mathrm{Aut}(H)$ generated by ϕ and let b denote the order of C. We form the semidirect product $H^+ = H \rtimes C$; explicitly, H^+ is the set of pairs (h, ϕ^i) with $h \in H$ and $i \in \mathbb{Z}/b\mathbb{Z}$ with multiplication $(h, \phi^i)(h', \phi^j) = (h\phi^i(h'), \phi^{i+j})$. For a an integer, let H_a^+ be the subgroup of H^+ generated by H and ϕ^a; it has index $\gcd(a, b)$ in H^+.

3.2. Let $\hat{H}$ denote the group of $k^\times$-valued characters of H. There is a natural action of C on $\hat{H}$: if $\chi \in \hat{H}$ and $h \in H$, then $\chi^\phi(h)$ is defined to be $\chi(\phi(h))$. Given $\chi \in \hat{H}$, let $a = a_\phi$ be the smallest positive integer such that $\chi^{\phi^a} = \chi$. Choose a (b/a)-th root of unity $\zeta \in k$. We extend χ to a character $\tilde{\chi}$ of H_a^+ by setting $\tilde{\chi}(\phi^a) = \zeta$. It is not hard to check that the induced representation $\mathrm{Ind}_{H_a^+}^{H^+} \tilde{\chi}$ is irreducible and up to isomorphism it only depends on ζ and the orbit of the C action on $\hat{H}$ containing χ. We denote this orbit by o and write $\sigma_{o,\zeta}$ for $\mathrm{Ind}_{H_a^+}^{H^+} \tilde{\chi}$. Every irreducible representation of H^+ is isomorphic to a $\sigma_{o,\zeta}$ for a unique pair (o, ζ). (This is a special case of the "method of little groups." See [Ser77, 8.2] for details.)

It is easy to see that the dual of $\sigma_{o,\zeta}$ is $\sigma_{-o,\zeta^{-1}}$ where $-o = \{\chi^{-1} | \chi \in o\}$. In particular, $\sigma_{o,\zeta}$ is self-dual if and only if $o = -o$ and $\zeta \in \{\pm 1\}$. We write σ_o for $\sigma_{o,1}$.

3.3. Let $\Sigma = \mathrm{Ind}_C^{H^+} \mathbf{1}$ where we write $\mathbf{1}$ for the trivial representation of C with coefficients in k. I claim that

$$\Sigma \cong \bigoplus_{o\subset\hat{H}} \sigma_o \tag{3.3.1}$$

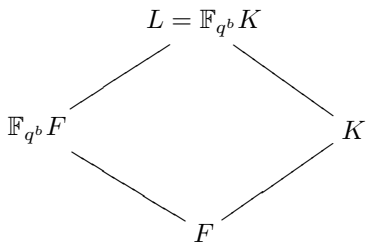
where the sum on the right is over the orbits of C acting on $\hat{H}$. Indeed, for each pair (o, ζ) choose $\chi \in o$ and extend it to $\tilde{\chi}$ as above. Then using standard notation for the inner product on the representation rings of H^+ and C, we have

$$\begin{aligned}\langle \sigma_{o,\zeta}, \Sigma \rangle_{H^+} &= \langle \mathrm{Ind}_{H_a^+}^{H^+} \tilde{\chi}, \mathrm{Ind}_C^{H^+} \mathbf{1} \rangle_{H^+} \\ &= \langle \mathrm{Res}_C^{H^+} \mathrm{Ind}_{H_a^+}^{H^+} \tilde{\chi}, \mathbf{1} \rangle_C\end{aligned}$$

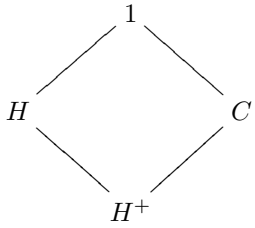
which is the multiplicity of 1 as eigenvalue of ϕ on $\mathrm{Ind}_{H_a^+}^{H^+} \tilde{\chi}$. By Lemma 2.2, this is the same as the multiplicity of 1 as an eigenvalue of $\tilde{\chi}(\phi^a)$, namely 1 if $\zeta = 1$ and 0 if $\zeta \neq 1$. Thus each σ_o appears in Σ exactly once and no $\sigma_{o,\zeta}$ with $\zeta \neq 1$ appears. This establishes the claim.

3.4. Note that $(\chi^\phi)^{-1} = (\chi^{-1})^\phi$ so if $o \subset \hat{H}$ is an orbit of C such that $o = -o$ (a "self-dual orbit") then the involution $\chi \mapsto \chi^{-1}$ of o is either trivial or has no fixed points. The first case happens exactly when o consists entirely of characters of order dividing 2 (in which case we say that o "consists of order 2 characters") and the second case happens when all the characters in o have (the same) order larger than 2 (in which case we say o "consists of higher order characters").

3.5. In the applications of these results, F will be the function field of a curve over a finite field $\mathbb{F}_q$, and K will be a finite extension of F which is "geometrically abelian," i.e., such that the extension $\overline{\mathbb{F}}_q K / \overline{\mathbb{F}}_q F$ is abelian. Then H will be $\mathrm{Gal}(\overline{\mathbb{F}}_q K / \overline{\mathbb{F}}_q F)$ and ϕ will be the action of the geometric (q^{-1}-power) Frobenius on H. It is easy to see that b is then the degree of the algebraic closure of $\mathbb{F}_q$ in the Galois closure L of K/F and we have the diagram of fields



and the corresponding diagram of Galois groups:



3.6. Specializing further, the most interesting applications will be in the case where d is an integer prime to the characteristic of F and $K = F(u^{1/d})$ for some $u \in F$ such that $[K : F] = d$. In this case, $H = \mu_d$ by Kummer theory, $\hat{H} = \mathbb{Z}/d\mathbb{Z}$, and the action of ϕ is just multiplication by q^{-1}. There are at most two orbits o consisting of characters of order 2, namely $o = \{0\}$ and, if d is even, $o = \{d/2\}$. On the other hand there is a plentiful supply of self-dual orbits consisting of higher order characters. Indeed, if d divides $q^n + 1$ for some n, then $q^n \equiv -1 \pmod{d}$

and so every orbit is self-dual. Since $q^{2n} \equiv 1 \pmod{d}$ each orbit has cardinality at most $2n$ and so there are at least $(q^n - 1)/2n$ self-dual orbits consisting of higher order characters.

3.7. The results of this section can be extended, with some additional complications, to the case where H is an arbitrary finite group and the extended results seem to have interesting applications to arithmetic. I hope to report on this elsewhere.

4. Application to L-functions

We now apply the linear algebra result Proposition 2.1 to L-functions. The discussion is a generalization of [Ulm05, 3.2, 4.2, and 7.1].

4.1. Let $\mathcal{C}$ be a smooth, proper, geometrically irreducible curve over the finite field $\mathbb{F}_q$ of characteristic p and let $F = \mathbb{F}_q(\mathcal{C})$ be its field of functions. Choose an algebraic closure F^{alg} of F and let $\overline{F} \subset F^{\text{alg}}$ be the separable closure of F. Let $G_F = \text{Gal}(\overline{F}/F)$ be the absolute Galois group of F. For each place v of F we choose a decomposition group $D_v \subset G_F$ and we let I_v and Fr_v be the corresponding inertia group and geometric Frobenius class. We write $\deg v$ for the degree of v and $q_v = q^{\deg v}$ for the cardinality of the residue field at v. For a finite extension K of F, we denote $\text{Gal}(\overline{F}/K)$ by G_K.

Fix a prime $\ell \neq p$ and let $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$, the field of ℓ-adic numbers. Fix also imbeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$ and a compatible isomorphism $\iota : \overline{\mathbb{Q}}_\ell \to \mathbb{C}$. Whenever a square root of q is needed in $\overline{\mathbb{Q}}_\ell$, we take the one mapping to the positive square root of q in $\mathbb{C}$. Having made this choice, we can define Tate twists by half integers.

4.2. Fix a continuous representation $\rho : G_F \to \text{GL}_r(\overline{\mathbb{Q}}_\ell)$. (As is well-known, ρ factors through $\text{GL}_r(E)$ for some finite extension E of $\mathbb{Q}_\ell$. See [KS99, 9.0.7-9.0.8] for a discussion.) We assume that ρ satisfies the following conditions:

(1) ρ is unramified outside a finite set of places, so that it factors through $\pi_1(U, \overline{\eta})$ for some non-empty open subscheme $j : U \hookrightarrow \mathcal{C}$. (Here $\overline{\eta}$ is the geometric point of $\mathcal{C}$ defined by the fixed embedding $F \hookrightarrow F^{\text{alg}}$.)
(2) ρ is ι-pure of some integer weight w, i.e., for every place v where ρ is unramified, each eigenvalue α of $\rho(Fr_v)$ satisfies $|\iota(\alpha)| = q_v^{w/2}$.
(3) ρ is self-dual of weight w and sign $\text{Sign}(\rho) \in \{\pm 1\}$. In other words, we assume that the space $\overline{\mathbb{Q}}_\ell{}^r$ on which G_F acts via ρ admits a non-degenerate, G_F-equivariant bilinear pairing $\langle , \rangle$ with values in $\overline{\mathbb{Q}}_\ell(-w)$ and with $\langle v, v' \rangle = \text{Sign}(\rho)\langle v', v \rangle$ for all $v, v' \in \overline{\mathbb{Q}}_\ell{}^r$.

For each place v of F we write $\text{Cond}_v \rho$ for the exponent of the Artin conductor of ρ at v. (See [Ser79, Chap. VI] for definitions.) We let $\text{Cond}(\rho) = \sum_v (\text{Cond}_v \rho)[v]$ be the global Artin conductor of ρ, viewed as an effective divisor on $\mathcal{C}$.

4.3. Attached to ρ we have an L-function, defined formally by a product over the places of F:

$$L(\rho, F, T) = \prod_v \det\left(1 - \rho(Fr_v) T^{\deg v} \,\middle|\, (\overline{\mathbb{Q}}_\ell{}^r)^{\rho(I_v)}\right)^{-1}$$

and, for a complex variable s, we define $L(\rho, F, s)$ to be $L(\rho, F, q^{-s})$.

Grothendieck's analysis of L-functions shows that $L(\rho, F, T)$ is a rational function in T and satisfies the functional equation

$$L(\rho, F, T) = \left(q^{\frac{w+1}{2}} T\right)^N L(\rho, F, (q^{w+1}T)^{-1})$$

where

$$N = (2g_{\mathcal{C}} - 2)(\deg \rho) + \deg(\mathrm{Cond}(\rho)).$$

(See, for example, [Mil80], especially Section VI.13.)

If K is a finite extension of F contained in $\overline{F}$, we abbreviate $L(\rho|_{G_K}, K, T)$ to $L(\rho, K, T)$.

4.4. Fix a finite extension K of F which is geometrically abelian in the sense that $\overline{\mathbb{F}}_q K/\overline{\mathbb{F}}_q F$ is Galois. We adopt the definitions and notation of Subsection 3.5, so that the Galois closure of K/F is $L = \mathbb{F}_{q^b} K$, $H = \mathrm{Gal}(\overline{\mathbb{F}}_q K/\overline{\mathbb{F}}_q F)$, $C = \mathrm{Gal}(\mathbb{F}_{q^b} K/K) \cong \mathrm{Gal}(\mathbb{F}_{q^b}/\mathbb{F}_q)$ generated by the q^{-1}-power Frobenius ϕ, and $H^+ = \mathrm{Gal}(L/F) \cong H \rtimes C$.

Continuing with the notations of Section 3 we let $\Sigma = \mathrm{Ind}_C^{H^+} \mathbf{1}$ so that $\Sigma \cong \oplus_{o \subset \hat{H}} \sigma_o$ where the sum is over orbits of C on $\hat{H}$, the dual group of H. We view Σ and the σ_o as representations of G_F via the natural surjection $G_F \to H^+$.

Now consider $L(\rho, K, T) = L(\mathrm{Res}_{G_K}^{G_F} \rho, K, T)$. By standard properties of L-functions (e.g., [Del73, 3.8]) and basic representation theory,

$$\begin{aligned} L(\mathrm{Res}_{G_K}^{G_F} \rho, K, T) &= L(\mathrm{Ind}_{G_K}^{G_F} \mathrm{Res}_{G_K}^{G_F} \rho, F, T) \\ &= L(\rho \otimes \mathrm{Ind}_{G_K}^{G_F} \mathbf{1}, F, T) \\ &= L(\rho \otimes \Sigma, F, T) \\ &= \prod_{o \subset \hat{H}} L(\rho \otimes \sigma_o, F, T) \end{aligned}$$

Our basic result about L-functions says that for a suitable K, many of the factors on the right hand side of the last equation vanish at the center point of their functional equations:

4.5. Theorem. *Let F, ρ, and K be as in 4.1, 4.2, and 4.4 respectively. We keep the notations H, $\hat{H}$, and C of 4.4. Fix an orbit $o \subset \hat{H}$ for the action of C of cardinality $|o|$ which is self-dual ($o = -o$) and consists of characters of higher order ($\chi \in o \implies \chi \neq \chi^{-1}$). Assume that for one (and thus every) $\chi \in o$ the degree of $\mathrm{Cond}(\rho \otimes \chi)$ is odd. Let w be the weight of ρ and let $\epsilon = -\mathrm{Sign}(\rho)$. Then $1 - \epsilon \left(T q^{\frac{w+1}{2}}\right)^{|o|}$ divides the numerator of $L(\rho \otimes \sigma_o, F, T)$.*

Proof. The theorem is a fairly straightforward application of the linear algebra result of Section 2 and the cohomological interpretation of L-functions.

Let $j : U \hookrightarrow \mathcal{C}$ be a non-empty open subscheme over which both ρ and σ_o (and therefore also $\rho \otimes \sigma_o$) are unramified. These three representations give rise to lisse ℓ-adic sheaves on U and we let $\mathcal{F}_\rho$, $\mathcal{F}_{\sigma_o}$, and $\mathcal{F}_{\rho \otimes \sigma_o}$ denote their direct images under j on $\mathcal{C}$. (These are the "middle extension" sheaves on $\mathcal{C}$ attached to the representations.)

Grothendieck's analysis of L-functions and our hypotheses on ρ give a cohomological calculation of $L(\rho\otimes\sigma_o,F,T)$:

$$L(\rho\otimes\sigma_o,F,T)=\frac{\det\left(1-\phi T|H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})\right)}{\det\left(1-\phi T|H^0(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})\right)\det\left(1-\phi T|H^2(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})\right)}$$

where ϕ is the geometric Frobenius in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. By Deligne's theorem on weights, there is no cancellation in this expression and so the numerator of the L-function is precisely

$$\det\left(1-\phi T|H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})\right).$$

The theorem is invariant under twisting and so we may replace ρ with $\rho\otimes\overline{\mathbb{Q}}_\ell(\frac{w+1}{2})$ and assume that ρ is self-dual of weight -1 and sign $\mathrm{Sign}(\rho)$. Since $-o=o$, σ_o is self-dual with sign $+1$ and so $\rho\otimes\sigma_o$ is self-dual with sign $\mathrm{Sign}(\rho)$. Poincaré duality implies that $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})$ is self-dual of weight 0 and sign $\epsilon=-\mathrm{Sign}(\rho)$ as a representation of $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$.

On the other hand, σ_o factors as a representation of $\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_qF)$ into lines and so on $\overline{\mathcal{C}}=\mathcal{C}\times\overline{\mathbb{F}}_q$

$$\mathcal{F}_{\rho\otimes\sigma_o}\cong\bigoplus_{\chi\in o}\mathcal{F}_{\rho\otimes\chi}$$

where $\mathcal{F}_{\rho\otimes\chi}$ is the middle extension sheaf attached to $\rho\otimes\chi$. Thus we have a factorization

$$H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})=\bigoplus_{\chi\in o}H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\chi}).$$

Under the Poincaré duality pairing on $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})$, the subspaces $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\chi})$ and $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\chi^{-1}})$ are dual to one another. Moreover, ϕ preserves the pairing and sends $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\chi})$ to $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\chi^\phi})$.

For any middle extension sheaf $\mathcal{F}_\tau$ on $\mathcal{C}$ associated to an ℓ-adic representation τ of G_F satisfying the first hypothesis of Subsection 4.2, we have

$$\dim H^0(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_\tau)=\dim H^2(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_\tau)$$

both of these being the multiplicity with which the trivial representation appears in τ restricted to $\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_qF)$. It follows that the dimension of $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_\tau)$ has the same parity as the Euler characteristic $(2-2g_{\mathcal{C}})\deg(\tau)-\deg\mathrm{Cond}(\tau)$ and this has the same parity as the degree of $\mathrm{Cond}(\tau)$. Therefore, our hypotheses imply that the dimension of $H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\chi})$ is odd.

Theorem 4.5 now follows easily from Proposition 2.1. Indeed, fix $\chi\in o$ and set $V=H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\sigma_o})$ and $W_i=H^1(\mathcal{C}\times\overline{\mathbb{F}}_q,\mathcal{F}_{\rho\otimes\chi^{\phi^i}})$. The geometric Frobenius ϕ permutes the W_i cyclically. Since o is self-dual consisting of higher order characters, $a=|o|$ is even. Poincaré duality give a non-degenerate pairing on V which induces a duality between W_0 and $W_{a/2}$ and the dimension of W_0 is odd. Thus the hypotheses of Proposition 2.1 are satisfied and so $1-\epsilon T^a$ divides the numerator of the twisted L-function and $1-\epsilon(q^{\frac{w+1}{2}}T)^a$ divides the numerator of the untwisted L-function $L(\rho\otimes\sigma_o,F,T)$. □

4.6. *Remark.* One can formulate a variant of Theorem 4.5 with Proposition 2.7 playing the role of Proposition 2.1. This variant does not seem to lead to unbounded ranks and so we omit it.

We now give a context in which Theorem 4.5 can be applied to deduce unbounded ranks in towers. For the definition of the Swan conductor of a representation, we refer to [Mil80, p. 188].

4.7. Theorem. *Let $F = \mathbb{F}_q(u)$ where q is a power of p and for each d prime to p let $F_d = \mathbb{F}_q(t)$ with $t^d = u$. Let ρ be a representation satisfying the hypotheses of 4.2 which is self dual of weight w and sign -1. Let $\mathfrak{n}$ be the conductor of ρ, let $\mathfrak{n}'$ be the part of $\mathfrak{n}$ which is prime to the places 0 and ∞ of F, and let $\mathrm{Swan}_0(\rho)$ and $\mathrm{Swan}_\infty(\rho)$ be the exponents of the Swan conductors of ρ at 0 and ∞. If $\deg \mathfrak{n}' + \mathrm{Swan}_0(\rho) + \mathrm{Swan}_\infty(\rho)$ is odd then $\mathrm{ord}_{s=(w+1)/2} L(\rho, F_d, s)$ is unbounded as d varies through integers prime to p. More precisely, for d of the form $d = q^n + 1$ we have*

$$\mathrm{ord}_{s=(w+1)/2} L(\rho, F_d, s) \geq d/2n - c$$

and

$$\mathrm{ord}_{s=(w+1)/2} L(\rho, \mathbb{F}_{q^{2n}} F_d, s) \geq d - c$$

where c is a constant independent of n.

Proof. Clearly it suffices to prove the "more precisely" assertion. The extension F_d/F is geometrically abelian with geometric Galois group $H = \mu_d$ and the Frobenius ϕ acts on $\hat{H} = \mathbb{Z}/d\mathbb{Z}$ by multiplication by q^{-1}. For d of the form $q^n + 1$ we have $q^n \equiv -1 \pmod{d}$ and so every orbit o of C (the group generated by ϕ) on $\mathbb{Z}/d\mathbb{Z}$ satisfies $o = -o$, i.e., is self-dual. As pointed out in 3.6, there are at least $(q^n - 1)/2n$ self-dual orbits consisting of characters of higher order.

Now for n sufficiently large and all o such that each $\chi \in o$ has sufficiently large order, the space of invariants of $\rho \otimes \chi$ under the inertia group at 0 or ∞ is trivial. For such n and χ,

$$\deg \mathrm{Cond}(\rho \otimes \chi) = \deg(\mathfrak{n}') + \mathrm{Swan}_0(\rho) + \mathrm{Swan}_\infty(\rho) + 2 \dim \rho$$

which is odd and so Theorem 4.5 implies that for each such orbit o, the L-function $L(\rho \otimes \sigma_{o,f}, F, s)$ vanishes at $s = (w+1)/2$. The number of "bad" orbits is bounded independently of n and so the factorization in Subsection 4.4 shows that $L(\rho, F_d, s)$ has a zero of order at least $d/2n - c$ at $s = (w+1)/2$ for some constant c independent of n.

Extending scalars to $\mathbb{F}_{q^{2n}} F$, each factor $1 - \left(Tq^{\frac{w+1}{2}}\right)^{|o|}$ dividing the L-function becomes $\left(1 - Tq^{2n\frac{w+1}{2}}\right)^{|a|}$ and so the total order of vanishing of $L(\rho, \mathbb{F}_{q^{2n}} F(u^{1/d}), s)$ at $s = (w+1)/2$ is $\geq d - c$ for some constant c independent of n. □

The analytic rank assertions in Theorems 1.1, 1.2, and 1.3 will all be established using the "towers" Theorem 4.7. The Tate-Shafarevitch Theorem 1.4 will follow similarly from an orthogonal ($\mathrm{Sign}(\rho) = 1$) variant of the towers theorem.

We end this section with another example of towers leading to unbounded ranks. The proof is quite similar to that of Theorem 4.7 and thus will be omitted.

4.8. Theorem. *Let E be an elliptic curve over a finite field $\mathbb{F}_q$ of characteristic p and let $F = \mathbb{F}_q(E)$. Let ℓ and ℓ' be (not necessarily distinct) prime numbers $\neq p$ with ℓ' odd. For each $n \geq 1$ let $F_n = \mathbb{F}_q(E)$ and view F_n as an extension of F via pullback under the multiplication-by-ℓ'^n isogeny $\ell'^n : E \to E$. Assume that some power of Frobenius acting on the ℓ'-torsion $E[\ell']$ has eigenvalue -1. Let ρ be an*

ℓ-adic representation satisfying the hypotheses of 4.2 which is self dual of weight w and sign -1. Assume that the degree of the conductor of ρ is odd. Then

$$\operatorname{ord}_{s=(w+1)/2} L(\rho, F_n, s) \geq n.$$

4.9. *Remark.* The hypothesis on E in the theorem is very mild. By assuming more about E we can improve the lower bound in the theorem to $\Omega(\ell'^n)$. We omit the details.

5. Proof of the first part of Theorem 1.1

In this section we will show that there are many examples of curves over $\mathbb{F}_p(t)$ whose Jacobians satisfy the first part of Theorem 1.1, namely they are absolutely irreducible, non-isotrivial, and have large analytic rank. To keep the exposition brief, we have chosen examples where the necessary calculations have already appeared in the literature, but the reader who is so inclined will have no trouble finding many other examples. In the following two sections we will give examples where one can also prove the conjecture of Birch and Swinnerton-Dyer and therefore conclude that algebraic ranks are also large. As will be apparent, the class of examples for which one can currently prove large algebraic ranks is considerably smaller than that for which one can prove large analytic ranks.

5.1. Fix a prime p and a positive integer g. Let $F = \mathbb{F}_p(u)$ and for each d not divisible by p let $F_d = \mathbb{F}_p(t)$ where $u = t^d$. Suppose that C is a curve of genus g smooth and proper over F, let $J = J(C)$ be its Jacobian, and let $V = V_\ell J \otimes \overline{\mathbb{Q}}_\ell$ be the ℓ-adic Tate module of J for some prime $\ell \neq p$. Let $\rho : G_F \to \operatorname{Aut}(V^*) \cong \mathrm{GL}_{2g}(\overline{\mathbb{Q}}_\ell)$ be the natural representation of Galois on $V^* \cong H^1(C \times \overline{F}, \overline{\mathbb{Q}}_\ell)$. The representation ρ satisfies the hypotheses of Section 4.2 with weight $w = 1$ and sign $\operatorname{Sign}(\rho) = -1$.

The L-function of J is of course the same as the L-function of ρ and so if ρ satisfies the hypotheses of the towers Theorem 4.7, then J will have large analytic rank over F_d for suitable d.

5.2. We consider the monodromy groups attached to ρ. Let ρ' be the Tate twist $\rho \otimes \overline{\mathbb{Q}}(1/2)$ which has weight $w = 0$ and let ρ'_0 be the restriction $\rho'|_{\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_p F)}$. Let G^{arith} be the Zariski closure of the image of ρ' and let G^{geom} be the Zariski closure of the image of ρ'_0. The latter group is a (possibly non-connected) semi-simple algebraic group over $\overline{\mathbb{Q}}_\ell$ and, because ρ is self-dual of sign -1, both groups are *a priori* contained in the symplectic group Sp_{2g}. In the examples we will consider below, it will turn out that $G^{\mathrm{arith}} = G^{\mathrm{geom}} = \mathrm{Sp}_{2g}$.

As usual, we say that ρ' is irreducible if V^* has no non-trivial subspaces invariant under $\rho'(G_F)$, or equivalently, under the action of G^{arith}. We say that ρ' is Lie irreducible if the restriction of ρ' to any finite index subgroup of G_F is irreducible. This is equivalent to saying that G^{arith} acts irreducibly and is connected and in this case we also say that G^{arith} acts Lie irreducibly.

5.3. We say that J is non-isotrivial if there does not exist an abelian variety J_0 defined over a finite field $\mathbb{F}_q$ and a finite extension K of $F = \mathbb{F}_p(t)$ containing $\mathbb{F}_q$ such that $J \times_F K \cong J_0 \times_{\mathbb{F}_q} K$.

It is clear that if the monodromy group G^{arith} acts Lie irreducibly, then J is absolutely simple and non-isotrivial. Indeed, if J had a non-trivial isogeny decomposition over a finite separable extension K/F, or if J became isomorphic to a constant abelian variety over a finite separable extension K/F, then ρ' restricted to G_K would be reducible. Since the monodromy group G^{arith} is invariant under finite, purely inseparable extensions similar statements hold for any finite extension K/F.

In fact it is clear that when G^{arith} acts Lie irreducibly (as defined in 5.2), J is not even isogenous to a constant abelian variety over any extension, since G^{arith} is invariant under isogeny. Therefore, for all finite extensions K/F, the $K/\mathbb{F}_q$-trace and $K/\mathbb{F}_q$-image of $J \times_F K$ vanish. (See Conrad [Con06] for a modern treatment of the K/k-trace and K/k-image.)

In light of this discussion, to prove the first part of Theorem 1.1, it will suffice to exhibit curves whose Tate-module representations have $G^{\mathrm{arith}} = \mathrm{Sp}_{2g}$ and which satisfy the conductor hypothesis of the towers Theorem 4.7. We do this in the following two subsections.

5.4. Assume that $p > 2$ and choose a polynomial $f(x) \in \mathbb{F}_p[x]$ of degree $2g$ with distinct roots, one of which is 0. Consider the curve C of genus g smooth and proper over $F = \mathbb{F}_p(u)$ with affine equation

$$y^2 = f(x)(x - u). \tag{5.4.1}$$

Let J be the Jacobian of C and let ρ be the representation of G_F on $H^1(C \times \overline{F}, \overline{\mathbb{Q}}_\ell)$. As we will explain in the rest of this subsection, results of Katz and Sarnak show that ρ satisfies the hypotheses of Theorem 4.7 and has $G^{\mathrm{arith}} = \mathrm{Sp}_{2g}$ and so J is an example satisfying the first part of Theorem 1.1.

In order to apply the results of Katz and Sarnak, we need to make one translation. Namely, they work with a lisse sheaf $\mathcal{F}$ on an open subset of $\mathbb{P}^1$ whose generic stalk is the cohomology with compact supports of the affine curve defined by equation 5.4.1. The smooth, proper model of this curve is obtained by adding exactly one point at infinity, and so the compactly supported H^1 of the open curve is canonically isomorphic to the usual H^1 of the proper curve. This implies that Katz and Sarnak's sheaf $\mathcal{F}$ is the restriction to an open of $\mathbb{P}^1$ of the middle extension sheaf $\mathcal{F}_\rho$ we considered in the proof of Theorem 4.5. The same issue arises in the next subsection, with the same resolution.

Now by [KS99, 10.1.12], ρ is everywhere tame and so $\mathrm{Swan}_0(\rho) = \mathrm{Swan}_\infty(\rho) = 0$. By [KS99, 10.1.9 and 10.1.12], $\mathfrak{n}'$, the prime-to-zero-and-infinity part of the conductor of ρ, is the sum of the zeros of f except 0, each taken with multiplicity one. Thus, $\deg \mathfrak{n}' = 2g - 1$ is odd and so $\deg \mathfrak{n}' + \mathrm{Swan}_0(\rho) + \mathrm{Swan}_\infty(\rho)$ is odd. Thus Theorem 4.7 implies that the analytic rank of J is unbounded in the tower of fields F_d.

By [KS99, 10.1.16], the geometric monodromy group of ρ is the full symplectic group Sp_{2g} and therefore the same is true of the arithmetic monodromy group since $G^{\mathrm{geom}} \subset G^{\mathrm{arith}} \subset \mathrm{Sp}_{2g}$. Thus J is absolutely simple and non-isotrivial.

This completes the proof of the first part of Theorem 1.1 for $p > 2$.

5.5. Now assume that $p = 2$ and consider the curve C of genus g smooth and proper over $\mathbb{F}_p(u)$ with affine equation

$$y^2 + xy = x^{2g+1} + ux.$$

Again let ρ be the representation of G_F on $H^1(C \times \overline{F}, \overline{\mathbb{Q}}_\ell)$. It is easy to see that C has good reduction away from $u = 0$ and ∞ and so ρ is unramified away from those two places. By [KS99, proof of 10.2.2], ρ is tamely ramified at 0 and by the first full paragraph of p. 302 of [KS99] and [Kat90, 7.5.4], the Swan conductor of ρ at ∞ is $2g-1$. Thus $\deg \mathfrak{n}' + \mathrm{Swan}_0(\rho) + \mathrm{Swan}_\infty(\rho) = 2g-1$ is odd and Theorem 4.7 shows that J has unbounded analytic rank in the tower of fields F_d.

By [KS99, 10.2.2], the geometric monodromy group of ρ is Sp_{2g} and so we conclude as in the previous section that J is absolutely simple and non-isotrivial.

This completes the proof of the first part of Theorem 1.1 for $p = 2$.

6. BSD for curves defined by four monomials

In this section we will show that the Jacobians of curves defined by particularly simple equations satisfy the conjecture of Birch and Swinnerton-Dyer. The main tools are a beautiful observation of Shioda [Shi86], already exploited in [Ulm02], that surfaces defined by four monomials are often dominated by Fermat surfaces and so satisfy the Tate conjecture, and well-known connections between the conjectures of Tate and of Birch and Swinnerton-Dyer.

6.1. Let k be a field and consider an irreducible polynomial $g \in k[x_1, x_2, x_3]$ which is the sum of exactly 4 non-zero monomials:

$$g = c_0 x_1^{a_{01}} x_2^{a_{02}} x_3^{a_{03}} + \cdots + c_3 x_1^{a_{31}} x_2^{a_{32}} x_3^{a_{33}} = \sum_{i=0}^{3} c_i \prod_{j=1}^{3} x_j^{a_{ij}}$$

For $i = 0, \ldots, 3$, let $a_{i0} = 1 - \sum_{j=1}^{3} a_{ij}$ and let A be the 4×4 integer matrix (a_{ij}). We say that g *satisfies Shioda's conditions* if two requirements hold. First, we require that the determinant of A be non-zero. Assuming so, A has an inverse in $\mathrm{GL}_4(\mathbb{Q})$ and there is a well-defined smallest positive integer δ such that $B = \delta A^{-1}$ has integer coefficients. Our second requirement is that δ be non-zero in k. Note that $AB = \delta I_4$. Note also that Shioda's conditions are independent of the ordering of the variables x_i and indeed independent of their names, i.e., the condition makes sense for any polynomial ring in three variables. The reader may be surprised to see the 1 in the definition of A rather than $\deg(g)$, but it gives better (less divisible) values of δ.

6.2. Theorem. *Let $F = \mathbb{F}_q(u)$ and let X be a curve smooth and proper over F. Let J be the Jacobian of X. Assume that there exists an irreducible polynomial $g \in \mathbb{F}_q[u, x, y] \subset F[x, y]$ which is the sum of exactly 4 non-zero monomials, which satisfies Shioda's conditions, and which gives rise to the function field $F(X)$ in the following sense: $F(X) \cong \mathrm{Frac}(F[x, y]/(g))$. Then the conjecture of Birch and Swinnerton-Dyer conjecture holds for J, namely* $\mathrm{Rank}\, J(F) = \mathrm{ord}_{s=1} L(J/F, s)$.

6.3. *Remarks.*

(1) It is known that over function fields the weak form of BSD (Rank = ord) is equivalent to the finiteness of Ш and implies the refined conjecture on the leading coefficient of the L-series. We give a few more details about this below.
(2) If X satisfies the hypotheses of the theorem, then it is easy to check that the same is true for $X \times_F \mathbb{F}_r(t)$ where $t^d = u$ for any positive integer d not

divisible by p and for any power r of q. Thus the theorem gives the truth of BSD for curves over towers of function fields.

Proof of Theorem 6.2. Let $\mathcal{Z}$ be the surface in $\mathbb{A}^3$ defined by $g = 0$. Since g is irreducible, $\mathcal{Z}$ is reduced and irreducible and so has a dense open subset smooth over $\mathbb{F}_q$. There is a morphism $\mathcal{Z} \to \mathbb{A}^1$, namely $(u, x, y) \mapsto u$.

Let $\mathcal{X}$ be a model of $\mathcal{Z}$ smooth and proper over $\mathbb{F}_q$. There is a rational map $\mathcal{X} \dashrightarrow \mathbb{P}^1$ and at the expense of blowing up and down we may assume that we have a morphism $\pi : \mathcal{X} \to \mathbb{P}^1$ which is relatively minimal. The generic fiber of π is a regular scheme (since its local rings are local rings of $\mathcal{X}$) of dimension 1 which is proper over F and has the same function field as X does and so it is isomorphic to $X \to \operatorname{Spec} F$.

Let F_δ be the Fermat surface of degree δ. The assumption that g satisfies Shioda's conditions implies that (extending the ground field $\mathbb{F}_q$ if necessary) there is a dominant rational map $\mathcal{F}_\delta \dashrightarrow \mathcal{Z}$ and therefore also a dominant rational map $\mathcal{F}_\delta \dashrightarrow \mathcal{X}$. Indeed, let us use the notation of Subsection 6.1 (setting $u = x_1$, $x = x_2$, and $y = x_3$) and define $\mathcal{Z}'$ as the zero set in $\mathbb{P}^3 \setminus \{x_0 = 0\}$ of the homogeneous Laurent polynomial $\sum_i c_i \prod_j x_j^{a_{ij}}$. Clearly $\mathcal{Z}'$ is birational to $\mathcal{Z}$. If $y_0, \dots, y_3$ are the standard coordinates on F_δ (so that $y_0^\delta + \cdots + y_3^\delta = 0$), then a rational map $F_\delta \dashrightarrow \mathcal{Z}'$ is given by $x_j \mapsto \prod_k d_k y_k^{b_{jk}}$ where $(b_{jk}) = B = \delta A^{-1}$ and $d_0, \dots, d_3 \in \overline{\mathbb{F}}_q$ are solutions to $\prod_j d_j^{a_{ij}} = c_i^{-1}$. This proves that there is a dominant rational map from F_δ to $\mathcal{X}$.

Now the Fermat surface $\mathcal{F}_\delta$ is dominated by a product of Fermat curves [SK79] and therefore so is $\mathcal{X}$. As we will explain presently, this domination by a product of curves is enough to imply the Tate conjecture for $\mathcal{X}$ and the conjecture of Birch and Swinnerton-Dyer for J. (There is a large literature on the connection between these conjectures; the approach that follows is perhaps ahistorical, but has the virtue of being efficient and clear-cut.) That $\mathcal{X}$ is dominated over an extension of $\mathbb{F}_q$ by a product of curves implies [Tat94, §5] that the Tate conjecture (relating the rank of the Néron-Severi group of $\mathcal{X}$ to it zeta function) holds for $\mathcal{X}$ over an extension of $\mathbb{F}_q$ and therefore also over $\mathbb{F}_q$. Consideration of the Kummer sequence in étale cohomology [Tat66, 5.2] implies that the ℓ-primary part of the Brauer group of $\mathcal{X}$ is finite for all $\ell \neq p$. A theorem of Artin generalized by Grothendieck implies that the same holds for the ℓ-primary parts of the Tate-Shafarevitch group of J over F. (This can be extracted from [Gro68, §4]; in the case when X has an F-rational point, it is proven in [Gro68, §4] that $Br(\mathcal{X}) = Ш(J/F)$.) Finally, a recent paper of Kato and Trihan [KT03] proves that the full conjecture of Birch and Swinnerton-Dyer holds for J over F as soon as one ℓ-primary part of $Ш$ is finite. (In the applications below, we will only need the theorem in cases where X is a curve with an F-rational point and in this case, the reference to [KT03] may be replaced with the simpler [Mil86, III.9.7].) □

6.4. *Remark.* The above proof of the Tate conjecture for $\mathcal{X}$ ultimately comes down to two facts: Tate's theorem on isogenies of abelian varieties over finite fields and the fact that $\mathcal{X}$ is dominated by a product of curves, Fermat curves as it turns out. It is not difficult to produce examples of surfaces not defined by four monomials which are dominated by products of curves. But the four monomials property has the charm that it is obviously preserved in towers, i.e., when u is replaced by t^d. It

looks like an interesting problem to give examples of towers of surfaces dominated by products of curves beyond the four monomial case.

7. End of the proof of Theorem 1.1

In order to finish the proof of Theorem 1.1 we have to exhibit for every prime p and every integer $g > 0$ a curve X smooth and proper over $F = \mathbb{F}_p(u)$ of genus g with three properties: (i) the Galois representation ρ on $H^1(X \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ should satisfy the hypotheses of the towers Theorem 4.7 (so that we have large analytic ranks); (ii) the monodromy group of ρ should be Lie-irreducible (so that $J = J(X)$ will be absolutely simple and non-isotrivial, cf. Subsection 5.3); and (iii) X should satisfy the hypotheses of the "four monomials" Theorem 6.2 (so that the conjecture of Birch and Swinnerton-Dyer holds for J). In this section we will exhibit curves with these properties.

7.1. There are many examples of such curves. The ones we have chosen here allow for a fairly unified treatment and, as will be explained in Section 11, they have good properties with respect to rank bounds. Here are the curves we will study:

$$p > 2 \quad p \not| (2g+2)(2g+1) \qquad y^2 = x^{2g+2} + x^{2g+1} + u \tag{7.1.1}$$

$$p > 2 \quad p|(2g+2) \qquad y^2 = x^{2g+2} + x^{2g+1} + ux \tag{7.1.2}$$

$$p > 2 \quad p|(2g+1) \qquad y^2 = x^{2g+1} + x^{2g} + ux \tag{7.1.3}$$

$$p = 2 \qquad y^2 + xy = x^{2g+1} + ux \tag{7.1.4}$$

7.2. Let $F = \mathbb{F}_p(u)$ and let X be the regular, proper model of one of the affine curves over F defined by equations 7.1.1-7.1.4. Then it is easy to see that X is smooth over Spec F and satisfies the hypotheses of the four monomials Theorem 6.2. (The quantity δ appearing in Shioda's conditions is equal to 2 in the first three cases, and $2g+1$ in the fourth case.) Thus the Jacobian J of the curve X and all its base changes under $u \mapsto t^d$ satisfy the conjecture of Birch and Swinnerton-Dyer.

In Subsections 7.3 to 7.10 below, we will prove that the curve defined by equation 7.1.1 satisfies the hypotheses of the towers Theorem 4.7 and has Lie irreducible monodromy. Then in Section 7.11 we will give the minor modifications needed to treat equations 7.1.2 and 7.1.3. Finally, in Section 7.12 we treat the last case, equation 7.1.4.

7.3. Lemma. *Suppose that F is a global field of characteristic $p > 2$ and X is a smooth hyperelliptic curve over F with affine equation $y^2 = f(x)$ for some polynomial $f \in F[x]$ with distinct roots. Let ρ be the natural representation of G_F on $H^1(X \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ (ℓ any prime $\neq p$). Then ρ is everywhere tamely ramified if and only if the splitting field of f is an everywhere tamely ramified extension of F.*

Proof. The question of whether or not ρ is everywhere tame is independent of ℓ by [Sai03, 3.11] and thus we may assume $\ell = 2$. As a representation of G_F, $H^1(X \times \overline{F}, \mathbb{Q}_2)$ is dual to the 2-adic Tate module $V_2 J$ and so it suffices to show that the latter is everywhere tame. The 2-torsion in J is spanned by the classes of divisors of degree zero supported on the Weierstrass points $(\alpha, 0)$ where α is a root of f together with the point at infinity on X if the degree of f is odd. Using this it is not hard to check that the fixed field of the kernel of the action of Galois on the 2-torsion $J[2]$ is precisely the splitting field of f. The restriction of ρ to the Galois group of this field takes its values in $I + 2M_2(\mathbb{Z}_2)$ which is a pro-2 group and so

this restriction is at worst tamely ramified. Therefore ρ itself is tamely ramified if and only if the splitting field of f is tamely ramified over F. □

7.4. Lemma. *Let $p > 2$ be a prime and let $n > 1$ be an integer such that $p \nmid n(n-1)$. Then $f(x) = x^n + x^{n-1} + u$ is irreducible over $\overline{\mathbb{F}}_p(u)$ and its splitting field is everywhere tame with Galois group S_n, the symmetric group on n letters.*

Proof. We will see below that f is irreducible over $\overline{\mathbb{F}}_p(u)$. Let K be its splitting field. Considering f and its derivative $f' = nx^{n-1} + (n-1)x^{n-2}$ we see that the reduction of f at a place of $\overline{\mathbb{F}}_p(u)$ has distinct roots except at the places $u = 0$, $u = a := -(1-n)^{n-1}n^{-n}$, and $u = \infty$. Thus K is unramified over $\overline{\mathbb{F}}_p(u)$ away from these places.

Let F_0 be the completion $\overline{\mathbb{F}}_p((u))$ of $\overline{\mathbb{F}}_p(u)$ at $u = 0$. Consideration of the Newton polygon of f with respect to the valuation of F_0 shows that one root of f, call it α, lies in F_0 and is congruent to -1 modulo u and the other roots have valuation $1/(n-1)$. We have

$$f(x) = (x - \alpha)\left(x^{n-1} + (\alpha+1)x^{n-2} + \cdots + (\alpha^{n-2} + \alpha^{n-3})x - u/\alpha\right).$$

If $g(x)$ denotes the second factor on the right and β is a root of g, then $g(x/\beta)$ is congruent modulo the maximal ideal of $F_0(\beta)$ to $x^{n-1} + b$ where $b \neq 0$. Since $p \nmid (n-1)$, this reduction has distinct roots and so by Hensel's lemma all the roots of g lie in $F_0(\beta)$. Thus the splitting field of f over F_0 is a cyclic extension of degree $(n-1)$. We conclude that there are two places of K over $u = 0$, one unramified and the other totally ramified with index $e = n-1$. In particular, the ramification over 0 is tame.

Now let $v = 1/u$ and $F_\infty = \mathbb{F}_p((v))$ be the completion of $\overline{\mathbb{F}}_p(u)$ at $u = \infty$. Changing variables, let

$$h(x) = u^{-n} f(ux) = x^n + vx^{n-1} + v^{n-1}.$$

Consideration of the Newton polygon of h with respect to the valuation of F_∞ shows that h is irreducible over F_∞ (and so f is irreducible over $\overline{\mathbb{F}}_p(u)$) and that its roots all have valuation $(n-1)/n$. If γ is one of these roots, then modulo the maximal ideal of $F_\infty(\gamma)$, $h(x/\gamma)$ is congruent to $x^n + c$ with $c \neq 0$. Since $p \nmid n$ this reduction has distinct roots and so by Hensel's lemma, all of the roots of h lie in $F_\infty(\beta)$. Therefore the splitting field of f over $\mathbb{F}_\infty$ is a cyclic extension of degree n and is totally ramified ($e = n$). Thus K is totally and tamely ramified over the place $u = \infty$ of $\overline{\mathbb{F}}_p(u)$.

Now let $v = u - a$ and $F_a = \overline{\mathbb{F}}_p((v))$ be the completion of $\overline{\mathbb{F}}_p(u)$ at $u = a$. The specialization of f to $u = a$ has $n-2$ simple roots and a double root $b = (1-n)/n$. By Hensel's lemma, f has $n-2$ of its roots in F_a. Considering the Newton polygon of $f(x+b)$, we see that the other two roots of f have valuation $1/2$ and thus lie in a ramified quadratic extension of F_a. Thus K has $n-2$ split places ($e = 1$) and one place with $e = 2$ over $u = a$. Since $p > 2$, the ramification is tame.

This shows that K is everywhere tame over $\overline{\mathbb{F}}_p(u)$. Inertia at 0 is generated by an $(n-1)$-cycle σ, inertia at ∞ is generated by an n-cycle τ and inertia at a is generated by a simple transposition ρ. Moreover, by the known structure of the tame fundamental group of $\mathbb{P}^1$ minus 3 points, we may choose these generators so that $\rho\sigma = \tau$. Choosing labels so that 1 is the fixed point of σ and $\tau = (12\cdots n)$ we see immediately that $\rho = (12)$. Since the symmetric group is generated by (12) and $(12\cdots n)$ we conclude that the Galois group of K over $\overline{\mathbb{F}}_p(u)$ is S_n. □

7.5. Corollary. *With hypotheses as in Lemma 7.4, The affine plane curve defined by*

$$g(x,x') = x^n + x^{n-1} - x'^n - x'^{n-1} = 0$$

has exactly two irreducible components over $\overline{\mathbb{F}}_p$ both of which are rational over $\mathbb{F}_p$.

Proof. With notation as in Lemma 7.4, the curve in question is the fiber product of two copies of $f = 0$ over the u-line. Its set of irreducible components is thus in bijection with the orbits of S_n on the set of ordered pairs of roots of f in $\overline{\mathbb{F}_p(u)}$ and there are two such orbits, the diagonal and the rest. The equations of the two components are $x - x' = 0$ and $g(x,x')/(x-x') = 0$, both of which are $\mathbb{F}_p$-rational. □

7.6. From here through 7.10 we let X be the curve defined by 7.1.1 and J its Jacobian. We let ρ be the representation of G_F on $H^1(X \times \overline{F}, \overline{\mathbb{Q}}_\ell)$. Let $\pi : \mathcal{X} \to \mathbb{P}^1$ be the model of X constructed in the proof of Theorem 6.2. Then $j : U \hookrightarrow \mathbb{P}^1$, with $U = \mathbb{P}^1 \setminus \{0, a, \infty\}$, is the largest open subset of $\mathbb{P}^1$ over which π is smooth. Let $\mathcal{F}_U$ be the lisse sheaf on U corresponding to the representation ρ and set $\mathcal{F} = j_*\mathcal{F}_U$. This is the "middle extension" sheaf attached to ρ and we may recover ρ from it as the stalk $\mathcal{F}_{\overline{\eta}}$ at the geometric generic point $\overline{\eta}$ corresponding to the fixed algebraic closure F^{alg} of F.

Recall that a linear transformation is called a unipotent pseudoreflection if all of its eigenvalues are 1 and its space of invariants has codimension 1.

7.7. Lemma. *The sheaf $\mathcal{F}$ is everywhere tamely ramified. At the place $u = a$ inertia acts via unipotent pseudoreflections and in particular the exponent of the Artin conductor is 1. Therefore, $\mathcal{F}$ (or rather ρ) satisfies the hypotheses of Theorem 4.7.*

Proof. The preceding two lemmas show that ρ is everywhere tamely ramified and therefore the same is true of $\mathcal{F}$. To analyze the ramification at $u = a$, consider the following surface: let

$$V_1 = \operatorname{Spec} \mathbb{F}_p[u,x,y]/\left(y^2 - (x^{2g+2} + x^{2g+1} + u)\right)$$
$$V_2 = \operatorname{Spec} \mathbb{F}_p[u,x',y']/\left(y'^2 - (1 + x' + ux'^{2g+2})\right)$$

and define $\mathcal{Y}$ as the result of glueing V_1 and V_2 using the map

$$(x', y', u) = (x^{-1}, yx^{-g-1}, u).$$

There is a map $\mathcal{Y} \to \mathbb{A}^1$ (projection onto the u coordinate) which is proper, relatively minimal, and whose generic fiber is X. Moreover, $\mathcal{Y}$ is a regular surface and therefore we may identify Y with the open subset $\pi^{-1}(\mathbb{A}^1) \subset \mathcal{X}$ where $\pi : \mathcal{X} \to \mathbb{P}^1$ was constructed in the proof of Theorem 6.2. The restriction $\pi_{\mathbb{A}^1} : \mathcal{Y} \to \mathbb{A}^1$ is smooth except over $u = a$, and over $u = a$, it has an isolated singularity which is an ordinary double point. In classical language, $\pi_{\mathbb{A}^1}$ is a Lefschetz pencil. The famous Picard-Lefschetz formula ([SGA7-2, 3.4] or [Mil80, V.3.14]) gives the action inertia on $\mathcal{F}_{\mathbb{A}^1} = R^1\pi_{\mathbb{A}^1 *}\overline{\mathbb{Q}}_\ell$ and in particular it shows that the action of inertia at $u = a$ is by unipotent pseudoreflections. Since the ramification at $u = a$ is tame, the exponent of the Artin conductor is just the codimension of the space of inertia invariants which is 1. □

7.8. Lemma. *$\mathcal{F}$ is geometrically irreducible as middle extension sheaf on $\overline{\mathbb{P}^1}$. Equivalently, ρ restricted to $\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_p F)$ is geometrically irreducible.*

Proof. We apply the diophantine criterion for irreducibility of Katz, along the lines of [KS99, 10.1.15]. This criterion amounts to using the Grothendieck-Lefschetz trace formula and the Weil conjectures to prove that $\mathrm{End}_{\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_p F)}(\rho)$ is one-dimensional by estimating certain sums of traces. By Schur's lemma, this one-dimensionality is equivalent to the desired irreducibility. We refer to [KS99, 10.1.15] for more details.

What has to be shown is that

$$\sum_{\substack{u\in\mathbb{F}_q\\ u\neq 0,a}} Tr(Fr_u|\mathcal{F})^2 = q^2 + O(q^{3/2})$$

as q ranges through all powers of p.

Using the Grothendieck-Lefschetz trace formula on the fibers of π we see that

$$\begin{aligned} Tr(Fr_u|\mathcal{F}) &= q - 1 - \sum_{x\in\mathbb{F}_q} \left(1 + \chi(x^{2g+2} + x^{2g+1} + u)\right) \\ &= -1 - \sum_{x\in\mathbb{F}_q} \chi(x^{2g+2} + x^{2+1} + u) \end{aligned}$$

where χ is the nontrivial quadratic character of ${\mathbb{F}_q}^\times$ extended as usual to a function on $\mathbb{F}_q$. (The reader will note that there are two points at infinity on the affine curve 7.1.1.) By theorems of Weil and Deligne, the trace is $O(q^{1/2})$. Thus the sum to be estimated is

$$\sum_{\substack{u\in\mathbb{F}_q\\ u\neq 0,a}} \left(-1 - \sum_{x\in\mathbb{F}_q} \chi(x^{2g+2} + x^{2g+1} + u)\right)^2$$

and because of the Deligne estimate, we may drop the conditions $u \neq 0, a$. Thus our sum is

$$\begin{aligned} &\sum_{u\in\mathbb{F}_q} \sum_{x,x'\in\mathbb{F}_q} \chi\left((x^{2g+2} + x^{2g+1} + u)(x'^{2g+2} + x'^{2g+1} + u)\right) + O(q^{3/2}) \\ &\qquad = \sum_{x,x'\in\mathbb{F}_q} \sum_{u\in\mathbb{F}_q} \chi\left(u^2 + u(x^{2g+2} + x^{2g+1} + x'^{2g+2} + x'^{2g+1})\right. \\ &\qquad\qquad \left. + (x^{2g+2} + x^{2g+1})(x'^{2g+2} + x'^{2g+1})\right) + O(q^{3/2}). \end{aligned}$$

The inner sum over u is related to the number of points on the hyperelliptic curve

$$y^2 = u^2 + u(x^{2g+2} + x^{2g+1} + x'^{2g+2} + x'^{2g+1}) + (x^{2g+2} + x^{2g+1})(x'^{2g+2} + x'^{2g+1}).$$

Noting that $g(x,x') = (x^{2g+2} + x^{2g+1}) - (x'^{2g+2} + x'^{2g+1}) = 0$ if and only if the quadratic polynomial in u has a double root, we see that the sum over u is -1 if $g(x,x') \neq 0$ and it is $q-1$ if $g(x,x') = 0$. Therefore the sum to be estimated is

$$\sum_{\substack{x,x'\in\mathbb{F}_q\\ g(x,x')\neq 0}} (-1) + \sum_{\substack{x,x'\in\mathbb{F}_q\\ g(x,x')=0}} (q-1) + O(q^{3/2}).$$

The first sum is over an affine open subset of $\mathbb{A}^2$ and is therefore $-q^2 + O(q)$. The second sum is over a curve which by Corollary 7.5 has exactly 2 components and therefore has $2q + O(q^{1/2})$ points. Thus the second sum contributes $2q^2 + O(q^{3/2})$ and the entire sum is $q^2 + O(q^{3/2})$. □

7.9. *Remark.* Another approach to irreducibility would be to assume $\ell = 2$ and use Lemma 7.4 to argue that the mod 2 representation $J[2]$ is irreducible and so *a fortiori* the 2-adic representation $V_2 J$ is irreducible. But this argument does not apply to the other curves 7.1.2 and 7.1.3 whereas the argument given above does apply with minor modifications.

We recall from Subsection 5.2 the notion of a Lie irreducible representation.

7.10. Lemma. *The representation ρ is Lie irreducible. In fact, the geometric monodromy group of ρ is the full symplectic group Sp_{2g}.*

Proof. Later in the proof we are going to assume that $\ell = 2$. It follows from [Chi04] and the fact that G^{geom} is *a priori* contained in Sp_{2g} that if $G^{\mathrm{geom}} = \mathrm{Sp}_{2g}$ for one $\ell \neq p$ then it is so for all $\ell \neq p$. The reader who prefers not to go into this may simply assume that $\ell = 2$ for the entire proof of the last part of Theorem 1.1.

We have already seen that $\rho' := \rho|_{\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_p F)}$ is irreducible. It follows from [Kat87, Proposition 1] that ρ' is either Lie irreducible, tensor decomposable (in the sense that $\rho' \cong \sigma \otimes \tau$ where σ and τ are representations of $\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_p F)$ with σ Lie irreducible and τ of degree > 1 with finite image), or is induced from a representation of a proper subgroup of $\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_p F)$. We rule out the last two possibilities.

Since inertia at $u = 1$ acts via a unipotent pseudoreflection, ρ' can be tensor decomposable only if the degree of σ is 1, which implies that σ has finite image. But if it were so, then ρ' would also have finite image and this is impossible because a unipotent pseudoreflection has infinite order.

Now suppose that ρ' is induced from a representation σ of some subgroup of $\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_p F)$ corresponding to a cover $\pi : \mathcal{C} \to \overline{\mathbb{P}^1}$. We write $\rho'(x)$ for ρ viewed (by restriction) as a representation of the inertia group $I(x)$ at a place $x \in \overline{\mathbb{P}^1}$ and similarly for σ. We have

$$\rho'(x) = \bigoplus_{y \mapsto x} \mathrm{Ind}_{I(y)}^{I(x)} \sigma(y)$$

where the sum is over points of $\mathcal{C}$ mapping to x. Considering this equality at the place $u = a$ where inertia acts with invariants of codimension 1, we see that $I(y) = I(a)$ for all y over a, in other words, σ must be unramified over a. We also must have that σ is at worst tamely ramified over 0 and ∞. This means that π must be a cyclic cover obtained by extracting a root of u, i.e., $\mathcal{C} = \mathbb{P}^1$ with coordinate v and $\pi^*(u) = v^m$.

We argue that $m > 1$ is incompatible with what we know about the action of inertia at $u = 0$ on 2-torsion. Indeed, if $m > 1$ and h is a generator of tame inertia at 0, then the trace of h on $\rho'(0)$ is zero. On the other hand, the action of h on the 2-torsion subgroup $J[2]$ has non-zero trace. More precisely, label the roots α_i ($i = 0, \dots, 2g+1$) of $f(x) = x^{2g+2} + x^{2g+1} + t$ so that α_0 is fixed by $I(0)$ and the others are permuted cyclically (cf. the proof of Lemma 7.4). Let P_i be the Weierstrass point $(\alpha_i, 0)$ on X and let D_i be the class of $P_i - P_0$ in $J[2]$. Then $J[2]$ is generated as $\mathbb{F}_2$ vector space by $D_1, \dots, D_{2g+1}$ with the single relation $\sum D_i = 0$. The proof of 7.4 shows that h permutes the D_i cyclically. Considering the matrix of h in the basis $D_1, \dots, D_{2g}$ of $J[2]$ we see that h has trace $-1 = 1$ on $J[2]$ and therefore h has non-zero trace on $\rho'(0)$. Thus $m > 1$ is impossible and so $\mathcal{F}$ is not induced from any non-trivial cover.

This completes the proof that ρ is Lie irreducible. Since there is a place where inertia acts on ρ by a unipotent pseudoreflection, in fact the geometric monodromy group of ρ is Sp_{2g} (see [Kat90, 1.5] for details). □

7.11. This completes the proof that the curves 7.1.1 are examples for Theorem 1.1. For 7.1.2 and 7.1.3, the proof is essentially the same. Very minor modifications are needed in Lemma 7.7 (checking that $\mathcal{X} \to \mathbb{P}^1$ is a Lefschetz pencil over $\mathbb{A}^1 \setminus \{0\}$) and in Lemma 7.8 (applying the diophantine criterion for irreducibility). At the end of the proof of Lemma 7.10 (checking Lie irreducibility), for 7.1.2, we use the action of monodromy at ∞ (which again is a cyclic permutation of order $2g+1$) and for 7.1.3 we use Lemma 7.4 to see that in terms of a suitable basis of $J[2]$, a generator h of tame inertia at 0 has one fixed vector and permutes the other $2g-1$ vectors cyclically. Altogether this completes the proof of Theorem 1.1 for $p > 2$.

7.12. For $p = 2$ and the curve 7.1.4, we already saw in Subsection 5.5 that the hypotheses of the towers Theorem 4.7 are satisfied and that this curve has large geometric monodromy group. We also saw in Subsection 7.2 that the hypotheses of the four monomials Theorem 6.2 are satisfied. This completes the proof of Theorem 1.1 for $p = 2$.

8. Proof of Theorem 1.2

We will use some basic representation theory to see that the action of G_F on $H^k_{prim}(J, \overline{\mathbb{Q}}_\ell)$ satisfies the hypotheses of Theorem 4.7 where J is the Jacobian of one of the curves studied in Section 5.4 for suitable g and k.

8.1. If A is a principally polarized abelian variety of dimension g over a field F (e.g., a Jacobian), then the étale cohomology group $H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ carries a non-degenerate symplectic form $\langle , \rangle$. If k is odd, then the same is true of $H^k(A \times \overline{F}, \overline{\mathbb{Q}}_\ell) \cong \bigwedge^k H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$.

If $k > 1$, define a linear map $\phi : \bigwedge^k H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell) \to \bigwedge^{k-2} H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ by

$$\phi(w_1 \wedge \cdots \wedge w_k) = \sum_{1 \le i < j \le k} (-1)^{i+j-1} \langle w_i, w_j \rangle w_1 \wedge \cdots \wedge \hat{w}_i \wedge \cdots \wedge \hat{w}_j \wedge \cdots \wedge w_k$$

where a hat denotes a vector to omit.

Choose a symplectic basis $v_1, \ldots, v_{2g}$ of $H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$, i.e., one satisfying $\langle v_i, v_{j+g} \rangle = \delta_{ij}$ and $\langle v_i, v_j \rangle = \langle v_{i+g}, v_{j+g} \rangle = 0$ for $1 \le i, j \le g$. Define a linear map $\psi : \bigwedge^{k-2} H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell) \to \bigwedge^k H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ by

$$\psi(w) = w \wedge (v_1 \wedge v_{g+1} + \cdots + v_g \wedge v_{2g}).$$

The map ψ is independent of the choice of basis; it depends only on the symplectic form $\langle , \rangle$.

We define the primitive part $H^k_{prim}(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ to be the kernel of ϕ. It is well known that if $k \le g$ then ψ is injective and we have a direct sum decomposition

$$H^k(A \times \overline{F}, \overline{\mathbb{Q}}_\ell) \cong H^k_{prim}(A \times \overline{F}, \overline{\mathbb{Q}}_\ell) \bigoplus \mathrm{Im}(\psi). \tag{8.1.1}$$

Also, both ϕ and ψ are equivariant for the action of G_F and so this direct sum decomposition is respected by Galois. The symplectic pairing on $H^k(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ induced by $\langle , \rangle$ restricts to a non-degenerate symplectic pairing on $H^k_{prim}(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$.

8.2. Now assume that $p > 2$ and let C be one of the curves considered in Section 5.4 and J its Jacobian. Let ρ_1 be the representation of G_F on $H^1(J \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ and let ρ_k be the representation of G_F on $H^k_{prim}(J \times \overline{F}, \overline{\mathbb{Q}}_\ell)$. Then ρ_k is self-dual of weight k and sign -1. Because the monodromy group of ρ_1 is the full symplectic group, ρ_k is irreducible.

The representation ρ_1 is everywhere tamely ramified and at each finite place $u_0 \in \mathbb{A}^1$ of bad reduction, the local inertia group $I(u_0)$ acts via unipotent pseudoreflections. (By [KS99, 10.1.13] the action is either trivial or by unipotent pseudoreflections, but it is not hard to see that the fibration $\mathcal{X} \to \mathbb{P}^1$ attached to the curves we are considering is a Lefschetz fibration over $\mathbb{A}^1$ and so the local monodromies at finite places of bad reduction are in fact unipotent pseudoreflections.) This means that in terms of a suitable symplectic basis $v_1, \dots, v_{2g}$, the action of inertia is

$$\begin{aligned} s(v_1) &= v_1 + \lambda(s) v_{g+1} \\ s(v_i) &= v_i \qquad i = 2, \dots, 2g \end{aligned} \tag{8.2.1}$$

where $\lambda : I(u_0) \to \overline{\mathbb{Q}}_\ell$ is a non-zero character.

Because ρ_1 is everywhere tame, ρ_k is also everywhere tame. In particular, the exponent of the conductor of ρ_k at a place u_0 is just the codimension of the space of invariants of $\rho_k(I(u_0))$. We will show that at finite u_0 this codimension depends only on g and k and that for every k there are infinitely many g such that this codimension is odd. For such g and k, the representation ρ_k satisfies the hypotheses of Theorem 4.7 and this will prove Theorem 1.2.

8.3. We fix a finite place $u_0 \neq 0$ of F where C has bad reduction and consider the action of the inertia group $I(u_0)$ on $\bigwedge^k H^1(J \times \overline{F}, \overline{\mathbb{Q}}_\ell)$. Choose a symplectic basis $v_1, \dots, v_{2g}$ of $V = H^1(A \times \overline{F}, \overline{\mathbb{Q}}_\ell)$ such that the action of $I(u_0)$ is given by 8.2.1. Let V_1 be the span of v_1 and v_{g+1} and let V_2 be the span of $v_2, \dots, v_g$ and $v_{g+2}, \dots, v_{2g}$. Then we have

$$\bigwedge^k V \cong (\bigwedge^2 V_1 \otimes \bigwedge^{k-2} V_2) \bigoplus (V_1 \otimes \bigwedge^{k-1} V_2) \bigoplus (\bigwedge^k V_2).$$

It is easy to see using 8.2.1 that $I(u_0)$ acts trivially on the first and third summands and that the codimension of its invariants on the middle summand is $\dim \bigwedge^{k-1} V_2 = \binom{2g-2}{k-1}$.

A similar analysis shows that the space of $I(u_0)$-invariants on $\psi(\bigwedge^{k-2} V)$ has codimension $\binom{2g-2}{k-3}$. From the direct sum decomposition 8.1.1 we conclude that the exponent of the conductor of ρ_k at u_0, i.e., the codimension of the $I(u_0)$ invariants on $H^k_{prim}(J \times \overline{F}, \overline{\mathbb{Q}}_\ell)$, is $\binom{2g-2}{k-1} - \binom{2g-2}{k-3}$.

8.4. To conclude the proof of Theorem 1.2, we will show that for every odd k there are infinitely many g such that $\binom{2g-2}{k-1} - \binom{2g-2}{k-3}$ is odd. We recall the well-known fact that the 2-adic valuation of $\binom{n}{m}$ is equal to the number of carries in the sum of m and $n-m$ in base 2. Since k is odd, exactly one of $k-1$ and $k-3$ is congruent to 2 (mod 4) and the other is congruent to 0 (mod 4). To fix ideas, suppose $k-1$ is 0 (mod 4). Let a be an integer so that $2^a > k$ and choose g so that $2g-k-1$ is congruent to 0 (mod 2^a). Then there are no carries in the sum $(k-1)+(2g-k-1)$ and so $\binom{2g-2}{k-1}$ is odd. On the other hand, both $k-3$ and $2g-k+1$ are congruent

to 2 (mod 4) and so there is at least one carry in the sum $(k-3)+(2g-k+1)$ and $\binom{2g-2}{k-3}$ is even. The case where $k-1 \equiv 2 \pmod 4$ is similar and will be left to the reader. This completes the proof of Theorem 1.2.

8.5. *Remark.* The above proof would carry over verbatim to $p=2$ if we had a curve over $\mathbb{F}_2(u)$ with large, everywhere tame monodromy, and inertia acting by unipotent reflections at an odd number of non-zero finite places.

9. Proof of Theorem 1.3

Let p be any prime, q a power of p, and E an elliptic curve over $F=\mathbb{F}_q(v)$. Let ρ be the representation of G_F on $H^1(E\times\overline{F},\overline{\mathbb{Q}}_\ell)$ for some $\ell\neq p$; ρ is self dual of weight 1 and sign -1. For every finite separable extension K of F, we have $L(E/K,s)=L(\rho,K,s)$. We prove Theorem 1.3 by showing that after replacing F with an extension of the form $\mathbb{F}_r(u)$, the hypotheses of Theorem 4.7 are met and so E obtains large analytic rank over $\mathbb{F}_r(t)$ with $t^d=u$ for large d of the form r^n+1.

9.1. Lemma. *Suppose that E is an elliptic curve over $F=\mathbb{F}_q(v)$ with $j(E)\notin\mathbb{F}_q$. Then there is a finite separable extension of F of the form $\mathbb{F}_r(u)$ over which E has an $\mathbb{F}_r$-rational place of multiplicative reduction and two $\mathbb{F}_r$-rational places of good reduction.*

Proof. Extending the ground field to $\mathbb{F}_r$ and making a linear change of coordinates, we may assume that the j-invariant of E has a pole at $v=0$. It is well known that there is a finite separable extension of the completion $\mathbb{F}_r((v))$ over which E obtains multiplicative reduction.

The following lemma (whose proof is due to Bjorn Poonen) says that we may realize the local extension as the completion of a global extension of *rational* fields. Admitting the lemma, E has an $\mathbb{F}_r$-rational place of multiplicative reduction over $\mathbb{F}_r(u)$. Clearly at the expense of increasing r we may insure that E also has two $\mathbb{F}_r$-rational places of good reduction over $\mathbb{F}_r(u)$. □

9.2. Lemma. *Let $F=\mathbb{F}_r(v)$ and let K_0 be a finite separable extension of $F_0:=\mathbb{F}_r((v))$. Then there exists a finite separable extension K of F of the form $K=\mathbb{F}_r(u)$ so that the completion of K at the place $u=0$ is isomorphic, as extension of F_0, to K_0.*

Proof. It is well known that K_0 is abstractly isomorphic to $\mathbb{F}_r((\varpi))$. Let $g(T)\in\mathbb{F}_r[[T]]$ (T an indeterminate) be the formal series such that $g(\varpi)=v$ in K_0. Since K_0/F_0 is a separable extension, $g'(\varpi)$, the derivative series evaluated at ϖ, is not zero. For a positive integer n, let g_n be the sum of the first n terms of g. Then as $n\to\infty$, the valuation of $g_n'(\varpi)$ stabilizes at a finite value whereas the valuation of $g_n(\varpi)-v$ tends to infinity. By Hensel's lemma, for any sufficiently large n, there is a root u of $g_n(T)-v$ in K_0 which is congruent to ϖ modulo a high power of ϖ and which is thus a uniformizer of K_0. Now let K be the subfield of K_0 generated by $\mathbb{F}_r$ and u. Since v is a polynomial in u with a non-zero derivative, K is a finite, separable extension of F. □

9.3. With these preliminaries out of the way, we can prove Theorem 1.3. Since the j-invariant of E is not in $\mathbb{F}_q$, ρ is irreducible.

If the degree of the conductor of E is odd, we make a linear change of coordinates so that $u=0$ and $u=\infty$ are places of good reduction. Then, in the notation of

Theorem 4.7, $\deg(\mathfrak{n}') + \mathrm{Swan}_0(\rho) + \mathrm{Swan}_\infty(\rho)$ is the degree of the conductor of E which is odd. Thus ρ satisfies the hypotheses of Theorem 4.7.

If the degree of the conductor of E is even, we make a change of coordinates so that $u = 0$ is a place of good reduction and $u = \infty$ is a place of multiplicative reduction. Then, in the notation of Theorem 4.7, $\deg(\mathfrak{n}') + \mathrm{Swan}_0(\rho) + \mathrm{Swan}_\infty(\rho)$ is one less than the degree of the conductor of E and is therefore odd. Again ρ satisfies the hypotheses of Theorem 4.7. □

9.4. In [Ulmer] we give examples of elliptic curves over $\mathbb{F}_q(u)$ with bounded rank in the tower $\mathbb{F}_q(t)$ $(t^d = u)$, $d \to \infty$.

10. Proof of Theorem 1.4

We use the notation of the statement of Theorem 1.4. Tate and Shafarevitch observed in [TS67] that to produce a quadratic twist E' of E with large rank, one must produce a hyperelliptic curve $\mathcal{C} \to \mathbb{P}^1_t$ whose Jacobian has many factors isogenous to E_0. More precisely, if E' is the twist of E by the quadratic extension $\mathbb{F}_p(\mathcal{C})$, then the rank of $E'(\mathbb{F}_p(t))$ is equal to the rank of the endomorphsim ring of E_0 (which in our case is 2) times the number of isogeny factors of $J(C)$ isogenous to E_0. (See [Ulmer, §4] for more details.) Moreover, we may detect the number of times a particular abelian variety appears in the Jacobian of a curve via Honda-Tate theory by considering the inverse roots of its zeta function. In the rest of this section we will use an orthogonal variant of the towers Theorem 4.7 to produce hyperelliptic curves whose Jacobians have many isogeny factors isogenous to a given supersingular elliptic curve.

10.1. We call the inverse roots of the zeta function of a curve its *Weil numbers*. It is well known (see, e.g., [Wat69, Chap. 4]) that a supersingular elliptic curve over $\mathbb{F}_p$ (any p) either has Weil number $\zeta_4\sqrt{p}$ with ζ_4 a primitive 4-th root of unity, or $p = 3$ and the Weil number is $\zeta_{12}\sqrt{3}$ with ζ_{12} a primitive 12-th root of unity, or $p = 2$ and the Weil number is $\zeta_8\sqrt{2}$ with ζ_8 a primitive 8-th root of unity. We start with the case $p > 2$ and E_0 a supersingular elliptic curve with Weil number $\zeta_4\sqrt{p}$.

10.2. Let $F = \mathbb{F}_p(u)$ and let C_1 be a geometrically irreducible curve smooth and proper over $\mathbb{F}_p$ with genus $g \geq 0$ equipped with a degree 2 morphism $\pi : C_1 \to \mathbb{P}^1$. We assume π to be ramified at $2g + 2$ geometric points $(a_1, \dots, a_{2g+1}, \infty)$ one of which is infinity and none of which are 0. Corresponding to the covering $\pi : C_1 \to \mathbb{P}^1$ is a character ρ of G_F of order 2. The numerator of the zeta function of C_1 is $L(\rho, F, s)$.

For a positive integer d not divisible by p, we let $F_d = \mathbb{F}_p(t)$ be the extension of F with $u = t^d$ and we let $\pi_d : C_d \to \mathbb{P}^1_t$ be the 2-1 covering corresponding to ρ restricted to $\mathrm{Gal}(\overline{F}/\mathbb{F}_p(t))$. It is not hard to check that C_d is the normalization of the fiber product $C_1 \times_{\mathbb{P}^1_u} \mathbb{P}^1_t$. The ramification points of π_d are the d-th roots of the a_i, 0, and, if d is odd, ∞.

10.3. The numerator of the zeta function of C_d is $L(\rho, F_d, s)$ and by the analysis in Subsection 4.4,

$$L(\rho, F_d, s) = \prod_{o \subset \mathbb{Z}/d\mathbb{Z}} L(\rho \otimes \sigma_o, F, s)$$

where the product is over the orbits of multiplication by p on $\mathbb{Z}/d\mathbb{Z}$. If χ is a character of $\mathrm{Gal}(\overline{F}/\mathbb{F}_p(\mu_d, u))$ of order d corresponding to the extension $\mathbb{F}_p(\mu_d, t)$,

then it is easy to see that $\deg \mathrm{Cond}(\rho\otimes\chi^i)$ is odd except when χ^i has order dividing 2. It follows from Theorem 4.5 that if $d = p^n + 1$ and $o \subset \mathbb{Z}/d\mathbb{Z}$ is any orbit for multiplication by p other than $\{0\}$ or $\{d/2\}$ and $a = \#o$, then $1 + (Tp^{1/2})^a$ divides $L(\rho\otimes\sigma_o, F, s)$. If we take n odd and let o be an orbit passing through $i \in (\mathbb{Z}/d\mathbb{Z})^\times$, then a is $2n$ and so $\zeta_4\sqrt{p}$ is a root of $1+(Tp^{1/2})^a$. Since there are $\phi(p^n+1)/2n$ such orbits, we see that $\zeta_4\sqrt{p}$ is an inverse root of the numerator of the zeta function of C_d with large multiplicity. As discussed above, this shows that E' has large rank over $F_d = \mathbb{F}_p(t)$.

10.4. Now consider the case where E_0 is a supersingular elliptic curve over $\mathbb{F}_3$ with Weil number $\zeta_{12}\sqrt{3}$ where ζ_{12} is a primitive 12-th root of unity. We proceed as above except that we assume that $n \equiv 3 \pmod 6$ so that $\zeta_{12}\sqrt{3}$ is an inverse root of $1 + (T\sqrt{3})^a$ where $a = 2n$.

10.5. If $p = 2$ then we proceed as above starting with a curve $C_1 \to \mathbb{P}^1_u$ corresponding to a quadratic character ρ satisfying the conductor condition of 4.7, namely that $\mathrm{Swan}_0(\rho)+\mathrm{Swan}_\infty(\rho)+\deg\mathfrak{n}'$ is odd. (For example, $y^2+y = u$.) If the Weil number of E_0 is $\zeta_4\sqrt{2}$ then we take $d = p^n + 1$ with n odd and if the Weil number of E_0 is $\zeta_8\sqrt{2}$ then we take $d = p^n + 1$ with $n \equiv 2 \pmod 4$.

10.6. Interestingly, the argument above does not prove that if E_0 is any supersingular elliptic curve over $\mathbb{F}_q$ then there are quadratic twists of E with high rank, only the slightly weaker statement that there is a power r of q and quadratic twists of E with high rank over $\mathbb{F}_r(t)$. The problem is that if the Weil number of E_0 is $\zeta_m\sqrt{q}$ with m odd, then this Weil number is not a root of $1+(q^{1/2}T)^a$ for any even a.

11. A remark on rank bounds

Suppose as usual that F is the function field of a curve $\mathcal{C}$ of genus $g_\mathcal{C}$ over $\mathbb{F}_q$ and that ρ is a representation of G_F satisfying the hypotheses of Subsection 4.2 and (for simplicity) that ρ restricted to $\mathrm{Gal}(\overline{F}/\overline{\mathbb{F}}_qF)$ has no trivial constituents. Let $\mathfrak{n}$ be the conductor of ρ. Then the Grothendieck-Ogg-Shafarevitch formula says that the degree of the L-function ρ over F as a polynomial in q^{-s} is $D = \deg(\mathfrak{n}) + \deg(\rho)(2g_\mathcal{C} - 2)$. In particular, we have the "geometric" rank bound (cf. [Ulm04])

$$\mathrm{ord}_{s=(w+1)/2}\, L(\rho, F, s) \le \mathrm{ord}_{s=(w+1)/2}\, L(\rho, \mathbb{F}_rF, s) \le D \tag{11.1}$$

valid for any power r of q.

This can be improved when D is large with respect to q, $g_\mathcal{C}$, and $\deg(\rho)$. Indeed, minor modifications of Brumer's argument in [Bru92] (itself modelled on Mestre's [Mes86]) allow one to prove the arithmetic rank bound

$$\mathrm{ord}_{s=(w+1)/2}\, L(\rho, F, s) \le \frac{D}{2\log_q D} + O\left(\frac{D}{(\log_q D)^2}\right) \tag{11.2}$$

where the implied constant depends only on q, $g_\mathcal{C}$, and $\deg(\rho)$.

In [Ulm02] we showed that the main term of this arithmetic bound, as well as the geometric bound, are sharp for L-functions of elliptic curves. The towers Theorem 4.7 gives a large supply of other examples related to this question.

Indeed, suppose that ρ is a representation of G_F where $F = \mathbb{F}_q(u)$ satisfying the hypotheses of 4.7 and let N be the quantity $\mathrm{Swan}_0(\rho)+\mathrm{Swan}_\infty + \deg(\mathfrak{n}')$ appearing in that result. Then the degree of $L(\rho, F_d, s)$, where $F_d = \mathbb{F}_q(t)$ with $u = t^d$, is

asymptotic to Nd; they differ by an amount bounded independently of d. The towers Theorem 4.7 shows that for d of the form $d = q^n + 1$

$$\operatorname{ord}_{s=(w+1)/2} L(\rho, F_d, s) \geq \frac{d}{2\log_q d} - c$$

and

$$\operatorname{ord}_{s=(w+1)/2} L(\rho, \mathbb{F}_{q^{2n}} F_d, s) \geq d - c'$$

where c and c' are constants independent of n. These lower bounds are roughly $1/N$ times the upper bounds discussed above.

For the curves discussed in Section 7 with $p > 2$, we have $N = 1$ and so we have a large collection of interesting representations for which the main term of the rank bounds are sharp.

References

[Blo84] S. Bloch, *Algebraic cycles and values of L-functions*, J. Reine Angew. Math. **350** (1984), 94–108.

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

[Chi04] C. Chin, *Independence of l of monodromy groups*, J. Amer. Math. Soc. **17** (2004), 723–747 (electronic).

[Con06] B. Conrad, *Chow's K/k-image and K/k-trace, and the Lang-Néron theorem*, Enseign. Math. (2) **52** (2006), 37–108.

[CT02] A. Cortella and J-P. Tignol, *The asymmetry of an anti-automorphism*, J. Pure Appl. Algebra **167** (2002), 175–193.

[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), 1973, pp. 501–597. Lecture Notes in Math., Vol. 349 (French).

[Ellen] J. S. Ellenberg, *Selmer groups and Mordell-Weil groups of elliptic curves over towers of function fields* (2005), Preprint, to appear in *Compositio Mathematica*.

[Gro68] A. Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, 1968, pp. 88–188 (French).

[KT03] K. Kato and F. Trihan, *On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$*, Invent. Math. **153** (2003), 537–592.

[Kat87] N. M. Katz, *On the monodromy groups attached to certain families of exponential sums*, Duke Math. J. **54** (1987), 41–56.

[Kat90] ———, *Exponential sums and differential equations*, Annals of Mathematics Studies, vol. 124, Princeton University Press, Princeton, NJ, 1990.

[KS99] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications, vol. 45, American Mathematical Society, Providence, RI, 1999.

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

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

[Mil86] ———, *Arithmetic duality theorems*, Perspectives in Mathematics, vol. 1, Academic Press Inc., Boston, MA, 1986.

[Sai03] T. Saito, *Weight spectral sequences and independence of l*, J. Inst. Math. Jussieu **2** (2003), no. 4, 583–634.

[Ser77] Jean-Pierre Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977.

[Ser79] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979.

[SGA7-2] P. Deligne and N. M. Katz, *Groupes de monodromie en géométrie algébrique. II*, Springer-Verlag, Berlin, 1973 (French).

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

[SK79] T. Shioda and T. Katsura, *On Fermat varieties*, Tôhoku Math. J. (2) **31** (1979), 97–115.

[Tat66] J. T. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, 1966, Vol. 9, Exp. No. 306, pp. 415–440.

[Tat94] ———, *Conjectures on algebraic cycles in l-adic cohomology*, Motives (Seattle, WA, 1991), 1994, pp. 71–83.

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

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

[Ulm04] ———, *Elliptic curves and analogies between number fields and function fields*, Heegner points and Rankin L-series, 2004, pp. 285–315.

[Ulm05] ———, *Geometric non-vanishing*, Invent. Math. **159** (2005), 133–186.

[Ulmer] ———, *Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields* (2005), Preprint.

[Wat69] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560.

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