ELLIPTIC CURVES WITH LARGE RANK OVER FUNCTION FIELDS

DOUGLAS ULMER

ABSTRACT. We produce explicit elliptic curves over $\mathbb{F}_p(t)$ whose Mordell-Weil groups have arbitrarily large rank. Our method is to prove the conjecture of Birch and Swinnerton-Dyer for these curves (or rather the Tate conjecture for related elliptic surfaces) and then use zeta functions to determine the rank. In contrast to earlier examples of Shafarevitch and Tate, our curves are not isotrivial.

Asymptotically these curves have maximal rank for their conductor. Motivated by this fact, we make a conjecture about the growth of ranks of elliptic curves over number fields.

1. INTRODUCTION

1.1. Let K be a field and consider elliptic curves defined over K. A natural question is whether there exist elliptic curves over K with arbitrarily large Mordell-Weil rank. In other words, for every r is there an E such that $E(K)$ contains at least r independent points of infinite order? The general expectation seems to be that such curves exist for any field K which is not algebraic over a finite field.

1.2. For fields of characteristic zero, it obviously suffices to treat the case $K = \mathbb{Q}$. Here the question is open and it seems to be quite difficult to produce examples with large rank. At this writing, the largest known rank is 24 ([MM00]) and the largest proven analytic rank (i.e., order of vanishing of L-series at $s = 1$) is 3 ([GZ86]).

1.3. For fields of characteristic p, it suffices to consider the rational function field $K = \mathbb{F}_p(t)$. In [TS67], Shafarevitch and Tate produced elliptic curves over K of arbitrarily large rank. They considered a supersingular curve E_0 defined over $\mathbb{F}_p$ (viewed as a curve E over K in the obvious way) and showed that that there are quadratic extensions L/K such that the Jacobian of the curve over $\mathbb{F}_p$ attached to L has a large number of factors isogenous to E_0 over $\mathbb{F}_p$. This implies that the quadratic twist of E by L has large rank.

1.4. The examples of Shafarevitch and Tate are "isotrivial," i.e., after a finite extension (L/K in fact), they become isomorphic to elliptic curves defined over $\mathbb{F}_p$. (Equivalently, their j-invariants lie in $\mathbb{F}_p$.) There is no analog of this property for an elliptic curve over $\mathbb{Q}$ and so it is not clear whether their examples provide evidence for the question over $\mathbb{Q}$. (On the other hand, isotriviality makes sense for fields like $\mathbb{Q}(t)$, and it is conceivable that the arguments of Tate and Shafarevitch might be generalized to this context.)

Date: September 19, 2001.

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

The aim of this paper is to produce elliptic curves over $K = \mathbb{F}_p(t)$ which are non-isotrivial ($j \notin \mathbb{F}_p$) and which have arbitrarily large rank.

1.5. Theorem. *Let p be an arbitrary prime number, $\mathbb{F}_p$ the field of p elements, and $\mathbb{F}_p(t)$ the rational function field in one variable over $\mathbb{F}_p$. Let E be the elliptic curve defined over $K = \mathbb{F}_p(t)$ by the Weierstrass equation*

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

where $d = p^n + 1$ and n is a positive integer. Then $j(E) \notin \mathbb{F}_p$, the conjecture of Birch and Swinnerton-Dyer holds for E over K, and the rank of $E(K)$ is at least $(p^n - 1)/2n$.

1.6. Remarks.

(1) We give a simple expression for the exact rank of $E(K)$ in Theorem 9.2. The j-invariant of E is $t^{-d}(1 - 2^4 3^3 t^d)^{-1}$.
(2) In fact we prove the conjecture of Birch and Swinnerton-Dyer for E over $\mathbb{F}_q(t)$ for q any power of p, and we show that $\operatorname{Rank} E(\mathbb{F}_{p^{2n}}(t)) = \operatorname{Rank} E(\overline{\mathbb{F}}_p(t)) = p^n$ if $6 \nmid d$ and $p^n - 2$ if $6|d$.
(3) In Section 10 we explain that the curves in Theorem 1.5 asymptotically have maximal ranks for their conductor and we make a conjecture about ranks of elliptic curves over number fields.
(4) The displayed Weierstrass equation also defines an elliptic curve over $\mathbb{Q}(t)$. It turns out that this curve has rank which is bounded independently of d, even over $\overline{\mathbb{Q}}(t)$.

1.7. The proof of the theorem involves an appealing mix of geometry and arithmetic. We begin with the geometry: First, we construct an elliptic surface $\mathcal{E} \to \mathbb{P}^1$ over $\mathbb{F}_p$ whose generic fiber is E/K. The rank of the Mordell-Weil group $E(K)$ is closely related to the rank of the Néron-Severi group of $\mathcal{E}$, i.e., to curves on $\mathcal{E}$ up to algebraic equivalence. Next, we define a dominant rational map from a Fermat surface F_d to $\mathcal{E}$, which induces a birational isomorphism between $\mathcal{E}$ and a certain quotient F_d/Γ of the Fermat surface. Thirdly, we carry out a fairly detailed analysis of the geometry of this birational map.

Then comes the arithmetic: The Tate conjecture (on cycles and poles of zeta functions) is known for Fermat surfaces and this allows us to deduce it for $\mathcal{E}$. (The conjecture of Birch and Swinnerton-Dyer for E is equivalent to the Tate conjecture for $\mathcal{E}$.) Also, the detailed analysis of the birational isomorphism between F_d/Γ and $\mathcal{E}$ allows us to express the zeta function of $\mathcal{E}$ in terms of that of F_d which was calculated by Weil in terms of Gauss sums. Finally, an explicit calculation of Gauss sums allows us to show that the zeta function of $\mathcal{E}$ has a large order pole at $s = 1$, and therefore $E(K)$ has large rank.

1.8. One of the key ideas of the proof, namely relating $\mathcal{E}$ to a Fermat surface, is due to Shioda. In [Shi86, Section 5], he exhibited (non-isotrivial) elliptic curves E_n ($n \geq 1$ an integer) defined over $\mathbb{F}_p(t)$ (with $p \equiv 3 \pmod 4$) which are related in a similar way to Fermat surfaces. This allowed him to calculate the rank of E_n over $\overline{\mathbb{F}}_p(t)$ and thus to show that it tends to infinity with n. (In fact, it is not difficult to see that Shioda's curves achieve their full rank over $\mathbb{F}_{p^{2n}}(t)$, i.e., $E_n(\mathbb{F}_{p^{2n}}(t)) = E_n(\overline{\mathbb{F}}_p(t))$.) The methods of this paper can be used to show that the rank of $E_n(\mathbb{F}_p(t))$ also tends to infinity (although in general, $E_n(\mathbb{F}_p(t))$ has smaller rank than $E_n(\overline{\mathbb{F}}_p(t))$).

1.9. Our theorem says that $E(K)$ has large rank, but the proof does not explicitly produce any points. Exhibiting explicit points, and computing invariants such as the height pairing, looks like an interesting project. Do these Mordell-Weil lattices have high densities or other special properties?

1.10. It is a pleasure to thank Felipe Voloch for bringing Shioda's paper [Shi86] to my attention, Pavlos Tzermias for his help with p-adic Gamma functions and the Gross-Koblitz formula, and Dinesh Thakur for a number of useful remarks.

2. Invariants of E

2.1. We work in somewhat greater generality than in the introduction. Let k be a perfect field (of characteristic $p = 0$ or a prime) and set $K = k(t)$. Fix a positive integer d which is not divisible by p. Let E_d be the elliptic curve over K with plane cubic model

$$y^2 + xy = x^3 - t^d. \tag{2.1.1}$$

We will usually drop d from the notation and write E for E_d.

2.2. Straightforward calculation shows that the discriminant of this model is $\Delta = t^d(1 - 2^4 3^3 t^d)$ and $j(E) = 1/\Delta$. Thus E has good reduction at all places of K except $t = 0$, the divisors of $(1 - 2^4 3^3 t^d)$ and possibly $t = \infty$.

Applying Tate's algorithm ([Tat75]), we see that at $t = 0$, E has split multiplicative reduction of type I_d and all geometric components of the special fiber are rational over k. At places v dividing $(1 - 2^4 3^3 t^d)$, E has multiplicative reduction of type I_1; the tangent directions at the node are rational over $k_v(\mu_4)$ where k_v is the residue field at v and μ_4 denotes the 4th roots of unity.

2.3. The reduction type of E at $t = \infty$ depends on $d \pmod 6$ and on k. Write $d = 6a - b$ where $0 \le b < 6$. Changing coordinates via $x = t^{2a}x'$, $y = t^{3a}y'$, and $t = t'^{-1}$ we have the model

$$y'^2 + t'^a x' y' = x'^3 - t'^b.$$

Applying Tate's algorithm, we find the data in the following table.

b	0	1	2	3	4	5
Reduction	I	II	IV	I_0^*	IV^*	II^*
c	1	1	1 if $\mu_4 \not\subset k$ 3 if $\mu_4 \subset k$	2 if $\mu_3 \not\subset k$ 4 if $\mu_3 \subset k$	1 if $\mu_4 \not\subset k$ 3 if $\mu_4 \subset k$	1
n	1	1	2 if $\mu_4 \not\subset k$ 3 if $\mu_4 \subset k$	4 if $\mu_3 \not\subset k$ 5 if $\mu_3 \subset k$	5 if $\mu_4 \not\subset k$ 7 if $\mu_4 \subset k$	9

Here c is the number of geometric components of multiplicity 1 in the special fiber which are k-rational and n is the number of irreducible components of the special fiber as a scheme over k.

The exponent of the conductor at $t = \infty$ is 0 if $b = 0$; 2 if $b > 0$ and $p \nmid 6$; and $d + 2$ if $p|6$.

3. Construction of $\mathcal{E}$

3.1. As before, we let k be a perfect field of characteristic p (possibly 0), $K = k(t)$, and E the elliptic curve over K defined by Equation 2.1.1. Our purpose in this section is to construct the unique elliptic surface $\pi : \mathcal{E} \to \mathbb{P}^1$ over k such that $\mathcal{E}$ is regular and π is proper, flat, and relatively minimal, with generic fiber $E \to \operatorname{Spec} K$. We also relate the Néron-Severi group of $\mathcal{E}$ to the Mordell-Weil group $E(K)$.

3.2. To that end, let U be the closed subset of $\mathbb{P}^2 \times \mathbb{A}^1$ over k defined by the equation

$$y^2z + xyz - x^3 + z^3t^d = 0$$

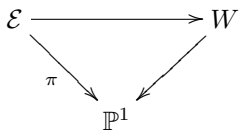
where x, y, and z are the coordinates on $\mathbb{P}^2$ and t is the coordinate on $\mathbb{A}^1$. Similarly, define $U' \subset \mathbb{P}^2 \times \mathbb{A}^1$ by the equation

$$y'^2z' + t'^a x'y'z' - x'^3 + z'^3t'^b = 0$$

where $d = 6a - b$ with $0 \le b < 6$.

Let W be the result of glueing $U \setminus \{t = 0\}$ and $U' \setminus \{t' = 0\}$ via the identification $([x', y', z'], t') = ([t^{-2a}x, t^{-3a}y, z], t^{-1})$. ($W$ stands for "Weierstrass model.") Projection onto the t or t' coordinate gives a proper, flat, and relatively minimal morphism $W \to \mathbb{P}^1$ whose fibers are the naive reductions of E at places of K. However, W may not be regular; there are singularities at the point $([0, 0, 1], 0)$ in U if $d > 1$, and at $([0, 0, 1], 0)$ in U' if $b > 1$. We note that W is a local complete intersection and non-singular in codimension 1, so is normal.

3.3. To resolve the singularity in U we must blow up W $\lfloor d/2 \rfloor$ times. The fiber over $t = 0$ is then a chain of d rational curves meeting transversally, i.e., it is the fiber in the Néron model of E at $t = 0$. Tate's algorithm gives the recipe for resolving the singularity in U'. The fiber over $t = \infty$ was recorded in the previous section. We denote by $\mathcal{E}$ the result of this desingularization. We have a commutative diagram



where $\mathcal{E} \to W$ is a birational isomorphism and the maps to $\mathbb{P}^1$ are proper, flat, and relatively minimal. The map π admits a canonical section, the "0-section," defined in the U coordinates by $t \mapsto ([0, 1, 0], t)$.

3.4. Let $\overline{\mathcal{E}} = \mathcal{E} \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. The Néron-Severi group $NS(\overline{\mathcal{E}})$ is by definition the group of divisors on $\overline{\mathcal{E}}$ modulo algebraic equivalence. The "theorem of the base" asserts that this is a finitely generated abelian group. The Néron-Severi group of $\mathcal{E}$ is by definition the image of the group of divisors on $\mathcal{E}$ in $NS(\overline{\mathcal{E}})$. I.e., it is the group of (k-rational) divisors on $\mathcal{E}$ modulo algebraic equivalence over $\overline{k}$. (If k is finite, $NS(\mathcal{E})$ is the set of $\operatorname{Gal}(\overline{k}/k)$-invariant elements of $NS(\overline{\mathcal{E}})$.)

3.5. Let $L \subset NS(\mathcal{E})$ be the subgroup generated by the the class of the 0-section and classes of divisors supported in fibers of π. The formula of Tate and Shioda ([Tat66, Shi72]) says that

$$\begin{aligned}\operatorname{Rank} E(K) &= \operatorname{Rank} NS(\mathcal{E}) - \operatorname{Rank} L \\ &= \operatorname{Rank} NS(\mathcal{E}) - 2 - \sum_v (n_v - 1)\end{aligned}$$

where the sum is over all closed points of $\mathbb{P}^1_k$ and n_v is the number of irreducible components of the fiber at v.

Although they are not strictly necessary for our purposes, the following remarks may help to clarify this formula. We have an exact sequence

$$0 \to L \to NS(\mathcal{E}) \to E(K) \to 0$$

where the map $NS(\mathcal{E}) \to E(K)$ can be defined as follows: given a divisor on $\mathcal{E}$, take its intersection with the generic fiber E and add the resulting points in $E(K)$. With some work, this can be shown to be well-defined with kernel L.

There is a section $s : E(K) \to NS(\mathcal{E})$ which sends a point in $E(K)$ to its closure in $\mathcal{E}$. But note that this section is not in general a homomorphism. (There is a canonical section after tensoring the exact sequence with $\mathbb{Q}$ which makes $NS(\mathcal{E}) \otimes \mathbb{Q}$ the orthogonal direct sum, with respect to the intersection pairing, of $L \otimes \mathbb{Q}$ and $E(K) \otimes \mathbb{Q}$.) The exact sequence is equivalent to the assertion that that $s(E(K))$ is a set of coset representatives for L in $NS(\mathcal{E})$. See [MP86] for more details.

The Shioda-Tate formula will allow us to compute the rank of $E(K)$ in terms of $NS(\mathcal{E})$, which we will eventually compute using the Tate conjecture.

3.6. We will want to consider the situation for different degrees, so we write U_d, U'_d, W_d and $\mathcal{E}_d$ for the surfaces considered in this section; we then have similar definitions where d is replaced by 1. Note that there is a finite morphism $W_d \to W_1$ defined in the U coordinates by $([x, y, z], t) \mapsto ([x, y, z], t^d)$.

4. Fermat surfaces

4.1. In this section we will make a connection between Fermat surfaces and the elliptic surface $\mathcal{E}$.

Let F_d be the Fermat surface of degree d, i.e., the hypersurface in $\mathbb{P}^3$ defined by

$$x_0^d + x_1^d + x_2^d + x_3^d = 0.$$

We write μ_d for the group of d-th roots of unity in $\overline{k}$. Let $G \subset \operatorname{Aut}_{\overline{k}}(F_d)$ be the quotient of ${\mu_d}^4$ modulo a diagonally embedded copy of μ_d. The action on F_d is

$$z \cdot x = [\zeta_0, \zeta_1, \zeta_2, \zeta_3] \cdot [x_0, x_1, x_2, x_3] = [\zeta_0 x_0, \zeta_1 x_1, \zeta_2 x_2, \zeta_3 x_3].$$

The canonical morphism $F_d \to F_1$ ($[x_0, x_1, x_2, x_3] \mapsto [x_0^d, x_1^d, x_2^d, x_3^d]$) induces an isomorphism $F_d/G \cong F_1 \cong \mathbb{P}^2$.

4.2. We define dominant rational maps $F_d \dashrightarrow W_d$ and $W_d \dashrightarrow F_1$ using the U_d coordinates as follows:

$$[x_0, x_1, x_2, x_3] \mapsto \left([(x_0 x_1 x_2)^d, (x_0^2 x_2)^d, -x_1^{3d}], \frac{x_0^3 x_2^2 x_3}{x_1^6} \right)$$

and

$$([x, y, z], t) \mapsto [y^2 z, xyz, -x^3, z^3 t^d].$$

The rational map $W_d \dashrightarrow F_1$ factors as $W_d \to W_1 \dashrightarrow F_1$ and $W_1 \dashrightarrow F_1$ is a birational isomorphism (with inverse $[x_0,x_1,x_2,x_3] \mapsto ([x_0x_1x_2, x_0^2x_2, -x_1^3], x_0^3x_2^2x_3/x_1^6)$) and so $W_d \dashrightarrow F_1$ has generic degree d. Also, the composition $F_d \dashrightarrow W_d \dashrightarrow F_1$ is the canonical morphism $F_d \to F_1$ which has degree d^3, so $F_d \dashrightarrow W_d$ has generic degree d^2.

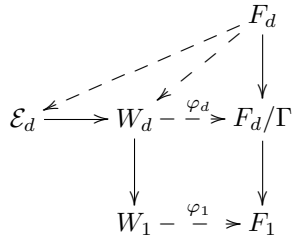
4.3. Fix a primitive d-th root $\zeta \in \overline{k}$ and let $\Gamma \subset G$ be the subgroup generated by $[\zeta^2,\zeta,1,1]$ and $[1,\zeta,\zeta^3,1]$, which can also be described as

$$\Gamma = \left\{ [\zeta_0,\zeta_1,\zeta_2,\zeta_3] \,\middle|\, \zeta_0^3\zeta_1^{-6}\zeta_2^2\zeta_3 = 1 \right\}.$$

It is evident from the definitions that the rational map $F_d \dashrightarrow W_d$ factors through F_d/Γ. Considering degrees, we see that the induced map $F_d/\Gamma \dashrightarrow W_d$ is a birational isomorphism. We denote its inverse by $\varphi_d : W_d \dashrightarrow F_d/\Gamma$.

Note that since F_d is regular, and thus normal, F_d/Γ is normal.

To summarize, we have the following commutative diagram, where the vertical arrows are finite surjective morphisms, the horizontal arrows are birational isomorphisms, and the diagonal arrows are dominant rational maps.



The surfaces W_d, W_1, and F_d/Γ are normal, whereas F_d, $\mathcal{E}_d$, and F_1 are regular.

5. Analysis of φ_d

5.1. We will eventually compute the zeta-function of $\mathcal{E}_d$ in terms of that of F_d. In order to do this, we need some detailed geometric information about $\varphi_d : W_d \dashrightarrow F_d/\Gamma$. Specifically, we need to find explicit closed sets to be removed from W_d and F_d/Γ so that φ_d induces an isomorphism on the remaining open sets. Attacked directly, this computation could be rather unpleasant, since we would need equations for F_d/Γ.

To avoid this problem, we prove a lemma which could be phrased colloquially as saying that "a rational map from a normal variety is defined at a point if and only if its composition with a finite map is."

5.2. Lemma. *Let W, X, Y, and Z be varieties over k (separated integral schemes of finite type over k) and assume that X is normal. Let $g : X \dashrightarrow Y$ be a rational map and let $f : W \to X$ and $h : Y \to Z$ be finite morphisms, with f surjective.*

1. *$g \circ f$ is defined at $w \in W$ if and only if g is defined at $f(w)$.*
2. *g is defined at $x \in X$ if and only if $h \circ g$ is defined at x.*

Proof. We may assume that all our varieties are affine, say $W = \operatorname{Spec} R$, $X = \operatorname{Spec} S$, $Y = \operatorname{Spec} T$, and $Z = \operatorname{Spec} U$, and that we have homomorphisms $g^* : T \to S[1/s]$ for some $s \in S$ and $f^* : S \to R$, and $h^* : U \to T$. The hypotheses imply that R, S, T, and U are domains, S is integrally closed, R is integral over $f^*(S)$, T is integral over $h^*(U)$ and f^* is injective.

To prove 1, we must show that $(g\circ f)^*$ factors through R if and only if g^* factors through S. The "if" direction is trivial. For the converse, take $t \in T$ and write down an equation of integrality for $f^*(g^*(t))$ over $f^*(S)$:

$$f^*(g^*(t))^n + f^*(s_1)f^*(g^*(t))^{n-1} + \cdots + f^*(s_n) = 0.$$

Since f^* is injective, this implies

$$g^*(t)^n + s_1 g^*(t)^{n-1} + \cdots + s_n = 0.$$

But S is integrally closed and $g^*(t) \in S[1/s]$, so $g^*(t) \in S$.

To prove 2, we must show that $(h\circ g)^*$ factors through S if and only if g^* factors through S. Again the "if" direction is trivial. For the converse, take $t \in T$ and write down an equation of integrality over $h^*(U)$:

$$t^n + h^*(u_1)t^{n-1} + \cdots + h^*(u_n) = 0.$$

Applying g^* we have an equation of integrality for $g^*(t)$ over $(h\circ g)^*(U) \subset S$. Since S is integrally closed and $g^*(t) \in S[1/s]$, we have $g^*(t) \in S$.

□

5.3. Corollary. *Consider a diagram of varieties*

$$\begin{array}{ccc} \tilde{X} & \overset{\tilde{\phi}}{\dashrightarrow} & \tilde{Y} \\ {\scriptstyle \pi_X}\downarrow & & \downarrow{\scriptstyle \pi_Y} \\ X & \overset{\phi}{\dashrightarrow} & Y \end{array}$$

where the vertical arrows are finite surjective morphisms, the horizontal arrows are dominant rational maps and $\tilde{X}$ and $\tilde{Y}$ are normal. If $V \subset X$ and $V' \subset Y$ are open subsets such that ϕ induces a biregular isomorphism $\phi : V \tilde{\to} V'$, then $\tilde{\phi}$ induces a biregular isomorphism from $\tilde{V} = \pi_X^{-1}(V)$ to $\tilde{V}' = \pi_Y^{-1}(V')$.

Proof. By the trivial half of part 1 of the lemma, $\phi\circ\pi_X$ is defined on $\tilde{V}$, thus $\pi_Y \circ \tilde{\phi}$ is defined there as well. Part 2 of the lemma then implies that $\tilde{\phi}$ is defined on $\tilde{V}$. Similarly, $\tilde{\phi}^{-1}$ is defined on $\tilde{V}'$. Obviously $\tilde{\phi}(\tilde{V}) \subset \tilde{V}'$ and $\tilde{\phi}^{-1}(\tilde{V}') \subset \tilde{V}$. Since $\tilde{\phi}^{-1} \circ \tilde{\phi} : \tilde{V} \to \tilde{V}$ and $\tilde{\phi} \circ \tilde{\phi}^{-1} : \tilde{V}' \to \tilde{V}'$ represent the rational maps $id_{\tilde{X}}$ and $id_{\tilde{Y}}$, they must be the identity maps. □

5.4. Now we apply the corollary to the diagram

$$\begin{array}{ccc} W_d & \overset{\varphi_d}{\dashrightarrow} & F_d/\Gamma \\ \downarrow & & \downarrow \\ W_1 & \overset{\varphi_1}{\dashrightarrow} & F_1. \end{array}$$

The rational map φ_1 is defined in the U_1 coordinates by

$$\varphi_1([x,y,z],t) = [y^2z, xyz, -x^3, z^3t]$$

and φ_1^{-1} is defined by

$$\varphi_1^{-1}([x_0,x_1,x_2,x_3]) = ([x_0x_1x_2, x_0^2x_2, -x_1^3], \frac{x_0^3x_2^2x_3}{x_1^6}).$$

We let $V \subset W_1$ be the subset of U_1 where $xyz \neq 0$ and let $V' \subset F_1$ be the subset where $x_0x_1x_2 \neq 0$. It is easy to see that φ_1 is defined on V, φ_1^{-1} is defined on V',

and they are inverse morphisms. We conclude that φ_d maps the subset of U_d where $xyz \neq 0$ isomorphically onto a certain subset of F_d/Γ which will be described in the next subsection.

5.5. Consider the projection morphisms $F_d \to F_d/\Gamma \to F_1$. The subset $x_0x_1x_2 = 0$ of F_1 has 3 irreducible components, all lines. Its inverse image in F_d consists of 3 irreducible curves (Fermat curves of degree d). It follows that the inverse image of $x_0x_1x_2 = 0$ in F_d/Γ is also the union of 3 irreducible curves. Thus the open set $V' \subset F_d/\Gamma$ of the preceding subsection is the complement of the union of 3 irreducible curves.

5.6. Now we consider the open subset $V \subset W_d$. It is obtained from W_d by removing the subset where $t' = 0$ from U'_d, as well as the subset where $xyz = 0$ from U_d.

The subset of U'_d where $t' = 0$ is an irreducible curve.

The subset $\{x = 0\} = \{x = 0 = y^2z + z^3t^d\}$ of U_d consists of the zero section ($z = 0$) and 1 or 2 other components, 1 if d is odd or $\mu_4 \not\subset k$ and 2 if d is even and $\mu_4 \subset k$.

The subset $\{y = 0\} = \{y = 0 = x^3 - z^3t^d\}$ of U_d is irreducible if $3 \nmid d$, it has 2 components if $3|d$ and $\mu_3 \not\subset k$, and it has 3 components if $3|d$ and $\mu_3 \subset k$.

The subset where $z = 0$ is contained in the subset where $x = 0$.

In summary, V is obtained from W_d by removing a closed subset which is a union of curves. The number of irreducible components of this union is

$$1 + \begin{cases} 2 & \text{if } 2 \nmid d \text{ or } \mu_4 \not\subset k \\ 3 & \text{if } 2|d \text{ and } \mu_4 \subset k \end{cases} + \begin{cases} 1 & \text{if } 3 \nmid d \\ 2 & \text{if } 3|d \text{ and } \mu_3 \not\subset k \\ 3 & \text{if } 3|d \text{ and } \mu_3 \subset k. \end{cases}$$

5.7. We only used the trivial half of part 1 of the lemma. We included the other half because it is of use if one wants to analyze φ_d using the rational map $F_d \dashrightarrow W_d$.

6. The Tate conjecture

From now on, we take k to be $\mathbb{F}_q$, the field of q elements, where q is a power of p.

6.1. Let X be a variety over $\mathbb{F}_q$. The zeta function of X is by definition

$$\zeta(X, s) = \prod_x \frac{1}{1 - q^{-\deg(x)s}}$$

where the product is over all closed points of X and $\deg(x)$ is the degree of the residue field at x as an extension of $\mathbb{F}_q$. (For our purposes it is enough to view this as a formal series in q^{-s}.) Alternatively, $\zeta(X, s) = Z(X, q^{-s})$ where

$$Z(X, T) = \exp\left(\sum_{n=1}^{\infty} \frac{N_n T^n}{n}\right)$$

and N_n is the number of points on X rational over $\mathbb{F}_{q^n}$.

It is immediate from the definition that the zeta function is multiplicative for disjoint unions: if $X = X_1 \cup X_2$ is a disjoint union, then $\zeta(X, s) = \zeta(X_1, s)\zeta(X_2, s)$.

It is a theorem of Dwork that $Z(X,T)$ is a rational function of T. We will need the deeper connection with cohomology. Fix a prime $\ell \neq p$ and write $H^i(X)$ for the ℓ-adic étale cohomology group $H^i_{\text{ét}}(X \times_{\operatorname{Spec} \mathbb{F}_q} \operatorname{Spec} \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$. Then

$$Z(X,T) = \prod_{i=0}^{2\dim X} \det\left(1 - Fr^*\, T | H^i(X)\right)^{(-1)^{i+1}} \tag{6.1.1}$$

where $Fr : X \to X$ is the q-power Frobenius endomorphism.

Deligne's proof of the Weil conjectures implies that when X is smooth and proper over $\mathbb{F}_q$, the eigenvalues of Fr^* on $H^i(X)$ are algebraic numbers independent of ℓ and have absolute value $q^{i/2}$ in any complex embedding.

6.2. Now assume that X is a smooth and proper variety over $\mathbb{F}_q$. The Néron-Severi group $NS(X)$ is defined to be the group of divisors on X modulo algebraic equivalence over $\overline{\mathbb{F}}_q$. There is a cycle class map $NS(X) \to H^2(X)$ which induces an injection $NS(X) \otimes \mathbb{Q}_\ell \to H^2(X)^{Fr=q}$ where the exponent signifies the subspace where Fr^* acts by multiplication by q. This, together with the cohomological description of zeta functions, gives inequalities

$$\operatorname{Rank} NS(X) \leq \dim_{\mathbb{Q}_\ell} H^2(X)^{Fr=q} \leq -\operatorname{ord}_{s=1} \zeta(X,s). \tag{6.2.1}$$

The Tate conjecture ([Tat65]) asserts that these are all equalities. We will refer to this assertion as "(T) for X." (It would be more precise to refer to this as (T1), since there are conjectures for cycles of every codimension, but we will not need the others. Also, there are refined conjectures relating the leading coefficient of the Taylor expansion of $\zeta(X,s)$ at $s=1$ to other invariants of X.)

6.3. In the case where $X \to \mathcal{C}$ is an elliptic surface over $\mathbb{F}_q$ with a section (so that the generic fiber is an elliptic curve E over the function field $K = \mathbb{F}_q(\mathcal{C})$), the Tate conjecture for X is equivalent to the Birch and Swinnerton-Dyer conjecture for E. (More precisely (T) for X implies that $\operatorname{Rank} E(K) = \operatorname{ord}_{s=1} L(E/K,s)$. Moreover, Tate proved ([Tat66]) that when (T) holds the refined conjecture of Birch and Swinnerton-Dyer on the leading Taylor coefficient of $L(E/K,s)$ is true up to a power of p. Milne showed ([Mil75]) that the full refined conjecture is true at least if $p \neq 2$. We only need the rank conjecture.)

Still assuming that X is an elliptic surface, the cohomological expression 6.1.1 for the zeta function and the Euler characteristic formula of Grothendieck, Ogg, and Shafarevitch lead to an upper bound on $\operatorname{ord}_{s=1} L(E/K,s)$ and thus also to an upper bound on $\operatorname{Rank} E(K)$. If g is the genus of $\mathcal{C}$ and $\mathfrak{n}$ is the conductor of E (an effective divisor on $\mathcal{C}$), then we have

$$\operatorname{ord}_{s=1} L(E/K,s) \leq 4g - 4 + \deg(\mathfrak{n})$$

if E/K is non-constant, and

$$\operatorname{ord}_{s=1} L(E/K,s) \leq 4g$$

if E/K is constant. These bounds are "geometric" in that they are insensitive to the finite field $\mathbb{F}_q$. As we will explain in Section 10, there exists a more refined arithmetic bound, and asymptotically this bound is met by the curves in Theorem 1.5.

6.4. Proposition. *Let E be the elliptic curve over $\mathbb{F}_q(t)$ defined by Equation 2.1.1, let $\mathcal{E}$ be the elliptic surface over $\mathbb{F}_q$ defined in Section 3, and let F_d/Γ be the quotient of the Fermat surface of degree d over $\mathbb{F}_q$ defined in Section 4.*

(1) *The Tate conjecture holds for $\mathcal{E}$. Equivalently, the conjecture of Birch and Swinnerton-Dyer holds for E.*
(2) $\operatorname{Rank} E(\mathbb{F}_q(t)) = -\operatorname{ord}_{s=1}\zeta(F_d/\Gamma, s) - 1 + \epsilon$ *where*

$$\epsilon = \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } 4 \nmid q-1 \\ 1 & \text{if } 2|d \text{ and } 4|q-1 \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \\ 1 & \text{if } 3|d \text{ and } 3 \nmid q-1 \\ 2 & \text{if } 3|d \text{ and } 3|q-1. \end{cases}$$

6.5. Remark. The ϵ term accounts for the points on E with either $x = 0$ or $y = 0$.

Proof. Part 1 follows from the existence of a dominant rational map $F_d \dashrightarrow \mathcal{E}$ and well-known results on the Tate conjecture. (We refer to [Tat94], especially Section 5 for these results.) Indeed, if $X \dashrightarrow Y$ is a dominant rational map, (T) for X implies (T) for Y. But (T) is trivial for curves, and its truth for two varieties implies it for their product. Since a Fermat variety is dominated by a product of curves ([SK79]), (T) follows for Fermat varieties, and this implies (T) for $\mathcal{E}$.

The equivalence of (T) for $\mathcal{E}$ and the conjecture of Birch and Swinnerton-Dyer for E was already noted above.

To prove 2, we use the geometric analysis of Section 5 and the multiplicativity of zeta functions. From the Shioda-Tate formula (Subsection 3.5) and Part 1 we have

$$\begin{aligned} \operatorname{Rank} E(K) &= \operatorname{Rank} NS(\mathcal{E}) - \operatorname{Rank} L \\ &= -\operatorname{ord}_{s=1}\zeta(\mathcal{E}, s) - \operatorname{Rank} L. \end{aligned}$$

Since $\mathcal{E}$ is obtained from W by blowing up, i.e., by removing points and adding curves, multiplicativity of zeta functions yields that

$$\begin{aligned} -\operatorname{ord}_{s=1}\zeta(\mathcal{E}, s) &= -\operatorname{ord}_{s=1}\zeta(W, s) + \sum_v (n_v - 1) \\ &= -\operatorname{ord}_{s=1}\zeta(W, s) + \operatorname{Rank} L - 2 \end{aligned}$$

where n_v is the number of irreducible components in the fibre at v. Combining multiplicativity with the geometric analysis of Section 5 shows that

$$-\operatorname{ord}_{s=1}\zeta(W, s) - 4 - \epsilon = -\operatorname{ord}_{s=1}\zeta(F_d/\Gamma, s) - 3.$$

Assembling these ingredients gives the desired formula. □

6.6. Note that we did not need the actual values of n_v in the proof, since they cancel out. Nevertheless, we recorded them in Section 2 for future use, e.g., for height computations.

7. The zeta function of a Fermat surface

7.1. The zeta functions of Fermat varieties were computed in terms of Gauss and Jacobi sums by Weil in his landmark paper [Wei49]. We will need a refinement of this calculation due to Shioda which takes into account the action of G, and we will need to make the relevant Jacobi sums explicit. Remarkably, an explicit calculation of zeta functions of Fermat varieties *over the prime field* does not seem to be in the literature. When doing explicit calculations, most authors pass immediately to the case where $q \equiv 1 \mod d$. In the next two sections, we will explicitly compute the zeta function of F_d/Γ over any finite field $\mathbb{F}_q$, in the "supersingular" case, i.e., when d divides $p^n + 1$ for some positive integer n.

7.2. We will use the cohomological description

$$\zeta(X,s) = Z(X,q^{-s}) = \prod_{i=0}^{2\dim X} P_i(X,q^{-s})^{(-1)^{i+1}}$$

where

$$P_i(X,T) = \det\left(1 - Fr^*\, T | H^i(X)\right).$$

Since $H^i(F_d/\Gamma) = H^i(F_d)^\Gamma$ and the eigenvalues of Frobenius on $H^i(F_d)$ have absolute value $q^{i/2}$, only $P_2(F_d/\Gamma, q^{-s})$ can contribute to the order of pole of $\zeta(F_d/\Gamma, s)$ at $s = 1$. Thus we will concentrate on $H^2(F_d)$ and its Γ invariants.

7.3. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_{\overline{\mathbb{Q}}}$, the ring of integers of $\overline{\mathbb{Q}}$, over p. We view all finite fields of characteristic p as subfields of $\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p}$, which is an algebraic closure of $\mathbb{F}_p$.

Reduction modulo $\mathfrak{p}$ induces an isomorphism between the group of all roots of unity of order prime to p in $\mathcal{O}_{\overline{\mathbb{Q}}}$ and the multiplicative group of $\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p}$. We let $t : (\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p})^\times \to \overline{\mathbb{Q}}^\times$ denote the inverse of this isomorphism. We will use the same letter t for the restriction to any finite field ${\mathbb{F}_q}^\times$.

Fix an algebraic closure $\overline{\mathbb{Q}}_\ell$ of $\mathbb{Q}_\ell$ and an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. For convenience, we will assume that $\ell \equiv 1 \mod pd$ so that $\mathbb{Q}_\ell$ contains all the pd-th roots of unity.

7.4. Now we introduce Gauss and Jacobi sums. Fix a non-trivial character $\psi_0 : \mathbb{F}_p \to \overline{\mathbb{Q}}^\times$ and for each finite extension $\mathbb{F}_{p^f}$ of $\mathbb{F}_p$, let $\psi : \mathbb{F}_{p^f} \to \overline{\mathbb{Q}}^\times$ be defined by $\psi = \psi_0 \circ \mathrm{Tr}_{\mathbb{F}_{p^f}/\mathbb{F}_p}$. If $\chi : {\mathbb{F}_{p^f}}^\times \to \overline{\mathbb{Q}}^\times$ is a non-trivial character, we define a Gauss sum by

$$g(\chi,\psi) = -\sum_{x \in {\mathbb{F}_{p^f}}^\times} \chi(x)\psi(x).$$

If $\chi_1, \ldots, \chi_n$ are characters ${\mathbb{F}_{p^f}}^\times \to \overline{\mathbb{Q}}^\times$, not all trivial, such that the product $\chi_1 \cdots \chi_n$ is trivial, we define a Jacobi sum by

$$J(\chi_1,\ldots,\chi_n) = \frac{1}{p^f - 1} \sum_{\substack{x_1,\ldots,x_n \in {\mathbb{F}_{p^f}}^\times \\ x_1+\cdots+x_n=0}} \chi_1(x_1)\cdots\chi_n(x_n).$$

It is well-known (see [Wei49] for example) that

$$J(\chi_1,\ldots,\chi_n) = \begin{cases} \frac{(-1)^n}{p^f} \prod_{i=1}^n g(\chi_i,\psi) & \text{if all } \chi_i \text{ are non-trivial} \\ 0 & \text{otherwise} \end{cases}$$

and that (in any complex embedding) $|g(\chi,\psi)| = p^{f/2}$.

7.5. Recall the group G of automorphisms of F_d introduced in Section 4. Let $\hat{G}$ denote the group of characters G with values in $\overline{\mathbb{Q}}$ (and thus also $\overline{\mathbb{Q}}_\ell$ via our fixed embedding). Using the character $t : (\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p})^\times \to \overline{\mathbb{Q}}^\times$, we can identify $\hat{G}$ with

$$\left\{ a = (a_0,a_1,a_2,a_3) \in (\mathbb{Z}/d\mathbb{Z})^4 \,\middle|\, \sum a_i = 0 \right\}$$

where the pairing $G \times \hat{G} \to \overline{\mathbb{Q}}^\times$ is

$$a(z) = \langle (a_0, a_1, a_2, a_3), [\zeta_0, \zeta_1, \zeta_2, \zeta_3] \rangle = \prod_{i=0}^{3} t(\zeta_i)^{a_i}.$$

Note that by our assumption that $\ell \equiv 1 \mod pd$, the values of $a \in \hat{G}$ lie in $\mathbb{Q}(\mu_d) \subset \mathbb{Q}_\ell$.

For $a \in \hat{G}$, we denote by $H^2(F_d)(a)$ the subspace of classes $c \in H^2(F_d)$ such that $z^*(c) = a(z)c$ for all $z \in G$. Also, we write qa for $(qa_0, \dots, qa_3)$ if $a = (a_0, \dots, a_3)$.

Recall that $Fr : F_d \to F_d$ denotes the q-power Frobenius endomorphism. From the formula

$$Fr \circ [\zeta_0, \zeta_1, \zeta_2, \zeta_3] = [\zeta_0^q, \zeta_1^q, \zeta_2^q, \zeta_3^q] \circ Fr$$

we deduce that Fr^* sends $H^2(F_d)(a)$ to $H^2(F_d)(qa)$. For each $a \in \hat{G}$, we let $u(a)$ denote the smallest positive integer such that $q^{u(a)}a = a$. Then $(Fr^{u(a)})^*$ maps $H^2(F_d)(a)$ to itself.

It turns out that $H^2(F_d)(a)$ is zero or 1-dimensional, and $(Fr^{u(a)})^*$ acts by multiplication by a Jacobi sum. More precisely, for $a \in \hat{G}$, $a \neq 0$, define a Jacobi sum $J(a)$ as follows: Let $\chi_i : \mathbb{F}_{q^{u(a)}}^\times \to \overline{\mathbb{Q}}$ be defined as $\chi_i = t^{\frac{q^{u(a)}-1}{d} a_i}$ and set $J(a) = J(\chi_0, \dots, \chi_3)$. Note that $J(qa) = J(a)$. By convention, we set $J(0) = q$.

7.6. Proposition. (Shioda) *Let F_d be the Fermat surface of degree d over $\mathbb{F}_q$ and let $\hat{G}' = \{a = (a_0, \dots, a_3) \in \hat{G} \mid a = 0 \text{ or } a_i \neq 0 \text{ for } i = 0, \dots 3\}$.*

1. *$H^2(F_d)(a)$ is zero if $a \notin \hat{G}'$ and is 1-dimensional if $a \in \hat{G}'$.*
2. *If $a \in \hat{G}'$ then $(Fr^{u(a)})^*$ acts on $H^2(F_d)(a)$ by multiplication by $J(a)$.*
3. *If $a \in \hat{G}'$ then the characteristic polynomial of Fr^* on $\bigoplus_{i=0}^{u(a)-1} H^2(F_d)(q^i a)$ is equal to $(1 - J(a)T^{u(a)})$.*

Proof. In [SK79], Shioda and Katsura show that the cohomology of a Fermat variety is built up from the cohomology of lower dimensional Fermat varieties of the same degree. This allows one to reduce to the case of curves. The proposition for Fermat curves is [Kat81, Cor. 2.4].

We will sketch another proof, closely related to that in [Kat81], which works uniformly in all dimensions. For simplicity we will only discuss the case of Fermat surfaces.

To that end, consider the finite morphism $\pi : F_d \to F_d/G \cong \mathbb{P}^2$. The sheaf $\mathcal{F} = \pi_* \mathbb{Q}_\ell$ carries a natural action of G and we have a decomposition $\mathcal{F} = \oplus_{a \in \hat{G}} \mathcal{F}(a)$. By the Leray spectral sequence for π, $H^2(F_d)(a) = H^2_{\text{ét}}(\mathbb{P}^2 \times \operatorname{Spec} \overline{\mathbb{F}}_q, \mathcal{F})(a) = H^2_{\text{ét}}(\mathbb{P}^2 \times \operatorname{Spec} \overline{\mathbb{F}}_q, \mathcal{F}(a))$.

Now each $\mathcal{F}(a)$ is lisse of rank 1 on the locus $\{[y_0, \dots, y_3] | y_i \neq 0 \text{ if } a_i \neq 0\} \subset \mathbb{P}^2$ and is zero elsewhere. If $r = q^f$ is a power of $q^{u(a)}$ and y is an $\mathbb{F}_r$-rational point of $\mathbb{P}^2$ with corresponding Frobenius $Fr_y = Fr^f$, then Fr_y induces an automorphism of the geometric stalk, $Fr_y : \mathcal{F}(a)_{\overline{y}} \to \mathcal{F}(a)_{\overline{y}}$. We have $\operatorname{Tr} Fr_y | \mathcal{F}(a)_{\overline{y}} = \chi_{a,r}(y)$

where $\chi_{a,r}$ is defined by

$$\chi_{a,r}([y_0,\dots,y_3]) = \prod_{i=0}^{3} t^{\frac{r-1}{d}a_i}(y_i)$$
$$= \prod_{i=0}^{3} t^{\frac{q^{u(a)}-1}{d}a_i}\left(N_{\mathbb{F}_r/\mathbb{F}_{q^{u(a)}}}(y_i)\right)$$

and we interpret $t^b(0)$ as 0 if $b \neq 0$ and as 1 if $b = 0$.

Using the Grothendieck-Lefschetz trace formula and the Hasse-Davenport relation, we see that

$$\prod_{i=0}^{4} \det\left(1 - (Fr^{u(a)})^* T | H^i(F_d)(a)\right)^{(-1)^{i+1}}$$
$$= \begin{cases} (1-J(a)T)^{-1} & \text{if } a \neq 0 \\ (1-T)^{-1}(1-qT)^{-1}(1-q^2T)^{-1} & \text{if } a = 0. \end{cases}$$

Now Deligne's purity theorem for the $H^i(F_d)$ implies that $H^2(F_d)(a)$ is either 0 or 1-dimensional, and is non-zero if and only if $J(a) \neq 0$, i.e., if and only if $a \in \hat{G}'$. We also see that $(Fr^{u(a)})^*$ acts on $H^2(F_d)(a)$ by multiplication by $J(a)$.

Part 3 is an easy consequence of Part 2. □

The proposition reduces the problem of computing the order of pole of the zeta function of F_d/Γ to computing some Jacobi sums. Let $\Gamma^\perp \subset \hat{G}$ be the set of characters which are trivial on $\Gamma \subset G$. Clearly $\Gamma^\perp$ is the cyclic subgroup of order d generated by $(3, -6, 2, 1)$. With this notation, we have:

7.7. Corollary. *Let $A_1, \dots, A_k$ be the orbits of multiplication by q on $\Gamma^\perp \cap \hat{G}'$ and choose $a_i \in A_i$. Then*

$$P_2(F_d/\Gamma, T) = \prod_{i=1}^{k}(1 - J(a_i)T^{u(a_i)}).$$

8. Explicit Gauss and Jacobi sums

8.1. Proposition. *Suppose that some power of p is congruent to -1 modulo d. Then for all $a \in \hat{G}'$, $J(a) = q^{u(a)}$.*

The rest of this section is devoted to proving the proposition.

8.2. Lemma. *Let b be a rational number with $0 < b < 1$ and suppose that there exist positive integers n and f such that $(p^n+1)b \in \mathbb{Z}$ and $(p^f-1)b \in \mathbb{Z}$. If $b \neq 1/2$ then f is even and setting $e = \gcd(n, f/2)$, we have $(p^e+1)b \in \mathbb{Z}$.*

Proof. Write $b = c/d$ in lowest terms. If $b \neq 1/2$ then $d > 2$. Our assumptions imply that $p^n \equiv -1 \mod d$ and $p^f \equiv 1 \mod d$, and so f must be even since $d > 2$. Now

$$\gcd(p^{2n}-1, p^f-1) = p^{\gcd(2n,f)} - 1 = p^{2e} - 1$$

so $p^{2e} \equiv 1 \mod d$. Since $p^n = (p^e)^{(n/e)} \equiv -1 \mod d$, we must have that n/e is odd and $p^e \equiv -1 \mod d$. Thus $(p^e+1)b \in \mathbb{Z}$, as desired. □

8.3. Lemma. (Shafarevitch-Tate) *Let $\chi : \mathbb{F}_{p^{2f}}^\times \to \overline{\mathbb{Q}}^\times$ be a non-trivial character which is trivial on $\mathbb{F}_{p^f}^\times$. Then $g(\chi,\psi) = -\chi(x)p^f$ where $x \in \mathbb{F}_{p^{2f}}^\times$ is any element with $\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}(x) = 0$.*

Proof. Recall that $\psi(x) = \psi_0(\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_p}(x))$ where ψ_0 is a fixed non-trivial character of $\mathbb{F}_p$. Abbreviating $\mathrm{Tr}_{\mathbb{F}_{p^{2f}}/\mathbb{F}_{p^f}}$ to Tr, we have

$$\begin{aligned} g(\chi,\psi) &= -\sum_{x\in\mathbb{F}_{p^{2f}}^\times} \chi(x)\psi(x) \\ &= -\sum_{x\in\mathbb{F}_{p^{2f}}^\times/\mathbb{F}_{p^f}^\times} \chi(x) \sum_{y\in\mathbb{F}_{p^f}^\times} \psi(xy) \\ &= -\sum_{x\in\mathbb{F}_{p^{2f}}^\times/\mathbb{F}_{p^f}^\times} \chi(x) \begin{cases} p^f-1 & \text{if } \mathrm{Tr}(x)=0 \\ -1 & \text{if } \mathrm{Tr}(x)\neq 0 \end{cases} \\ &= -\sum_{\substack{x\in\mathbb{F}_{p^{2f}}^\times/\mathbb{F}_{p^f}^\times \\ \mathrm{Tr}(x)=0}} \chi(x)p^f. \end{aligned}$$

But $\mathrm{Tr} : \mathbb{F}_{p^{2f}} \to \mathbb{F}_{p^f}$ is $\mathbb{F}_{p^f}$-linear and surjective, so its kernel is a 1-dimensional $\mathbb{F}_{p^f}$-vector space. This means that there is just one term in the last displayed sum, and this proves the lemma. □

Proof of Proposition 8.1. If $a = 0$ then $u(a) = 1$ and $J(a) = q$ by definition. If $a = (d/2, d/2, d/2, d/2)$, then $u(a) = 1$ and $J(a) = g(t^{(q-1)/2},\psi)^4/q$. But it is elementary and well-known that $g(t^{(q-1)/2},\psi) = \pm\sqrt{\pm q}$, and so $J(a) = q$.

Now assume that $a \in \hat{G}'$ and $a \neq 0$, $a \neq (d/2, d/2, d/2, d/2)$. Lemma 8.2, applied to the $b_i = a_i/d$, shows that $u(a)$ is even. Setting $g_i = g(t^{\frac{q^{u(a)}-1}{d}a_i},\psi)$ and $e = \gcd(n, u(a)/2)$ we have

$$\begin{aligned} g_i &= -\sum_{x\in\mathbb{F}_{q^{u(a)}}^\times} t^{\frac{q^{u(a)}-1}{d}a_i}(x)\psi(x) \\ &= -\sum_{x\in\mathbb{F}_{q^{u(a)}}^\times} t^{\frac{q^{2e}-1}{d}a_i}\left(\mathrm{N}_{\mathbb{F}_{q^{u(a)}}/\mathbb{F}_{q^{2e}}}(x)\right)\psi(x) \end{aligned}$$

which, by the Hasse-Davenport relation, is

$$= \left(-\sum_{x\in\mathbb{F}_{q^{2e}}^\times} t^{\frac{q^{2e}-1}{d}a_i}(x)\psi(x)\right)^{u(a)/(2e)}.$$

(We have abusively written ψ for the additive characters of both $\mathbb{F}_{q^{u(a)}}$ and $\mathbb{F}_{q^{2e}}$.) But by Lemma 8.2, $(q^e+1)a_i/d \in \mathbb{Z}$ and so the inner sum is of the type considered in Lemma 8.3. Thus

$$g_i = \left(-t^{\frac{q^{2e}-1}{d}a_i}(x)\right)^{u(a)/(2e)} q^{u(a)/2}$$

where $x \in \mathbb{F}_{q^{2e}}^\times$ is any element with $\mathrm{Tr}_{\mathbb{F}_{q^{2e}}/\mathbb{F}_{q^e}}(x) = 0$.

Taking the product over $i = 0, \dots, 3$ and using the fact that $\sum_{i=0}^{3} a_i \equiv 0 \mod d$, we see that $J(a) = q^{u(a)}$. □

9. The rank of E

9.1. We are now in a position to compute the rank of E_d over $\mathbb{F}_q(t)$ for any d dividing $p^n + 1$. By Proposition 6.4, the rank is

$$-\operatorname{ord}_{s=1}\zeta(F_d/\Gamma, s) - 1 + \begin{cases} 0 & \text{if } 2 \nmid d \text{ or } 4 \nmid q-1 \\ 1 & \text{if } 2|d \text{ and } 4|q-1 \end{cases} + \begin{cases} 0 & \text{if } 3 \nmid d \\ 1 & \text{if } 3|d \text{ and } 3 \nmid q-1 \\ 2 & \text{if } 3|d \text{ and } 3|q-1. \end{cases}$$

By Corollary 7.7 and Proposition 8.1, $-\operatorname{ord}_{s=1}\zeta(F_d/\Gamma, s)$ is equal to the number of orbits of multiplication by q on $\Gamma^\perp \cap \hat{G}'$. Here

$$\hat{G}' = \{a \in \hat{G} \mid a = 0 \text{ or } a = (a_0, \dots, a_3) \text{ with } a_i \neq 0\}$$

and $\Gamma^\perp$ is the cyclic subgroup of $\hat{G}$ generated by $(3, -6, 2, 1)$. Thus $\Gamma^\perp \cap \hat{G}'$ is in bijection with $\{a_3 \in \mathbb{Z}/d\mathbb{Z} \mid 6a_3 \neq 0\} \cup \{0\}$. The size of the orbit of a_3 depends only on $e = \frac{d}{(d, a_3)}$ and is equal to $o_e(q)$, the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$. Thus we have

$$-\operatorname{ord}_{s=1}\zeta(F_d/\Gamma, s) = \sum_{\substack{e|d \\ e\nmid 6}} \frac{\phi(e)}{o_e(q)} + 1.$$

(The term 1 corresponds to $e = 1$, i.e., to $a_3 = 0$.)

Putting everything together, we have our main theorem.

9.2. Theorem. *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 $(\mathbb{Z}/e\mathbb{Z})^\times$.

9.3. We now specialize to the case where $d = p^n + 1$. If $q = p$ then $o_e(p) \leq 2n$ for all divisors e of d. Applying the theorem, we see that the rank of E over $\mathbb{F}_p(t)$ is at least $(p^n - 1)/2n$. This completes the proof of Theorem 1.5.

On the other hand, if we take q to be a power of p^{2n}, then $o_e(q) = 1$ for all divisors e of d. The theorem then implies that 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 $6|d$.

10. Rank bounds

10.1. Let $\mathcal{C}$ be a smooth complete curve of genus g over $\mathbb{F}_q$ and let E be an elliptic curve over $K = \mathbb{F}_q(\mathcal{C})$. Write $\mathfrak{n}$ for the conductor of E and let $\deg(\mathfrak{n})$ be the degree of $\mathfrak{n}$, viewed as an effective divisor on $\mathcal{C}$. As mentioned in Section 6, there is a geometric bound on the rank of E:

$$\operatorname{Rank} E(K) \leq \operatorname{ord}_{s=1} L(E/K, s) \leq \begin{cases} 4g & \text{if } E \text{ is constant} \\ 4g - 4 + \deg(\mathfrak{n}) & \text{if } E \text{ is not constant.} \end{cases}$$

This bound is geometric in that it is not affected if we extend the constant field $\mathbb{F}_q$. But as we have seen in the previous section, both $\operatorname{Rank} E(K)$ and $\operatorname{ord}_{s=1} L(E/K, s)$ can change dramatically if the constant field is enlarged.

In fact, there is an arithmetic bound, i.e., a bound which is sensitive to the finite field of constants. In [Bru92, Prop. 6.9] Brumer used Weil's "explicit formula" technique to prove an upper bound

$$\operatorname{ord}_{s=1} L(E/K, s) \leq \frac{4g - 4 + \deg(\mathfrak{n})}{2 \log_q \deg(\mathfrak{n})} + C \frac{\deg(\mathfrak{n})}{(\log_q \deg(\mathfrak{n}))^2}$$

where $\log_q$ denotes the logarithm to base q and C is an explicit constant depending only on g and q. (Here we ignore the finitely many elliptic curves over K with trivial conductor.) This is the function field analogue of a theorem of Mestre [Mes86] which says that if E is a modular elliptic curve over $\mathbb{Q}$ then, assuming a generalized Riemann hypothesis, $\operatorname{ord}_{s=1} L(E/\mathbb{Q}, s) = O(\log N / \log\log N)$.

Brumer's bound is visibly sensitive to the field of constants and is an improvement on the geometric bound when $\deg(\mathfrak{n})$ is large with respect to q.

10.2. The curves of Theorem 9.2 show that the main term of Brumer's arithmetic bound over $\mathbb{F}_p(t)$ is sharp. Indeed, the curve with $d = p^n + 1$ has $\deg(\mathfrak{n}) = p^n + 4$ if $6 \nmid d$ and $\deg(\mathfrak{n}) = p^n + 2$ if $6 | d$, and its rank (analytic and algebraic) is at least $(p^n - 1)/2n$. (Note also that these curves meet the geometric bound over $\mathbb{F}_q(t)$ when $\mathbb{F}_q$ contains $\mathbb{F}_{p^{2n}}$.)

10.3. The (isotrivial) elliptic curves of [TS67] also meet the main term of Brumer's arithmetic bound over $\mathbb{F}_p(t)$. Indeed, the curve of their Theorem 2 (with $f = p^n + 1$) has $\deg(\mathfrak{n})$ approximately $2p^n$ and rank approximately p^n/n.

10.4. The preceding remarks show that the Brumer arithmetic bound is asymptotically sharp in the function field case. We believe that the Mestre bound should likewise be asymptotically sharp in the number field case.

Let K now be a number field. For a positive integer N, let $r_K(N)$ be the maximum, over all elliptic curves E over K with conductor $\mathfrak{n}$ satisfying $N_{K/\mathbb{Q}}(\mathfrak{n}) = N$, of $\operatorname{Rank} E(K)$; if there are no such curves, we set $r_K(N) = 0$. Assuming various standard conjectures, it follows from a simple generalization of Mestre's argument that $r_K(N) = O(\log N / \log\log N)$ (where the constant of course depends on K), and so the limit in the following conjecture is finite.

10.5. Conjecture.

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

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

$$1 \leq \frac{N_{\mathbb{Q}}(E)^{[K:\mathbb{Q}]}}{N_K(E)} \leq C$$

for all elliptic curves E over $\mathbb{Q}$. This can be used to prove that the conjecture for a general number field K follows from the conjecture for $\mathbb{Q}$.

References

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

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

[Kat81] N. M. Katz, *Crystalline cohomology, Dieudonné modules, and Jacobi sums*, Automorphic forms, representation theory and arithmetic (Bombay, 1979), Tata Inst. Fundamental Res., Bombay, 1981, pp. 165–246.

[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.

[MM00] R. Martin and W. McMillen, *An elliptic curve over q with rank at least 24*, Preprint (2000), Posted to the Usenet newsgroup math.sci.nmbrthry by V. Miller on May 2, 2000. Available at `http://listserv.nodak.edu/archives/nmbrthry.html`.

[MP86] I. Morrison and U. Persson, *Numerical sections on elliptic surfaces*, Compositio Math. **59** (1986), 323–337.

[Shi72] T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59.

[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.

[Tat65] J. T. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963), Harper & Row, New York, 1965, pp. 93–110.

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

[Tat75] J. T. Tate, *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] J. T. Tate, *Conjectures on algebraic cycles in l-adic cohomology*, Motives (Seattle, WA, 1991), Amer. Math. Soc., Providence, RI, 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.

[Wei49] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. **55** (1949), 497–508.

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