Math. Res. Lett. **14** (2007), *no.* 3, 453–467

JACOBI SUMS, FERMAT JACOBIANS, AND RANKS OF ABELIAN VARIETIES OVER TOWERS OF FUNCTION FIELDS

Douglas Ulmer

1. Introduction

Given an abelian variety A over a function field $K = k(\mathcal{C})$ with $\mathcal{C}$ an absolutely irreducible, smooth, proper curve over a field k, it is natural to ask about the behavior of the Mordell-Weil group of A in the layers of a tower of fields over K. The simplest case, which is already very interesting, is when A is an elliptic curve, $K = k(t)$ is a rational function field, and one considers the towers $k(t^{1/d})$ or $\overline{k}(t^{1/d})$ as d varies through powers of a prime or through all integers not divisible by the characteristic of k.

When $k = \mathbb{Q}$ or more generally a number field, several authors (e.g., [Shi86], [Sti87], [Fas97], [Sil00], [Sil04], and [Ell06]) have considered this question and given bounds on the rank of A over $\mathbb{Q}(t^{1/d})$ or $\overline{\mathbb{Q}}(t^{1/d})$. In some interesting cases it can be shown that A has rank bounded independently of d in the tower $\overline{\mathbb{Q}}(t^{1/d})$. Of course no example is yet known of an elliptic curve over $\mathbb{Q}(t)$ with unbounded ranks in the tower $\mathbb{Q}(t^{1/d})$, nor of an elliptic curve over $\overline{\mathbb{Q}}(t)$ with non-constant j-invariant and unbounded ranks in the tower $\overline{\mathbb{Q}}(t^{1/d})$.

When k is a finite field, examples of Shioda and the author show that there are non-isotrivial elliptic curves over $\mathbb{F}_p(t)$ with unbounded ranks in the towers $\overline{\mathbb{F}}_p(t^{1/d})$ [Shi86, Remark 10] and $\mathbb{F}_p(t^{1/d})$ [Ulm02, 1.5]. More recently, the author has shown [Ulm07] that high ranks over function fields over finite fields are in some sense ubiquitous. For example, for every prime p and every integer $g > 0$ there are absolutely simple abelian varieties of dimension g over $\mathbb{F}_p(t)$ with unbounded ranks in the tower $\mathbb{F}_p(t^{1/d})$, and given any non-isotrivial elliptic curve E over $\mathbb{F}_q(t)$, there exists a finite extension $\mathbb{F}_r(u)$ such that E has unbounded (analytic) ranks in the tower $\mathbb{F}_r(u^{1/d})$.

One obvious difference between number fields and finite fields which might be relevant here is the complexity of their absolute Galois groups: that of a finite field is pro-cyclic while that of a number field is highly non-abelian. Ellenberg uses this non-abelianess in a serious way in his work on bounding ranks and, in a private communication, he asked whether it might be the case that, say, a non-isotrivial elliptic curve over $\mathbb{F}_q(t)$ always has unbounded rank in the tower $\mathbb{F}_q(t^{1/d})$.

Received by the editors November 1, 2005.

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

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

Our goal in this note, which is a companion to [Ulm07], is to give a number of examples of abelian varieties over function fields $\mathbb{F}_q(t)$ which have bounded ranks in the towers $\overline{\mathbb{F}}_q(t^{1/d})$ as d ranges through powers of a suitable prime or through all integers not divisible by p, the characteristic of $\mathbb{F}_q$. We also get some information about ranks in towers $k(t^{1/d})$ for arbitrary fields k. Along the way we prove some new results on Fermat curves which may be of independent interest. The main results are Theorems 2.4, 3.2, 3.3, 4.5, 5.2, and 6.2

2. Jacobi sums

2.1. Throughout the paper p will be a rational prime number, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ will be the prime field of characteristic p, and $q = p^f$ will be a power of p. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. All number fields considered will tacitly be assumed to be subfields of $\overline{\mathbb{Q}}$. We denote by μ_d the group of d-th roots of unity in $\overline{\mathbb{Q}}$.

Let $\mathfrak{p}$ be a prime of $\mathcal{O}_{\overline{\mathbb{Q}}}$, the ring of integers of $\overline{\mathbb{Q}}$, over p. The field $\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$ which we denote by $\overline{\mathbb{F}}_p$ and we write $\mathbb{F}_q$ for its subfield of cardinality q.

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 $(\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p})^\times = \overline{\mathbb{F}}_p^{\times}$. We let $t : \overline{\mathbb{F}}_p^{\times} \to \overline{\mathbb{Q}}^{\times}$ denote the inverse of this isomorphism. We will use the same letter t for the restriction to any of the finite fields $\mathbb{F}_q^\times$. Every character of $\mathbb{F}_q^\times$ is a power of t.

2.2. Fix a non-trivial additive character $\psi_p : \mathbb{F}_p \to \overline{\mathbb{Q}}^{\times}$. For each q we define an additive character ψ_q as $\psi_q = \psi_p \circ \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$.

For each q and each character χ of $\mathbb{F}_q^\times$, we define a Gauss sum

$$G_q(\chi) = -\sum_{x\in\mathbb{F}_q^\times} \chi(x)\psi_q(x) \in \mathbb{Q}(\mu_{p(q-1)}).$$

It is well known that $G_q(\chi) = 1$ if χ is the trivial character and that $G_q(\chi)$ is an algebraic integer with absolute value $q^{1/2}$ in every complex embedding if $\chi \neq 1$.

For any d prime to p, any $a \in \mathbb{Z}/d\mathbb{Z}$, and any $q \equiv 1 \pmod{d}$, we write $G_q(a)$ for $G_q(t^{-a(q-1)/d})$ which lies in $\mathbb{Q}(\mu_{pd})$. The analysis leading to Stickelberger's theorem [Was97, 6.2] shows that if $\wp$ is the prime of $\mathbb{Q}(\mu_{pd})$ under $\mathfrak{p}$, $q = p^f$, and $a \not\equiv 0 \pmod{d}$ then

$$\mathrm{ord}_\wp G_q(a) = (p-1)\sum_{j=0}^{f-1} \left\langle \frac{p^j a}{d} \right\rangle$$

where $\langle x\rangle$ is the fractional part of x, i.e., $0 \leq \langle x\rangle < 1$ and $x - \langle x\rangle \in \mathbb{Z}$.

2.3. Fix a positive integer w. For each q and each tuple of non-trivial characters $\chi_0, \dots, \chi_{w+1}$ of $\mathbb{F}_q^\times$ such that the product $\chi_0 \cdots \chi_{w+1}$ is trivial, we define a Jacobi sum

$$J_q(\chi_0, \dots, \chi_{w+1}) = \frac{1}{q-1} \sum_{\substack{x_0,\dots,x_{w+1}\in\mathbb{F}_{p^f}^\times \\ x_0+\cdots+x_{w+1}=0}} \chi_0(x_0)\cdots\chi_{w+1}(x_{w+1}) \in \mathbb{Q}(\mu_{q-1}).$$

It is well-known and elementary (see [Wei49, p. 501] for example) that

$$J_q(\chi_0, \ldots, \chi_{w+1}) = \frac{(-1)^w}{q} \prod_{i=0}^{w+1} G_q(\chi_i).$$

In particular, the Jacobi sum is an algebraic integer with absolute value $q^{w/2}$ in every complex embedding.

Let $A_{d,w} \subset (\mathbb{Z}/d\mathbb{Z})^{w+2}$ be the set of tuples $\mathbf{a} = (a_0, \ldots, a_{w+1})$ such that $a_i \neq 0$ for all i and $\sum a_i = 0$. If $\mathbf{a} \in A_{d,w}$ and $q \equiv 1 \pmod{d}$, we write $J_q(\mathbf{a})$ for $J_q(t^{-a_0(q-1)/d}, \ldots, t^{-a_{w+1}(q-1)/d})$; clearly $J_q(\mathbf{a}) \in \mathbb{Q}(\mu_d)$. If $\wp$ is the prime of $\mathbb{Q}(\mu_d)$ under $\mathfrak{p}$ and $q = p^f$, then

$$\operatorname{ord}_\wp J_q(\mathbf{a}) = \sum_{i=0}^{w+1} \sum_{j=0}^{f-1} \left\langle \frac{p^j a_i}{d} \right\rangle - f.$$

We write $A'_{d,w}$ for those $\mathbf{a} \in A_{d,w}$ such that $\gcd(d, a_0, \ldots, a_{w+1}) = 1$. Note that if $\mathbf{a} \in A_{d,w}$ and if $e = \gcd(d, a_0, \ldots, a_{w+1})$, $d' = d/e$ and $\mathbf{a}' = (a_0/e, \ldots, a_{w+1}/e) \in A'_{d',w}$ then for any $q \equiv 1 \pmod{d}$ we have $J_q(\mathbf{a}) = J_q(\mathbf{a}')$.

Many of our results on ranks will be based on part (2) of the following theorem about the distribution of Gauss and Jacobi sums. Roughly speaking, it says that sums involving characters of large order must either have large degree over $\mathbb{Q}$ or have valuation bounded away from 0.

2.4. Theorem.

(1) *Fix a real number $\epsilon > 0$ and a positive integer n. There exists a constant $C_{\epsilon,n}$ depending only on ϵ and n such that if $d > C_{\epsilon,n}$, $q = p^f \equiv 1 \pmod{d}$, $a \in (\mathbb{Z}/d\mathbb{Z})^\times$, and the degree of $G_q(a)$ over $\mathbb{Q}(\mu_p)$ is $\leq n$, then*

$$\left| \frac{\operatorname{ord}_\wp G_q(a)}{(p-1)f} - \frac{1}{2} \right| < \epsilon.$$

Here $\wp$ is the prime of $\mathbb{Q}(\mu_{pd})$ under $\mathfrak{p}$. Note that $\operatorname{ord}_\wp(q) = (p-1)f$.

(2) *Fix a positive integer n. There exist constants C_n and $\epsilon_n > 0$ depending only on n such that if $d > C_n$, $q = p^f \equiv 1 \pmod{d}$, $w \geq 1$, $\mathbf{a} \in A'_{d,w}$, and the degree of $J_q(\mathbf{a})$ over $\mathbb{Q}$ is $\leq n$, then*

$$\frac{\operatorname{ord}_\wp J_q(\mathbf{a})}{f} > \epsilon_n.$$

Here $\wp$ is the prime of $\mathbb{Q}(\mu_d)$ under $\mathfrak{p}$. Note that $\operatorname{ord}_\wp(q) = f$.

2.5. *Remarks.*

(1) The constants appearing in the theorem are *independent of* p and effectively computable.

(2) In part (2) of the theorem, we may replace "the degree of $J_q(\mathbf{a})$ over $\mathbb{Q}$ is $\leq n$" with "the degree of the largest subfield of $\mathbb{Q}(J_q(\mathbf{a}))$ in which p splits completely is $\leq n$" and similarly in part (1). I do not know whether this has any applications to geometry.

The theorem is a consequence of Stickelberger's theorem and the following simple estimate.

2.6. Proposition. *Fix a real number $\epsilon > 0$ and a positive integer n. There exists a constant $C_{\epsilon,n}$ depending only on ϵ and n such that if $d > C_{\epsilon,n}$ and $H \subset G = (\mathbb{Z}/d\mathbb{Z})^\times$ is a subgroup of index $\leq n$, then for all $a \in G$,*

$$\left| \frac{1}{|H|} \sum_{t \in H} \left\langle \frac{ta}{d} \right\rangle - \frac{1}{2} \right| < \epsilon.$$

Proof. We have

$$\begin{aligned} A := \frac{1}{|H|} \sum_{t \in H} \left\langle \frac{ta}{d} \right\rangle &= \frac{1}{|H|} \sum_{\substack{s=1 \\ (s,d)=1}}^{d-1} \frac{s}{d} \frac{1}{[G:H]} \sum_{\chi \in \widehat{G/H}} \chi(sa^{-1}) \\ &= \frac{1}{2} + \frac{1}{d\phi(d)} \sum_{1 \neq \chi \in \widehat{G/H}} \chi(a^{-1}) \sum_{\substack{s=1 \\ (s,d)=1}}^{d-1} \chi(s)s \end{aligned}$$

where $|H|$ denotes the order of H, $\widehat{G/H}$ denotes the group of characters of G/H (which we view as characters of G trivial on H), and $\phi(d) = |G|$ is Euler's function. Partial summation and the Polya-Vinogradov inequality [Dav00, §23] show that there is an absolute constant C such that the inner sum above is $< Cd^{3/2} \log d$ and so the quantity A to be estimated satisfies

$$\left| A - \frac{1}{2} \right| \leq \frac{Cnd^{1/2} \log d}{\phi(d)}.$$

Well-known estimates for $\phi(d)$ [HW79, Thm 327] say that for all $\delta > 0$, $\phi(d)/d^{1-\delta} \to \infty$ as $d \to \infty$ so there is a constant $C_{\epsilon,n}$ depending only on n and ϵ such that

$$\frac{Cnd^{1/2} \log d}{\phi(d)} < \epsilon$$

whenever $d > C_{\epsilon,n}$. This completes the proof of the proposition. □

2.7. Corollary. *Given n there exists a constant $\delta_n > 0$ depending only on n such that for any $d \geq 2$, any $0 \neq a \in \mathbb{Z}/d\mathbb{Z}$, and any subgroup $H \subset G = (\mathbb{Z}/d\mathbb{Z})^\times$ of index $\leq n$,*

$$\frac{1}{|H|} \sum_{t \in H} \left\langle \frac{ta}{d} \right\rangle > \delta_n$$

Proof. For $0 \neq a \in (\mathbb{Z}/d\mathbb{Z})$, set $e = \gcd(a,d)$, $d' = d/e$, $G' = (\mathbb{Z}/d'\mathbb{Z})^\times$, $a' = a/e$, and $H' = \operatorname{Im}(H \to G')$. Then the index of H' in G' is $\leq n$ and we have

$$A := \frac{1}{|H|} \sum_{t \in H} \left\langle \frac{ta}{d} \right\rangle = \frac{1}{|H'|} \sum_{t \in H'} \left\langle \frac{ta'}{d'} \right\rangle$$

and so we may assume that $\gcd(a,d) = 1$, i.e., that $a \in G$.

Given n, let $C_{1/4,n}$ be the constant furnished by the proposition for n and $\epsilon = 1/4$. If $d > C_{1/4,n}$ then by the proposition, $A > 1/4$. On the other hand, there are only finitely many $d \leq C_{1/4,n}$ and for each d, only finitely many subgroups $H \subset (\mathbb{Z}/d\mathbb{Z})$ of index $\leq n$. Since $A > 0$ for each of these finitely many possibilities, there is a $\delta_n > 0$ such that $A > \delta_n$ for all d and a. □

2.8. Proof of Theorem 2.4 (1). Given ϵ and n, suppose that d, $q = p^f \equiv 1 \pmod{d}$, and $a \in G = (\mathbb{Z}/d\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_{pd})/\mathbb{Q}(\mu_p))$, are such that $G_q(a) \in \mathbb{Q}(\mu_{pd})$ has degree $\leq n$ over $\mathbb{Q}(\mu_p)$. Let $H \subset G$ be the subgroup of G fixing $\mathbb{Q}(\mu_p, G_q(a))$, so that H has index $\leq n$ in G. If $\wp$ is the prime of $\mathbb{Q}(\mu_{pd})$ under $\mathfrak{p}$, then for every $t \in H$, we have $\mathrm{ord}_{\wp^t}(G_q(a)) = \mathrm{ord}_{\wp}(G_q(a))$. Therefore,

$$\begin{aligned}\frac{\mathrm{ord}_{\wp} G_q(a)}{(p-1)f} &= \frac{1}{|H|}\sum_{t\in H}\frac{\mathrm{ord}_{\wp^t} G_q(a)}{(p-1)f}\\ &= \frac{1}{|H|f}\sum_{t\in H}\sum_{j=0}^{f-1}\left\langle\frac{p^j ta}{d}\right\rangle\end{aligned}$$

where the second equality comes from Stickelberger's theorem. Let P be the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p and HP the subgroup generated by H and P. The last displayed sum is then equal to

$$\frac{1}{|HP|}\sum_{t\in HP}\left\langle\frac{ta}{d}\right\rangle.$$

Since H has index $\leq n$ in G, the same is true of HP and so Proposition 2.6 shows that if $d > C_{\epsilon,n}$ then

$$\left|\frac{\mathrm{ord}_{\wp} G_q(a)}{(p-1)f} - \frac{1}{2}\right| < \epsilon$$

as was to be shown. □

2.9. Proof of Theorem 2.4 (2). Given $\mathbf{a} \in A'_{d,w}$, set $d_i = d/\gcd(d, a_i)$. The following lemma tells us that if d is large then at least two of the d_i are also large.

2.9.1. Lemma. *With notation as above, there exists an absolute constant C such that at least two of the d_i are $\geq C \log d$.*

Proof. If ℓ divides d then from the definitions, there are at least two i's such that ℓ does not divide a_i. Therefore the largest prime power dividing d also divides at least two of the d_i.

To finish we note that Chebyschev's theorem [HW79, Thm. 7] implies that the largest prime power dividing d is $\geq C' \log d$ for some absolute constant C'. Indeed, let M be a positive number, let $p_1, \ldots, p_{\pi(M)}$ be the primes less than M, and let $p_i^{e_i}$ be the largest power of p_i less than M. If $N = \prod_{i=1}^{\pi(M)} p_i^{e_i}$ then

$$\log N = \sum_{i=1}^{\pi(M)} e_i \log p_i \leq \pi(M)\log M \leq C'M$$

by Chebyschev. This shows that if N is a product of prime powers less than M, then $N \leq e^{C'M}$. Therefore the largest prime power dividing N is at least $C \log N$ where $C = 1/C'$. □

Now fix n and consider those $q \equiv 1 \pmod{d}$ and $\mathbf{a}$ such that $J_q(\mathbf{a})$ has degree $\leq n$ over $\mathbb{Q}$. Let $H \subset G = (\mathbb{Z}/d\mathbb{Z})^\times \cong \mathrm{Gal}(\mathbb{Q}(\mu_d)/\mathbb{Q})$ be the subgroup fixing $\mathbb{Q}(J_q(\mathbf{a}))$ so that H has index $\leq n$ in G. Then we have

$$\begin{aligned} A(q,\mathbf{a}) := \frac{\operatorname{ord}_\wp J_q(\mathbf{a})}{f} &= \frac{1}{|H|}\sum_{t\in H}\frac{\operatorname{ord}_{\wp^t}(J_q(\mathbf{a}))}{f} \\ &= \frac{1}{|H|}\sum_{t\in H}\frac{1}{f}\left(\sum_{i=0}^{w+1}\sum_{j=0}^{f-1}\left\langle\frac{tp^j a_i}{d}\right\rangle - f\right) \\ &= \left(\sum_{i=0}^{w+1}\frac{1}{|HP|}\sum_{t\in HP}\left\langle\frac{ta_i}{d}\right\rangle\right) - 1 \end{aligned}$$

where as before P is the subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by p and HP is the subgroup generated by H and P. Reindexing $\mathbf{a}$, we may assume that d_0 and d_1 are $\geq C\log d$. Since H has index $\leq n$, so does HP and so we get bounds on the inner sums in the last displayed equation. More precisely, by Corollary 2.7, the inner sum is $> \delta_n$ for $i = 2,\dots,w+1$, and by Proposition 2.6, if d_0 and d_1 are sufficiently large (so that $C\log d > C_{\epsilon,n}$), the $i = 0$ and $i = 1$ terms are $> 1/2 - \epsilon$. Applying this with $\epsilon = \delta_n/4 \leq w\delta_n/4$, we see that for sufficiently large d, $A(q,\mathbf{a}) \geq (w - 1/2)\delta_n \geq \delta_n/2$. This completes the proof of part (2) of the theorem. □

3. Fermat Jacobians

3.1. Let k be an arbitrary field with separable closure $\overline{k}$. For each positive integer d not divisible by the characteristic of k we consider the Fermat curve F_d of degree d over k (the zero locus of $\sum_{i=0}^2 x_i^d$ in $\mathbb{P}^2$) and its Jacobian J_d. If A is an abelian variety over k, we say that "A appears in J_d" if there is a homomorphism of abelian varieties $A \to J_d$ with finite kernel. We say "A appears in J_d with multiplicity m" if m is the largest integer such that A^m appears in J_d. The multiplicity with which A appears in J_d obviously depends only on the k-isogeny class of A.

The following two theorems are the main results of this section.

3.2. Theorem. *Suppose that k is a field of characteristic zero. Then for every positive integer g, only finitely many k-isogeny classes of abelian varieties of dimension $\leq g$ appear in J_d as d varies through all positive integers. If A is an abelian variety over k, then the multiplicity with which A appears in J_d is bounded by a constant depending only on the dimension of A.*

If k has characteristic p and A is an abelian variety over k, the p-rank of A is by definition the dimension over $\mathbb{F}_p$ of the group of $\overline{k}$-rational p-torsion points on A. It is known that the p-rank lies in the interval $[0, \dim A]$ and that it is invariant under isogeny.

3.3. Theorem. *Suppose that k is a field of characteristic $p > 0$. Then for every positive integer g, only finitely many k-isogeny classes of abelian varieties with positive p-rank and dimension $\leq g$ appear in J_d as d varies through all positive integers prime to p. If A is an abelian variety over k with positive p-rank, then the multiplicity with which A appears in J_d is bounded by a constant depending only on the dimension of A.*

3.4. *Remarks.*

(1) We repeat that the constants in the theorems depend only on the dimension g. In particular, they are independent of the characteristic of k. As will be clear from the proof, they are also effectively computable.
(2) Theorem 3.2 is already known in a more precise quantitative form by results of Aoki [Aok91], building on work of Koblitz, Rohrlich, and Shioda. Theorem 3.3 may be known to experts but to my knowledge is not in the literature. We will give a very simple proof of Theorem 3.3 for k finite and use this to deduce the general case and Theorem 3.2.
(3) It is proven in [TS67], and by a different method in [Ulm07], that over a field of characteristic p, the multiplicity with which a supersingular elliptic curve appears in J_d is unbounded as d varies. Thus the last part of Theorem 3.3 would be false without the hypothesis of positive p-rank. It is not clear what to expect for abelian varieties with p-rank zero which are not $\overline{k}$-isogenous to a product of supersingular elliptic curves.
(4) Note added in proof: The complete list of d such that J_d has an elliptic factor over $\overline{\mathbb{Q}}$ appears in [Kob78]. The analogous list for the fields $\overline{\mathbb{F}}_p$ was computed by I. Barrientos, C. Jewell, and T. Occhipinti, three students at the University of Arizona. The two lists are identical and the largest integer appearing on them is $d = 60$.

The proofs of Theorems 3.2 and 3.3 will be given in rest of this section.

3.5. If $d' < d$ is a divisor of d, then there is a canonical surjective morphism $F_d \to F_{d'}$ ($x_i \mapsto x_i^{d/d'}$) which (because $F_d \to F_{d'}$ is totally ramified at some place) induces an injection of Jacobians $J_{d'} \hookrightarrow J_d$. We define the *old part* J_d^{old} to be the abelian subvariety of J_d generated by the images of the morphisms $J_{d'} \hookrightarrow J_d$ as d' varies through proper divisors of d and we define the *new part* J_d^{new} of J_d to be the abelian variety over k (well-defined only up to k-isogeny) such that J_d is isogenous to $J_d^{\mathrm{new}} \times J_d^{\mathrm{old}}$. It is not hard to check, for example by using the zeta function calculation mentioned in 3.8 below, that J_d is isogenous to $\prod_{d'|d} J_{d'}^{\mathrm{new}}$.

Theorem 3.2 therefore follows from the statement that there is a constant C_g depending only on g such that no abelian variety A of dimension $\leq g$ appears in J_d^{new} for any $d > C_g$. Theorem 3.3 follows from the same statement with the additional hypotheses that A has positive p-rank and d is not divisible by p.

3.6. Given a field k, let $\mathbb{F}$ be its prime field and k_0 be the algebraic closure of $\mathbb{F}$ in k. Then k_0 is a perfect field and so the extension k/k_0 is regular. The Fermat Jacobian J_d and its new part J_d^{new} are defined over $\mathbb{F}$ and so if A is an abelian variety over k which appears in $J_d^{\mathrm{new}} \times_{\mathbb{F}} k$ then there is an abelian variety A_0 defined over k_0 which appears in $J_d^{\mathrm{new}} \times_{\mathbb{F}} k_0$ and with $A_0 \times_{k_0} k \cong A$. (This is an old result of Chow which has been given a detailed modern treatment by Conrad, see [Con06, 3.21].) Moreover, the abelian variety A_0 and the morphism $A_0 \to J_d^{\mathrm{new}}$ are both defined over some finite extension of $\mathbb{F}$. Thus it will suffice to prove the existence of the constants C_g mentioned at the end of Subsection 3.5 (depending only on g, not on k) for the cases when k is a number field or a finite field.

3.7. Let k be $\mathbb{F}_q$, the subfield of $\overline{\mathbb{F}}_p = \mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p}$ with q elements. A *Weil q-integer of weight 1* is an algebraic integer α whose absolute value in every complex embedding is $q^{1/2}$. For the rest of this section we will call these simply *Weil numbers*.

Honda-Tate theory [Tat68] says that $\mathbb{F}_q$-isogeny classes of $\mathbb{F}_q$-simple abelian varieties are in bijection with $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ orbits of Weil numbers. If A corresponds to α, then $E = \mathrm{End}_{\mathbb{F}_q}(A) \otimes \mathbb{Q}$ is a central simple algebra over $\mathbb{Q}(\alpha)$ whose invariants in the Brauer group of $\mathbb{Q}(\alpha)$ can be calculated in terms of the decomposition of p in $\mathbb{Q}(\alpha)$. The dimension of A is $(1/2)[E : \mathbb{Q}(\alpha)]^{1/2}[\mathbb{Q}(\alpha) : \mathbb{Q}]$ and the eigenvalues of Frobenius on $H^1(A \times \overline{\mathbb{F}}_q, \mathbb{Q}_\ell)$ are the conjugates of α, each appearing with multiplicity $[E : \mathbb{Q}(\alpha)]^{1/2}$. The p-rank of A is equal to the number of eigenvalues of Frobenius which are units at $\mathfrak{p}$ and so A has positive p-rank if and only if some conjugate of α is a unit at $\mathfrak{p}$.

If C is a curve of genus g over $\mathbb{F}_q$ and the Z-function of C is

$$\frac{\prod_{i=1}^{2g}(1-\alpha_i T)}{(1-T)(1-qT)}$$

then the Weil numbers of the $\mathbb{F}_q$-simple factors of the Jacobian J of C are precisely the α_i. The multiplicity of α_i in the numerator is the multiplicity of the corresponding A in J up to $\mathbb{F}_q$-isogeny times $[E_A : \mathbb{Q}(\alpha)]^{1/2}$.

3.8. Given a positive integer d and a prime power q such that $q \equiv 1 \pmod d$ we consider the Fermat curve F_d over $\mathbb{F}_q$. By a theorem of Weil [Wei49], the Z-function of F_d over $\mathbb{F}_q$ is

$$\frac{\prod_{\mathbf{a} \in A_{d,1}}(1 - J_q(\mathbf{a})T)}{(1-T)(1-qT)}$$

where $A_{d,1}$ was defined in Subsection 2.3.

It is clear from Weil's computation of the Z-function that the Weil numbers of J_d^{new} are precisely the $J_q(\mathbf{a})$ as $\mathbf{a}$ runs through

$$A'_{d,1} = \{\mathbf{a} = (a_0, a_1, a_2) \in A_{d,1} \,|\, \gcd(d, a_0, a_1, a_2) = 1\}.$$

3.9. The case of finite fields. We assume $k = \mathbb{F}_q$ and that A is an abelian variety over k which has positive p-rank and dimension $\leq g$ and appears in J_d^{new}. In this case, the Weil numbers of A are among the Weil numbers of J_d^{new}. Extending k if necessary, we may assume that $d|(q-1)$ and so the Weil numbers of J_d^{new} are the Jacobi sums $J_q(\mathbf{a})$ where $\mathbf{a} \in A'_{d,1}$. By the results recalled in Subsections 3.7 and 3.8 it follows that some $J_q(\mathbf{a})$ has degree $\leq 2g$ over $\mathbb{Q}$ and is a unit at the prime $\mathfrak{p}$. This implies that d is $\leq C_{2g}$ where C_{2g} is the constant appearing in Theorem 2.4(2) for $n = 2g$. Therefore no abelian variety of positive p-rank and dimension $\leq g$ appears in J_d^{new} for large d and this establishes Theorem 3.3 for finite fields. The argument in Subsection 3.6 shows that the theorem also holds for arbitrary fields of positive characteristic.

3.10. The case of number fields. Suppose that A is an abelian variety of dimension $\leq g$ defined over a number field k. Suppose that d is larger than the constant $C(g) = C_{2g}$ appearing in Theorem 3.3 and that A appears in J_d^{new}. Then for every prime $\wp$ of k where A has good reduction, by Theorem 3.3 the reduction $A \times \mathbb{F}_\wp$ has p-rank 0. This would violate the following result, which appears in [Ogu82, 2.7.1]:

3.10.1. Lemma. (*Katz*) *If A is an abelian variety over a number field k, then for infinitely many primes of k, the reduction of A has positive p-rank.*

For the convenience of the reader, we sketch the proof of the lemma. Choose a prime ℓ larger than $2g$. Let L be a finite extension of k such that $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ acts trivially on the ℓ-torsion of A. If $\wp$ is a prime of L over the rational prime p where the reduction of A has p-rank zero, then the trace of the Frobenius at $\wp$ on $H^1(A \times \overline{k}, \mathbb{Q}_\ell)$ is an integer $\equiv 0 \pmod p$ and $\leq 2g(\mathrm{N}\,\wp)^{1/2}$. If $\wp$ has absolute degree 1 over $\mathbb{Q}$ (i.e., $\mathrm{N}\,\wp = p$), and $\sqrt{p} > 2g$ then we see that the trace must be zero. On the other hand, since $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$ acts trivially on ℓ-torsion, the trace must be $\equiv 2g \pmod \ell$. Since $\ell > 2g$ this is impossible. The conclusion is that the reduction of A at a prime of absolute degree one over a large p must have positive p-rank. Such primes have density one in L and the primes under them in k are an infinite set satisfying the conclusion of the lemma.

We note that a stronger version of this result for abelian varieties over $\mathbb{Q}$ is proven in [BG97, Prop. 5.1].

The lemma completes the proof of Theorem 3.2 for number fields and, as explained in Subsection 3.6, therefore also for arbitrary fields of characteristic zero.

4. Isotrivial abelian varieties with bounded ranks in $\hat{\mathbb{Z}}$ or $\hat{\mathbb{Z}}^{(p)}$-towers

4.1. In the rest of the paper we will give examples of abelian varieties with bounded ranks in towers of function fields over various fields k. Before doing so, let us dispense with a trivial situation: if A is an abelian variety over $k(t)$ with good reduction away from 0 and ∞ and at worst tame ramification at 0 and ∞, then for any d prime to the characteristic of k, the degree of the conductor of A over $k(t^{1/d})$ is bounded independently of d. Geometric rank bounds then show that the rank of A over $k(t^{1/d})$ is also bounded independently of d. Therefore it is only interesting to consider situations where the degree of the conductor grows in the tower under consideration. All our examples below are of this type.

4.2. We review some well-known facts about constant and isotrivial abelian varieties. Let k be any field, let L be the function field of a geometrically irreducible curve $\mathcal{C}$ smooth and proper over $\operatorname{Spec} k$, and let J be the Jacobian of $\mathcal{C}$. Let A_0 be an abelian variety over k and let $A = A_0 \times_k L$. Then it is clear that $A(L)$, the group of L-rational points of A, is canonically isomorphic to $\mathrm{Mor}_k(\mathcal{C}, A_0)$, the group of k-scheme morphisms from $\mathcal{C}$ to A_0. Moreover, we have an exact sequence

$$0 \to A_0(k) \to \mathrm{Mor}_k(\mathcal{C}, A_0) \to \mathrm{Hom}_{k\text{-av}}(J, A_0)$$

where a k point of A_0 is sent to the constant map with that value and a morphism from $\mathcal{C}$ to A_0 is sent to the homomorphism of abelian varieties induced by Albanese functoriality. If $\mathcal{C}$ has a k-rational divisor of degree 1 (for example if k is finite) then the last map above is surjective. If k is finitely generated over its prime field, then by the Lang-Néron theorem, $A_0(k)$ is finitely generated. (See [Con06] for a modern treatment of the Lang-Néron theorem.) For any k, $\mathrm{Hom}_{k\text{-av}}(J, A_0)$ is finitely generated and torsion free. If A_0 is k-simple, then the rank of $\mathrm{Hom}_{k\text{-av}}(J, A_0)$ is equal to the rank of the endomorphism ring of A_0 times the multiplicity with which A_0 appears in J up to k-isogeny.

4.3. Continuing with the notation of the last subsection, suppose that $\mathcal{C}$ is hyperelliptic, i.e., we are given a degree 2 morphism $\mathcal{C} \to \mathbb{P}^1$. Let A' be the twist of $A = A_0 \times_k k(t)$ by the quadratic extension $L/k(t)$. Since there are no non-constant morphisms from $\mathbb{P}^1$ to an abelian variety, we have $A(k(t)) = A_0(k)$. Since

$$A(L) \otimes \mathbb{Q} \cong (A(k(t)) \otimes \mathbb{Q}) \bigoplus (A'(k(t)) \otimes \mathbb{Q})$$

we conclude that $A'(k(t))$ has finite rank, bounded above by

$$\dim_{\mathbb{Q}} \operatorname{Hom}_{k\text{-av}}(J, A_0) \otimes \mathbb{Q} = \operatorname{Rank}_{\mathbb{Z}} \operatorname{Hom}_{k\text{-av}}(J, A_0) \tag{4.3.1}$$

with equality when $\mathcal{C}$ has a k-rational divisor of degree 1.

4.4. We can now apply the rank formula above and our results about Fermat Jacobians to give examples of bounded ranks in towers. Let $K_1 = k(t)$ and for every positive integer d not divisible by the characteristic of k, let $K_d = k(t^{1/d})$. If the characteristic of k is not 2, let $L_1 = k(u)$ with $u^2 = t - 1$; if the characteristic of k is 2, let $L_1 = k(u)$ with $u^2 + u = t$. For all d prime to the characteristic of k, let $L_d = L_1 K_d = k(t^{1/d}, u)$. Note that L_d is the function field of a hyperelliptic curve C_d over k. Using ideas analogous to [Ulm07, §6], one checks easily that there is a totally ramified, surjective morphism from a Fermat curve $F_n \to \mathcal{C}_d$; here $n = 2d$ if the characteristic of k is not 2 and $n = d$ if the characteristic of k is 2. It follows that the Jacobian of C_d is an isogeny factor of J_n. Applying the rank formula 4.3.1 and Theorems 3.2 and 3.3 we have the following.

4.5. Theorem. *Let k be a field and A_0 an abelian variety over k. If the characteristic of k is $p > 0$, assume that A_0 is isogenous to a product of k-simple abelian varieties each with positive p-rank. Let $A = A \times_k k(t)$ and let A' be the twist of A by the quadratic extension $k(u)/k(t)$ where u satisfies $u^2 = t - 1$ if the characteristic of k is not 2 and $u^2 + u = t$ if the characteristic of k is 2. Then the rank of the Mordell-Weil group $A'(k(t^{1/d}))$ is bounded as d varies through all positive integers relatively prime to the characteristic of k.*

5. Non-isotrivial elliptic curves with bounded ranks in $\mathbb{Z}_\ell$-towers

5.1. For examples of non-isotrivial elliptic curves with bounded ranks in $\mathbb{Z}_\ell$ extensions, we consider the curve E discussed in [Ulm02] with affine equation

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

over $\mathbb{F}_p(t)$.

5.2. Theorem. *Given p let S be the set of primes $\ell > 3$ such that $p \equiv 1 \pmod{\ell}$. If d is a product of powers of primes from S, then the rank of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is zero.*

The proof of the theorem will will be given in the rest of this section.

5.3. We use the notation of Subsection 2.3 on Jacobi sums. Given p, d prime to p, and $\mathbf{a} = (a_0, \dots, a_3) \in A_{d,2}$, we say that $\mathbf{a}$ is "supersingular" (some authors would say "pure") if for one (and thus every) $q = p^f \equiv 1 \pmod{d}$ and all $s \in (\mathbb{Z}/d\mathbb{Z})^\times$ we have

$$\sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\langle \frac{sp^j a_i}{d} \right\rangle = 2f.$$

If $\mathbf{a}$ is supersingular, then for every prime $\wp$ of $\mathbb{Q}(\mu_d)$ over p, the valuation $\mathrm{ord}_\wp J_q(\mathbf{a})$ is f and this implies that $J_q(\mathbf{a})$ is a root of unity times q; this is the motivation for the terminology "supersingular".

5.4. By [Ulm02, 6.4 and 7.7], if $(d, 6p) = 1$, then the rank of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is equal to the number of elements $t \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\}$ such that $\mathbf{a} = (t, -6t, 2t, 3t)$ is supersingular. We are going to show that for suitable d there are no supersingular $\mathbf{a}$ of this form by using a descending induction based on the following elementary identity. Suppose that $a \in \mathbb{Z}/d\mathbb{Z}$, ℓ is a prime such that $\ell^2 | d$ and $\ell \nmid a$. Let H be the cyclic subgroup of $(\mathbb{Z}/d\mathbb{Z})^\times$ generated by $1 + d/\ell$. Then we have

$$\sum_{s \in H} \left\langle \frac{sa}{d} \right\rangle = \left\langle \frac{a}{d/\ell} \right\rangle + \frac{\ell - 1}{2}.$$

It follows that if $\mathbf{a} = (a_0, \dots, a_3) \in A_{d,2}$, $\ell^2 | d$, $\ell \nmid a_i$ for all i, and if $\mathbf{a}$ is supersingular, then its image in $A_{d/\ell}$ is also supersingular. Indeed, we have

$$2f\ell = \sum_{s \in H} \sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\langle \frac{sp^j a_i}{d} \right\rangle = \sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\langle \frac{p^j a_i}{d/\ell} \right\rangle + 2f(\ell - 1)$$

and similarly if a is replaced by ta with $t \in (\mathbb{Z}/d\mathbb{Z})^\times$.

5.5. We can now prove the theorem. Suppose given p and d which is a product of primes in S. If the rank of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ were positive, then we would have a $t \in \mathbb{Z}/d\mathbb{Z}$ such that $\mathbf{a} = (t, -6t, 2t, 3t)$ is supersingular. Without loss of generality we may assume that $t \in (\mathbb{Z}/d\mathbb{Z})^\times$ and then that $\mathbf{a} = (1, -6, 2, 3)$. Applying the observation of the previous subsection repeatedly, we may "reduce the level" and find a d' which is a product of distinct primes from S such that $(1, -6, 2, 3) \in A_{d',2}$ is supersingular. But for such a d' we have $f = 1$, i.e., $p \equiv 1 \pmod{d'}$ and with this one easily checks that

$$\sum_{i=0}^{3} \sum_{j=0}^{f-1} \left\langle \frac{p^j a'_i}{d'} \right\rangle = \sum_{i=0}^{3} \left\langle \frac{a'_i}{d'} \right\rangle = 1 \neq 2f$$

and so we arrive at a contradiction to the assumption that $E(\overline{\mathbb{F}}_p(t^{1/d}))$ has positive rank. This completes the proof of the Theorem.

5.6. The theorem shows that for any prime p such that $p - 1$ is not a power of 2 times a power of 3, there is an elliptic curve over $\mathbb{F}_p(t)$ with bounded rank in a $\mathbb{Z}_\ell$ tower $\overline{\mathbb{F}}_p(t^{1/\ell^n})$ for suitable ℓ. We will prove a stronger result for certain small p not of this type (namely $p = 2, 3, 5, 7$) in the next section and so it seems likely that this kind of statement holds for all p.

In the same direction, it seems quite likely that a more refined analysis would show that given p, and for E as above, the rank of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is bounded as d runs through all integers which are products of powers of primes ℓ such that no power of p is congruent to -1 modulo ℓ.

Generalizing in another direction, a geometric analysis as in [Ulm02, §5] applied to the curves in [Ulm07, §7] might allow one to prove a version of Theorem 5.2 for higher dimensional abelian varieties.

Finally, we note that it is not hard to deduce from Theorem 5.2 that the curve defined over $\mathbb{Q}(t)$ by the equation $y^2 + xy = x^3 - t$ has bounded rank over $\overline{\mathbb{Q}}(t^{1/d})$ as d ranges over all positive integers. We omit the details since similar results were shown by Shioda [Shi86, Cor. 9] using closely related techniques.

6. Non-isotrivial elliptic curves with bounded ranks in $\hat{\mathbb{Z}}^{(p)}$-towers

6.1. We will use completely different techniques, unrelated to Fermat varieties, to give a few examples of non-isotrivial elliptic curves with bounded ranks in towers $\overline{\mathbb{F}}_p(t^{1/d})$ as d ranges over all integers prime to p.

6.2. Theorem. *If $p \in \{2, 3, 5, 7, 11\}$ then there exists an elliptic curve E over $\mathbb{F}_p(t)$ with $j(E) \notin \mathbb{F}_p$ such that the rank of $E(\overline{\mathbb{F}}_p(t^{1/d}))$ is zero for all positive integers d prime to p.*

The proof of the theorem, which uses ideas from [Ulm91], will be given in the rest of this section.

6.3. Given an elliptic curve E over $\mathbb{F}_p(t)$ with $j(E) \notin \mathbb{F}_p$, choose a non-zero invariant differential ω on E and let $\Delta = \Delta(E, \omega)$ and $A = A(E, \omega)$ be the discriminant and Hasse invariant of E; the definition of the latter is reviewed in [Ulm91, §2]. Our assumptions imply that Δ and A are non-zero elements of $\mathbb{F}_p(t)$.

Consider the following conditions on E:

- E has good or multiplicative reduction at $t = 0$ and $t = \infty$.
- At every finite non-zero place of $\mathbb{F}_p(t)$, E obtains good reduction over a tamely ramified extension.
- At every finite non-zero place v of $\mathbb{F}_p(t)$, we have

$$\frac{\mathrm{ord}_v(A)}{p-1} - \frac{\mathrm{ord}_v(\Delta)}{12} < \frac{1}{p}.$$

Note that the third condition is automatic at places where E has good ordinary reduction, in particular at places where A and Δ are units. Note also that if E satisfies these conditions then it continues to satisfy them over the extensions $\mathbb{F}_q(t^{1/d})$ for any power q of p and any d prime to p.

6.4. It follows from [Ulm91, Section 3 and the first sentence of Section 6] that an elliptic curve over $\mathbb{F}_p(t)$ satisfying the conditions of the previous subsection has rank 0 or 1 over any extension $K = \mathbb{F}_q(t^{1/d})$. To see this, we consider the Frobenius and Verschiebung isogenies

$$E \xrightarrow{Fr} E^{(p)} \xrightarrow{V} E$$

whose composition is multiplication by p. Section 3 of [Ulm91] computes the Selmer groups for Fr and V in terms of the reduction types of E, A, and Δ. Under the conditions of the previous subsection, the results are that $\mathrm{Sel}(K, V) = 0$; $\mathrm{Sel}(K, Fr)$

is zero if E has good reduction at 0 or ∞; and $\mathrm{Sel}(K, Fr)$ has order p if E has multiplicative reduction at both 0 and ∞.

We have an exact sequence

$$E^{(p)}(K) \to \mathrm{Sel}(K, Fr) \to \mathrm{Sel}(K, p) \to \mathrm{Sel}(K, V)$$

and so the Selmer group for p is either trivial or of order p. In the examples we give below, when $\mathrm{Sel}(K, Fr)$ is non-trivial, there is a point of order p in $E^{(p)}(K)$ mapping to a generator of $\mathrm{Sel}(K, Fr)$ and so $\mathrm{Sel}(K, p) = 0$ and $E(K)$ has rank 0.

6.5. We now give explicit examples of elliptic curves satisfying our conditions.

Suppose $p = 2$ and let E be defined by

$$y^2 + (t-1)xy + (t-1)^2 y = x^3.$$

If $\omega = dx/((t-1)x + (t-1)^2)$, then $A = (t-1)$, $\Delta = t(t-1)^8$, and $j = (t-1)^4/t$. Standard methods show that E has good, ordinary reduction away from 0, 1, and ∞; that E has multiplicative reduction at 0 and ∞; and that at $t = 1$, E obtains good reduction over an extension with ramification index 3 and the inequality involving A and Δ is satisfied. The point $(x, y) = ((t-1)^2, (t-1)^3)$ on $E^{(2)}$ has order 2 and maps non-trivially to $\mathrm{Sel}(K, Fr)$ and so $\mathrm{Sel}(K, 2) = 0$ for all $K = \mathbb{F}_q(t^{1/d})$.

If $p = 3$, let E be defined by

$$y^2 = x^3 + (t-1)^2 x^2 + t(t-1)^3 x.$$

If $\omega = dx/2y$, then $A = (t-1)^2$, $\Delta = -t^2(t-1)^9$, and $j = -(t-1)^3/t^2$. Standard methods show that E has good, ordinary reduction away from 0, 1, and ∞; that E has multiplicative reduction at 0 and ∞; and that at $t = 1$, E obtains good reduction over an extension with ramification index 4 and the inequality involving A and Δ is satisfied. The points $(x, y) = (t^2(t-1)^4, \pm t^2(t-1)^6)$ on $E^{(3)}$ have order 3 and map non-trivially to $\mathrm{Sel}(K, Fr)$ and so $\mathrm{Sel}(K, 3) = 0$ for all $K = \mathbb{F}_q(t^{1/d})$.

If $p = 5$, let E be defined by

$$y^2 = x^3 + 3(t-1)^4 x + (t+1)(t-1)^5.$$

If $\omega = dx/2y$, then $A = (t-1)^4$, $\Delta = 2t(t-1)^{10}$, and $j = (t-1)^2/2t$. Standard methods show that E has good, ordinary reduction away from 0, 1, and ∞; that E has multiplicative reduction at 0 and ∞; and that at $t = 1$, E obtains good reduction over an extension with ramification index 6 and the inequality involving A and Δ is satisfied. The points with x coordinate $2(t-1)^8(t^2 \pm 2t - 1)$ on $E^{(5)}$ have order 5 and map non-trivially to $\mathrm{Sel}(K, Fr)$ and so $\mathrm{Sel}(K, 5) = 0$ for all $K = \mathbb{F}_q(t^{1/d})$.

If $p = 7$, let E be defined by

$$y^2 = x^3 + (t-1)(t+1)^3 x + 5(t-1)(t+1)^5.$$

If $\omega = dx/2y$, then $A = (t-1)(t+1)^5$, $\Delta = 2(t-1)^2(t+1)^9$, and $j = 4(t-1)$. Standard methods show that E has good, ordinary reduction away from ± 1 and ∞; that E has multiplicative reduction at ∞; that at $t = 1$, E obtains good reduction over an extension with ramification index 6 and the inequality involving A and Δ is satisfied; and that at $t = -1$, E obtains good reduction over an extension with ramification index 4 and the inequality involving A and Δ is satisfied. It follows that $\mathrm{Sel}(K, 7) = 0$ for all $K = \mathbb{F}_q(t^{1/d})$.

If $p = 11$, let E be defined by

$$y^2 = x^3 + 8(t-1)(t+1)^3 x + 2(t-1)(t+1)^5.$$

If $\omega = dx/2y$, then $A = (t-1)^2(t+1)^8$, $\Delta = 9(t-1)^2(t+1)^9$, and $j = 5(t-1)$. Standard methods show that E has good, ordinary reduction away from ± 1 and ∞; that E has multiplicative reduction at ∞; that at $t = 1$, E obtains good reduction over an extension with ramification index 6 and the inequality involving A and Δ is satisfied; and that at $t = -1$, E obtains good reduction over an extension with ramification index 4 and the inequality involving A and Δ is satisfied. It follows that $\mathrm{Sel}(K, 11) = 0$ for all $K = \mathbb{F}_q(t^{1/d})$.

6.6. The theory of modular forms modulo p suggests that the strategy employed in this section will not work for large p. Nevertheless, I conjecture that for all p there are elliptic curves (indeed, absolutely simple abelian varieties of any dimension) over $\mathbb{F}_p(t)$ which have bounded Mordell-Weil ranks in the tower $\overline{\mathbb{F}}_q(t^{1/d})$.

Acknowledgements

It is a pleasure to thank Jordan Ellenberg for his stimulating questions about ranks of elliptic curves as well as Brian Conrey, Bill McCallum, and Dinesh Thakur for their help. Special thanks are due to Bjorn Poonen for several incisive remarks and for pointing out that some arguments originally given for elliptic curves apply more generally to higher-dimensional abelian varieties.

References

[Aok91] N. Aoki, *Simple factors of the Jacobian of a Fermat curve and the Picard number of a product of Fermat curves*, Amer. J. Math. **113** (1991), 779–833.

[BG97] P. Bayer and J. González, *On the Hasse-Witt invariants of modular curves*, Experiment. Math. **6** (1997), 57–76.

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

[Dav00] H. Davenport, *Multiplicative number theory*, Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000.

[Ell06] J. S. Ellenberg, *Selmer groups and Mordell-Weil groups of elliptic curves over towers of function fields*, Compos. Math. **142** (2006), 1215–1230.

[Fas97] L. A. Fastenberg, *Mordell-Weil groups in procyclic extensions of a function field*, Duke Math. J. **89** (1997), 217–224.

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

[Kob78] N. Koblitz, *Gamma function identities and elliptic differentials on Fermat curves*, Duke Math. J. **45** (1978), 87–99.

[Ogu82] A. Ogus, *Hodge cycles and crystalline cohomology*, Hodge cycles, motives, and Shimura varieties, Lecture Notes in Mathematics, vol. 900, Springer-Verlag, Berlin, 1982, pp. 357–414.

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

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

[Sil04] ———, *The rank of elliptic surfaces in unramified abelian towers*, J. Reine Angew. Math. **577** (2004), 153–169.

[Sti87] P. F. Stiller, *The Picard numbers of elliptic surfaces with many symmetries*, Pacific J. Math. **128** (1987), 157–189.

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

[Tat68] J. T. Tate, *Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)*, Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363, Lecture Notes in Mathematics, Vol. 179, Springer-Verlag, Berlin, 1971, pp. 95–110.

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

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

[Ulm07] ———, *L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields*, Invent. Math. **167** (2007), 379–408.

[Was97] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[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