TORSION IN RANK 1 DRINFELD MODULES AND THE UNIFORM BOUNDEDNESS CONJECTURE

BJORN POONEN

Abstract. It is conjectured that for fixed A, $r \geq 1$, and $d \geq 1$, there is a uniform bound on the size of the torsion submodule of a Drinfeld A-module of rank r over a degree d extension L of the fraction field K of A. We verify the conjecture for $r = 1$, and more generally for Drinfeld modules having potential good reduction at some prime above a specified prime of K. Moreover, we show that within an $\overline{L}$-isomorphism class, there are only finitely many Drinfeld modules up to isomorphism over L which have nonzero torsion. For the case $A = \mathbb{F}_q[T]$, $r = 1$, and $L = \mathbb{F}_q(T)$, we give an explicit description of the possible torsion submodules. We present three methods for proving these cases of the conjecture, and explain why they fail to prove the conjecture in general. Finally, an application of the Mordell conjecture for characteristic p function fields proves the uniform boundedness for the $\mathfrak{p}$-primary part of the torsion for rank 2 Drinfeld $\mathbb{F}_q[T]$-modules over a fixed function field.

1. Conjectures and Theorems

In a 1977 paper, Mazur [13] proved that if E is an elliptic curve over $\mathbb{Q}$, its torsion subgroup is one of the following fifteen groups:

$$\mathbb{Z}/N\mathbb{Z}, \qquad 1 \leq N \leq 10 \text{ or } N = 12;$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \qquad 1 \leq N \leq 4.$$

In particular, there is a uniform bound for the size of the torsion subgroup of an elliptic curve over $\mathbb{Q}$. (Although this in recent years has often been called Ogg's conjecture, it was essentially formulated by Levi [11] in 1908, and was again formulated by Nagell [15] in 1949, before the appearance of Ogg's paper [16] in 1971. See [19] for more history.)

Recently, this has been generalized to arbitrary number fields. Merel [14] proved that for every $d \geq 4$, the order of the torsion subgroup of an elliptic curve E over a number field K of degree d over $\mathbb{Q}$ is divisible only by primes less than $2^{d+1}(d!)^{5d/2}$. Earlier results of Kamienny and Mazur [10] and Abramovich [1] established bounds for $d \leq 14$. Also, Kamienny and Mazur [10] proved that the exponent of each such prime is bounded, with the bound depending only on d. (Earlier work of Manin [12] proved the boundedness of each exponent for fixed K.) Together, these results imply that there is a bound $N(d)$ depending only on d such that the order of the torsion subgroup of an elliptic curve over a number field of degree d over $\mathbb{Q}$ is at most $N(d)$. This paper considers the analogous questions for Drinfeld modules.

Date: June 19, 1995.

1991 *Mathematics Subject Classification.* Primary 11G09.

Key words and phrases. Drinfeld module, torsion, uniform boundedness, local height function, sign-normalized.

This research was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. Research at MSRI is supported in part by NSF grant DMS-9022140.

For an introduction to the theory of Drinfeld modules see [9] or Drinfeld's original paper [4]. As usual in this theory, let A denote the ring of regular functions on the affine curve obtained by deleting a closed point "∞" from a nonsingular projective curve X over $\mathbb{F}_q$. Let K be the fraction field of A. In this paper, we will always equip a field extension L of K with the inclusion homomorphism $A \to L$. In this context it makes sense to speak of rank r Drinfeld A-modules over L, for each $r \geq 1$. If ϕ is such a Drinfeld module, ${}^\phi L$ will denote the additive group of L equipped with the A-module structure coming from ϕ, and $({}^\phi L)_{\text{tors}}$ will denote its torsion submodule; i.e.,

$$({}^\phi L)_{\text{tors}} = \{\, \alpha \in L \mid \phi_a(\alpha) = 0 \text{ for some nonzero } a \in A \,\}.$$

Finally, $\#S$ will denote the cardinality of a set S. It is known (see [3], for example) that if L is a finite extension of K, then $\#({}^\phi L)_{\text{tors}} < \infty$.

The following two conjectures (a weak and a strong form) would give natural analogues of the recent results on uniform boundedness for elliptic curves.

Conjecture 1. For fixed A, $r \geq 1$, and finite extension L of K, there is a uniform bound on $\#({}^\phi L)_{\text{tors}}$ as ϕ ranges over rank r Drinfeld A-modules over L.

Conjecture 2. For fixed A, $r \geq 1$, and $d \geq 1$, there is a uniform bound on $\#({}^\phi L)_{\text{tors}}$ as L ranges over extensions of K of degree less than or equal to d, and ϕ ranges over rank r Drinfeld A-modules over L.

One might ask if there is a uniform bound over an even larger class of Drinfeld modules. It is certainly not reasonable to ask for a uniform bound if d is not fixed, because for any Drinfeld module ϕ over a function field L, the torsion submodule over $\overline{L}$ is infinite. If L is fixed, but r is allowed to vary, then again one cannot hope for a uniform bound on the torsion, because if V is any finite sub-$\mathbb{F}_q$-vector space in $K = \mathbb{F}_q(T)$, then there is a polynomial of the form

$$\phi_T(x) = Tx + a_1 x^q + a_2 x^{q^2} + \cdots a_r x^{q^r} \in K[x]$$

with zero set V, and this defines a Drinfeld $\mathbb{F}_q[T]$-module ϕ over K whose torsion submodule is of size at least $\#V$.

The first main goal of this paper is to prove the following partial result.

Theorem 1. *Conjecture 2 holds when $r = 1$ (for each A and d).*

In fact, we will show that for almost all rank 1 Drinfeld modules, there is no nontrivial torsion at all!

Theorem 2. *For fixed A and finite extension L of K, there are at most finitely many rank 1 Drinfeld A-modules ϕ over L (up to isomorphism over L) for which $({}^\phi L)_{tors} \neq 0$.*

Theorem 2 fails for rank $r \geq 2$. For example, if $A = \mathbb{F}_q[T]$, $L = K = \mathbb{F}_q(T)$, then each $\alpha \in L^*$ gives rise to a rank 2 Drinfeld module

$$\phi_T(x) = Tx - (\alpha + T)x^q + \alpha x^{q^2}$$

for which $1 \in {}^\phi L$ is torsion. In fact, this gives infinitely many examples with good reduction at a specified place.

For fixed A, there are only finitely many rank 1 Drinfeld modules over L up to isomorphism over the algebraic closure $\overline{L}$. In fact, their number is the class number of A. But each of these $\overline{L}$-isomorphism classes may consist of infinitely many distinct classes of Drinfeld modules up to isomorphism *over* L, and these may have different torsion submodules, as in Theorem 9 below, for example, so these theorems do not follow trivially even if L is fixed. On the other hand, the finiteness of the number of $\overline{L}$-isomorphism classes implies that Theorems 1 and 2 are corollaries of the following two theorems, which apply to Drinfeld modules of arbitrary rank. A *twist* of a Drinfeld module ϕ over L' is a Drinfeld module over L' which becomes isomorphic to ϕ over the algebraic closure.

Theorem 3. *Let ϕ be a Drinfeld A-module over a finite extension L of K. Also fix $d \geq 1$. There exists a uniform bound $C > 0$ (depending on ϕ, A, L, and d) such if ψ is a twist of ϕ over a field extension L' with $[L' : L] \leq d$, then $\#({}^{\psi}L')_{tors} \leq C$.*

Theorem 4. *If ϕ is a Drinfeld module over a finite extension L of K, then at most finitely many of its twists ψ over L have $({}^{\psi}L)_{tors} \neq 0$.*

The elliptic curve analogue of Theorem 4, namely that the torsion subgroups of almost all twists of a fixed elliptic curve over a number field are trivial, is not quite true, but becomes true if we ignore 2-torsion (and also 3-torsion in the case of zero j-invariant).

In fact, we can generalize Theorem 3 further, to the following analogue of a known result for abelian varieties. (To deduce Theorem 3 from the following, let $\mathfrak{p}$ be a prime of K above which lies a prime of good reduction of ϕ, and observe that every twist of ϕ then has potential good reduction at a place above $\mathfrak{p}$.)

Theorem 5. *Fix $r, d \geq 1$, fix A, and fix a prime $\mathfrak{p}$ of A. There exists $C > 0$ such that if L is a finite extension of K of degree at most d and ϕ is a rank r Drinfeld A-module over L with potential good reduction at some prime above $\mathfrak{p}$, then $\#({}^{\phi}L)_{tors} < C$.*

But, as was remarked after the statement of Theorem 2, we cannot generalize Theorem 4 in the same way.

Sections 2, 3 and 4 give three different approaches to proving Theorem 1. The first two, which use local fields and adelic parallelotopes respectively, also prove Theorem 2 and the more general versions (Theorems 3 and 4), and the first also proves Theorem 5. The third, which uses the explicit description of the action of Galois on the abelian extensions obtained by adjoining torsion of sign-normalized rank 1 Drinfeld modules, proves only Theorem 1.

Each method of proof has its own virtues. (So there is reason for providing several proofs for the same theorems, beyond that of simply desiring to exhibit the various techniques that can be used to attack such problems.) The proofs involving local fields are the quickest, and more importantly are the only ones which give Theorem 5. The proofs involving adelic parallelotopes require only computations within the field over which the Drinfeld modules of interest are defined, and this makes them especially suitable for working out specific examples, as we will do in Section 5. The proof involving class field theory gives the best bounds (just slightly worse than linear in the degree of the field, as opposed to exponentially large). In fact, the bounds it gives will be proven to be best possible, up to a constant factor.

Section 6 explains why these three methods fail to verify the conjectures for $r \geq 2$, and proves the following partial result for rank 2, which is analogous to Manin's local result for elliptic curves over number field mentioned above.

Theorem 6. *Let $A = \mathbb{F}_q[T]$ and $K = \mathbb{F}_q(T)$. Fix a prime $\mathfrak{p}$ of A and a finite extension L of K. Then there is a uniform bound on the size of the $\mathfrak{p}$-primary part of the torsion of rank 2 Drinfeld A-modules over L.*

2. Proofs using local fields

As mentioned in the introduction, whenever we have a Drinfeld module over an extension of K, it is understood that the ring homomorphism $A \to L$ is the inclusion map.

Proposition 1. *Let L be a finite extension of the completion $K_{\mathfrak{p}}$ of K at a place $\mathfrak{p}$ other than ∞, and let ϕ be a Drinfeld module over L. Then $({}^{\phi}L)_{tors}$ is finite.*

Proof. If we fix a non-constant $T \in A$, then we may consider ϕ as a Drinfeld $\mathbb{F}_q[T]$-module over L, and the torsion submodule will be the same subset of L, since the torsion submodule can be characterized as the set of elements which have finite orbit under iteration of ϕ_T. Thus without loss of generality assume $A = \mathbb{F}_q[T]$.

Let v be the discrete valuation on L. If $v(x)$ is sufficiently negative, then $v(\phi_T(x))$ is more negative, and is determined by the leading term of ϕ_T. From this, if $g \in A = \mathbb{F}_q[T]$, $v(\phi_g(x))$ will be determined by the leading term in g. In particular (still assuming $v(x)$ is sufficiently negative), $\phi_g(x)$ will not be zero. Hence torsion elements are bounded below in valuation, and their closure is compact. On the other hand, there are no nonzero torsion elements in a neighborhood of zero, because the action of ϕ_T near zero is locally analytically conjugate via a formal A-module isomorphism to multiplication-by-T, and $|T| \le 1$ with respect to the absolute value on L, so in a sufficiently small ball around 0, the entire Drinfeld A-action is analytically conjugate to the standard A-action. Thus the group $({}^{\phi}L)_{\mathrm{tors}}$ is discrete as well as compact, so it is finite. $\square$

Remark . The lemma could sometimes fail if L were allowed to be K_∞ or a finite extension thereof, as can be seen from the analytic uniformization theory. (The same thing happens for elliptic curves: an elliptic curve over a p-adic field has finite torsion, whereas an elliptic curve over $\mathbb{R}$ or $\mathbb{C}$ has infinite torsion.)

Theorem 5 follows immediately from the following quantitative version of Proposition 1 for Drinfeld modules of potential good reduction.

Theorem 7. *Fix $r, d \ge 1$, fix A, and fix a prime $\mathfrak{p}$ of A. There exists $C > 0$ such that if L is a finite extension of $K_{\mathfrak{p}}$ of degree at most d and ϕ is a rank r Drinfeld A-module over L with potential good reduction, then $\#({}^{\phi}L)_{tors} < C$.*

Proof. Pick $T \in \mathfrak{p}$. Any Drinfeld A-module can be considered as a Drinfeld $\mathbb{F}_q[T]$-module (with different but still bounded r and d), so we may assume $A = \mathbb{F}_q[T]$, and $K_{\mathfrak{p}} = \mathbb{F}_q((T))$. This time we equip any finite extension L of $K_{\mathfrak{p}}$ with the valuation v normalized by $v(T) = 1$. If ϕ is a rank r Drinfeld $\mathbb{F}_q[T]$-module over L with potential good reduction, then over the field obtained by adjoining the $(q^r - 1)$-th root of the leading coefficient of ϕ_T to L, it is isomorphic to a Drinfeld module with good reduction. Hence again replacing d by something larger, but bounded, we may assume ϕ has good reduction over L. In other words,

$$\phi_T(x) = Tx + (\text{higher powers of } x) \in O[x],$$

where O is the ring of integers of L. All torsion of ϕ over L is contained in O. If x is in the ideal T^2O, then $v(\phi_T(x)) = v(x)+1$, and then by induction we see that $v(\phi_{T^k}(x)) = v(x)+k$, which implies that the orbit of x under ϕ_T is infinite, and hence x cannot be torsion. Thus $({}^{\phi}L)_{\mathrm{tors}}$ injects (as a group) into O/T^2O, which is of size $q^{2[L:K_{\mathfrak{p}}]} \le q^{2d}$. $\square$

First proof of Theorem 2. Again we may assume $A = \mathbb{F}_q[T]$. Write

$$\phi_T(x) = Tx + a_1 x^q + a_2 x^{q^2} + \cdots a_r x^{q^r}.$$

Every twist ψ of ϕ over L is of the form

$$\psi_T(x) = Tx + u^{q-1}a_1x^q + u^{q^2-1}a_2x^{q^2} + \cdots u^{q^r-1}a_rx^{q^r},$$

for some $u \in \overline{L}^*$. In fact, the requirement that ψ_T have coefficients in L forces $u^n \in L$, where n is the GCD of $q^i - 1$ over all i for which $a_i \neq 0$. It is easy to see that n also equals $\#\operatorname{Aut}(\phi)$.

Let L_v be the completion of L at some finite place, and let F be the field extension obtained by adjoining to L_v all n-th roots of all elements. Since n is prime to char L_v, Kummer theory implies that F is a finite extension of L_v. Every twist ψ of ϕ is isomorphic to ϕ over F, so we obtain an isomorphism

$${}^{\psi}F \xrightarrow{u^{-1}} {}^{\phi}F.$$

If ψ and ψ' are two such Drinfeld modules, then the images of ${}^{\psi}L$ and ${}^{\psi'}L$ intersect nontrivially only if $u \in L$, in which case ψ and ψ' are isomorphic over L. Hence the union of $({}^{\psi}L)_{\text{tors}} \setminus \{0\}$, with ψ ranging over the distinct twists of ϕ over L, injects as a set into $({}^{\phi}F)_{\text{tors}}$, which is finite by Proposition 1. Hence there can be only finitely many such twists ψ for which $({}^{\psi}L)_{\text{tors}}$ is nontrivial. $\square$

3. Proofs using adelic parallelotopes

The torsion submodule of a Drinfeld module over a global field can be characterized as the set of elements where the (global) canonical height is zero, or equivalently where each canonical local height is zero. (See [3] for the global, [17] for the local.) The latter condition can be satisfied at a given place v only when the corresponding absolute value is small, and thus we can construct an adelic parallelotope in which all torsion lies. Making these estimates uniformly over varying Drinfeld modules leads to proofs of our theorems.

For each place $\mathfrak{p}$ of a global function field L, let $\| \; \|_{\mathfrak{p}}$ denote the associated absolute value, normalized so that for each x in the valuation ring $O_{\mathfrak{p}}$ of $\mathfrak{p}$, $\|x\| = \#(O_{\mathfrak{p}}/x)$. The first lemma below bounds the torsion of a Drinfeld module within a certain adelic parallelotope, and the next bounds the number of field elements within such a parallelotope.

Lemma 1. *Let ϕ be a Drinfeld A-module over L. Then for each place $\mathfrak{p}$ of L, there exists $c_{\mathfrak{p}} > 0$ such that for any extension $| \; |$ of $\| \; \|_{\mathfrak{p}}$ to a finite extension E of L, every $\alpha \in ({}^{\phi}E)_{tors}$ satisfies $|\alpha| \leq c_{\mathfrak{p}}$. Moreover one can take $c_{\mathfrak{p}} = 1$ for all but finitely many $\mathfrak{p}$.*

Proof. The case $E = L$ is essentially a restatement of (4) in Proposition 4 and (3) in Proposition 1 of [17], together with the observation (following from (3) in Proposition 4 of [17]) that if some canonical local height function is nonzero at α, then α is not in the torsion submodule. It is clear from the proofs there that the constant $c_{\mathfrak{p}}$ depends only on the absolute values of the coefficients of the polynomials defining the Drinfeld module, so a single constant can be chosen to work for all E. It is important here that $| \; |$ is literally an extension of $\| \; \|_{\mathfrak{p}}$ rather than the corresponding normalized absolute value, which is a power of $| \; |$. $\square$

Lemma 2. *For each place $\mathfrak{p}$ of a global function field L, let $x_{\mathfrak{p}}$ be a positive real number, such that $x_{\mathfrak{p}} = 1$ for all but finitely many $\mathfrak{p}$. Fix one such place $\mathfrak{q}$, and let $k_{\mathfrak{q}}$ denote its residue field. Let M be the number of $\alpha \in L$ such that $\|\alpha\|_{\mathfrak{p}} \leq x_{\mathfrak{p}}$ for all $\mathfrak{p}$. Then either $M = 1$ (i.e., the only such α is 0), or*

$$M \leq \#k_{\mathfrak{q}} \prod_{\mathfrak{p}} x_{\mathfrak{p}}.$$

Proof. This is a special case of Lemma 8 in [2]. The values of the constants in that lemma for this special case come out of its proof and case 3 of the proof of Lemma 7 there. ☐

Proof of Theorem 3. Just as in the proofs in Section 2, we may assume that $A = \mathbb{F}_q[T]$, at the expense of increasing the rank. Write

$$\phi_T(x) = Tx + a_1 x^q + a_2 x^{q^2} + \cdots a_r x^{q^r}.$$

Every twist ψ over L' isomorphic to ϕ over $\overline{L}$ is of the form

$$\psi_T(x) = Tx + u^{q-1} a_1 x^q + u^{q^2-1} a_2 x^{q^2} + \cdots u^{q^r-1} a_r x^{q^r},$$

for some $u \in \overline{L}^*$. The torsion submodule of ψ over L' consists of those $\alpha \in L'$ for which $u\alpha$ is a torsion element of ϕ. Let $E = L'(u)$.

Suppose $u\alpha$ is a torsion element of ϕ. For each place $\mathfrak{p}$ of L, pick a constant $c_\mathfrak{p}$ as in Lemma 1 for ϕ. Let $\mathfrak{P}$ be a place of E above the places $\mathfrak{p}'$ of L' and $\mathfrak{p}$ of L, and let $n(\mathfrak{P}/\mathfrak{p})$ denote local degree. Then $\| \; \|_{\mathfrak{P}}^{n(\mathfrak{P}/\mathfrak{p})^{-1}}$ is an absolute value on E extending $\| \; \|_\mathfrak{p}$. So by Lemma 1,

$$\begin{aligned} \|u\alpha\|_{\mathfrak{P}}^{n(\mathfrak{P}/\mathfrak{p})^{-1}} &\leq c_\mathfrak{p}, \\ \|\alpha\|_{\mathfrak{P}} &\leq c_\mathfrak{p}^{n(\mathfrak{P}/\mathfrak{p}')n(\mathfrak{p}'/\mathfrak{p})} \|u\|_{\mathfrak{P}}^{-1}, \end{aligned} \tag{1}$$

Now fix $\mathfrak{p}'$. If one takes the product of (1) over all places $\mathfrak{P}$ of E above $\mathfrak{p}'$, one obtains

$$\begin{aligned} \|\alpha\|_{\mathfrak{p}'}^{[E:L']} &\leq c_\mathfrak{p}^{[E:L']n(\mathfrak{p}'/\mathfrak{p})} \prod_{\mathfrak{P}|\mathfrak{p}'} \|u\|_{\mathfrak{P}}^{-1}, \\ \|\alpha\|_{\mathfrak{p}'} &\leq c_\mathfrak{p}^{n(\mathfrak{p}'/\mathfrak{p})} \prod_{\mathfrak{P}|\mathfrak{p}'} \|u\|_{\mathfrak{P}}^{-1/[E:L']}. \end{aligned} \tag{2}$$

Fix any prime $\mathfrak{q}$ of L, and let $\mathfrak{q}'$ be an extension to L'. By Lemma 2, the number of $\alpha \in L'$ satisfying (2) for all places $\mathfrak{p}'$ of L' is at most

$$\begin{aligned} & \#k_{\mathfrak{q}'} \prod_{\mathfrak{p}'} \left(c_\mathfrak{p}^{n(\mathfrak{p}'/\mathfrak{p})} \prod_{\mathfrak{P}|\mathfrak{p}'} \|u\|_{\mathfrak{P}}^{-1/[E:L']} \right) \\ \leq \; & (\#k_\mathfrak{q})^{[L':L]} \left(\prod_\mathfrak{p} c_\mathfrak{p}^{[L':L]} \right) \left(\prod_\mathfrak{P} \|u\|_{\mathfrak{P}}^{-1/[E:L']} \right) \\ = \; & \left(\#k_\mathfrak{q} \prod_\mathfrak{p} c_\mathfrak{p} \right)^{[L':L]}, \end{aligned}$$

by the product formula in E applied to u. Thus the size of the torsion submodule of ψ over L' is at most $C^{[L':L]} \leq C^d$, where

$$C = \#k_\mathfrak{q} \prod_\mathfrak{p} c_\mathfrak{p}.$$

☐

Second proof of Theorem 2. Again we may assume $A = \mathbb{F}_q[T]$. Write

$$\phi_T(x) = Tx + a_1 x^q + a_2 x^{q^2} + \cdots a_r x^{q^r}.$$

Every twist ψ of ϕ over L is of the form

$$\psi_T(x) = Tx + f^{(q-1)/n}a_1x^q + f^{(q^2-1)/n}a_2x^{q^2} + \cdots + f^{(q^r-1)/n}a_rx^{q^r}, \tag{3}$$

where n is as in the first proof of Theorem 3 and $f \in L^*$, and the isomorphism type of ψ depends only on the image of f in L^*/L^{*n}.

We claim that there exists a finite set of places S of L and integers m_v for each $v \in S$ such that any $g \in L^*$ can be multiplied by an n-power to obtain f satisfying

1. $v(f) \leq m_v$ if $v \in S$.
2. $0 \leq v(f) \leq n-1$ if $v \notin S$.

Let $\mathcal{D}$ denote the group of degree zero divisors on the curve of which L is the function field, and let $\mathcal{P}$ denote the subgroup of principal divisors. Then the class group $\mathcal{D}/\mathcal{P}$ of L is finite, and multiplication by n maps it surjectively onto $n\mathcal{D}/n\mathcal{P}$, so $n\mathcal{D}/n\mathcal{P}$ is finite as well. Let $D_1, \ldots, D_s$ be representatives for the cosets of $n\mathcal{P}$ in $n\mathcal{D}$. Let S be the set of places of L which occur in $D_1, \ldots, D_n$, and let v_0 be one of these places. (If S is empty, enlarge it so it contains at least one place.) Given g, with principal divisor $(g) = \sum \alpha_v v$, let D be the degree zero divisor $D = \sum \alpha'_v v$ where $\alpha'_v = n\lfloor \alpha_v/n \rfloor$ for $v' \neq v_0$, and α'_{v_0} is set to make the total degree 0. Then by definition of the D_i, we have $-D = D_i + n(u)$ for some i and some $u \in L^*$. So $f \overset{\text{def}}{=} gu^n$ satisfies

$$(f) = (g) + n(u) = (g) - D' - D_i.$$

The coefficient β_v of v in (f) is $\alpha_v \bmod n$ if $v \notin S$. If $v \in S$ but $v \neq v_0$, then β_v is bounded above and below, where the bound depends on the D_i but not on g. Since $\sum_v \beta_v = 0$, and we have lower bounds on each β_v for $v \neq v_0$ which are zero for all but finitely many v, we get also an upper bound on β_{v_0}, as desired.

From now on, we only consider twists ψ of the form (3) with f satisfying the two conditions of the previous paragraph. We claim there is an adelic parallelotope of L (of finite volume) which contains all torsion elements of all such ψ. Let T be the (finite) set of places of L which occur in the factorizations of the nonzero a_i.

First suppose $v \notin S \cup T$. Then $v(f) \leq n-1$ by condition 1 above. If $v(x) \leq -1$, then

$$\begin{aligned} v(f^{(q^r-1)/n}a_rx^{q^r}) - v(f^{(q^i-1)/n}a_ix^{q^i}) &= (q^r - q^i)/n \cdot v(f) + (q^r - q^i)v(x) \\ &\leq (q^r - q^i)(n-1)/n - (q^r - q^i) \\ &< 0, \end{aligned}$$

so the term $f^{(q^r-1)/n}a_rx^{q^r}$ is larger v-adically than all the other terms in (3). In particular it is larger than the term Tx, so $v(\psi_T(x)) < v(x)$. Hence x tends to infinity v-adically under iteration of ψ_T, and so cannot be a torsion element. In other words, the torsion of ψ over L lies within the set where $v(x) \geq 0$.

Now suppose $v \in S \cup T$. Since $v(f) \leq m_v$, we still have

$$v(f^{(q^r-1)/n}a_rx^{q^r}) - v(f^{(q^i-1)/n}a_ix^{q^i}) < 0$$

provided that $v(x) < c_v$ where c_v is sufficiently negative. Then the same argument in the previous paragraph shows that the torsion of ψ lies within the set where $v(x) \geq c_v$.

Thus we have shown that all torsion of ψ over L lies within an adelic parallelotope whose bounds are independent of f, hence independent of ψ. By Lemma 2, there are only finitely many elements $\alpha_1, \ldots, \alpha_M$ within this adelic parallelotope. If α_i is a nonzero torsion element for ψ for a particular f, then $\psi_T(\alpha_i)$ is also torsion, so $\psi_T(\alpha_i) = \alpha_j$ for some j. Rewriting this using (3) shows that f satisfies a algebraic equation, so there are finitely many possibilities for f, for each α_i and α_j. The (finite) union of all these over i and j lists every f for which the twist ψ might have a nonzero torsion element. $\square$

4. Proofs using explicit class field theory

The bounds on the size of the torsion submodule of rank 1 Drinfeld modules given by the proofs of the last two sections grow exponentially in the degree d. In this section we will give a third proof of Theorem 1, and this one will give a much better bound (just slightly worse than linear in d). In fact, the bound we obtain here will be shown to be best possible, up to a constant factor.

The basic tool we use in this section is the explicit description of the action of Galois on the torsion of a sign-normalized Drinfeld module. This lets us determine which torsion elements belong to a particular global field. The main drawback of these methods is that they apply only to rank 1 Drinfeld modules, and hence do not also give a proof of Theorem 3 on twists of Drinfeld modules of higher rank. The quantitative version of Theorem 1 we prove is the following:

Theorem 8. *For fixed A, there is a constant $C > 0$ such that if ϕ is a rank 1 Drinfeld A-module over a global field L with $[L : K] = d$, then*

$$\#({}^{\phi}L)_{tors} \leq C \cdot d \log\log d.$$

For each A, this bound is best possible up to a constant factor.

In the proof, we will need bounds on a characteristic p analogue of the Euler phi-function. If $\mathfrak{m}$ is an ideal of A, we let $|\mathfrak{m}| = \#A/\mathfrak{m}$, $\deg \mathfrak{m} = \dim_{\mathbb{F}_q} A/\mathfrak{m} = \log_q |\mathfrak{m}|$, and $\varphi_A(\mathfrak{m}) = \#(A/\mathfrak{m})^*$. Just as in the classical case, we have

$$\varphi_A(\mathfrak{m}) = |\mathfrak{m}| \cdot \prod_{\mathfrak{p}|\mathfrak{m}} (1 - 1/|\mathfrak{p}|). \tag{4}$$

Lemma 3. *For each A,*

$$\liminf_{|\mathfrak{m}|\to\infty} \frac{\varphi_A(\mathfrak{m}) \log\log |\mathfrak{m}|}{|\mathfrak{m}|}$$

is a (finite) positive real number.

Proof. First we estimate the number of primes of A of given degree. Recall that A is the ring of regular functions on a nonsingular projective curve X minus a closed point ∞. Degree m primes of A correspond to $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-conjugacy classes of points of X (other than ∞) defined over $\mathbb{F}_{q^m}$ but not over any smaller field. By the Riemann hypothesis for curves over finite fields, $\#X(\mathbb{F}_{q^m}) = q^m + O(q^{m/2})$ as m goes to infinity. (The constant implied by the big-O depends on X.) Of the points defined over $\mathbb{F}_{q^m}$, the number defined over smaller fields is at most

$$\sum_{s|m, s\neq m} \#X(\mathbb{F}_{q^s}) \leq \sum_{s=1}^{m/2} \left[q^s + O(q^{s/2})\right] = O(q^{m/2})$$

so there remain $q^m + O(q^{m/2})$ whose field of definition is $\mathbb{F}_{q^m}$. Hence the number of primes of A of degree m is $q^m/m + O(q^{m/2}/m)$. (It does not matter that we ignored the single prime ∞.)

Consider the product $\mathfrak{m}$ of the primes of degree up to n. As is standard, $\Theta(f(n))$ denotes a function which is bounded above and below by positive multiples of $f(n)$. We have

$$\deg \mathfrak{m} = \sum_{m=1}^{n} (q^m/m + O(q^{m/2}/m))m = \Theta(q^n)$$

$$\log\log|\mathfrak{m}| = \log\log q^{\Theta(q^n)} = n\log q + O(1) \tag{5}$$

and

$$\begin{aligned}
\sum_{\deg \mathfrak{p}\le n} \log(1-1/|\mathfrak{p}|) &= \sum_{m=1}^{n} (q^m/m + O(q^{m/2}/m))\log(1-q^{-m}) \\
&= \sum_{m=1}^{n} (q^m/m + O(q^{m/2}/m))(-q^{-m} + O(q^{-2m})) \\
&= \sum_{m=1}^{n} (-1/m + O(q^{-m/2})) \\
&= -\log n + O(1)
\end{aligned}$$

$$\prod_{\deg \mathfrak{p}\le n} (1-1/|\mathfrak{p}|) = \Theta(1/n). \tag{6}$$

(The estimate (6) is an analogue of Mertens' Theorem which was proved independently by Rosen [18], who also computes the constant implied by the Θ notation.) By (4), (5) and (6),

$$\frac{\varphi_A(\mathfrak{m})\log\log|\mathfrak{m}|}{|\mathfrak{m}|} = (n\log q + O(1))\Theta(1/n) = \Theta(1),$$

which proves that the lim inf is finite.

On the other hand, for any ideal $\mathfrak{m}$ of degree n, the number k of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ dividing $\mathfrak{m}$ having degree at least $\log_q n$ is at most $n/\log_q n$, so by (4),

$$\begin{aligned}
\varphi_A(\mathfrak{m})/|\mathfrak{m}| &= \prod_{i=1}^{k}(1-1/|\mathfrak{p}_i|) \prod_{\mathfrak{p}|\mathfrak{m}, \deg \mathfrak{p}<\log_q n} (1-1/|\mathfrak{p}|) \\
&\ge (1-1/q^{\log_q n})^{n/\log_q n} \prod_{\deg \mathfrak{p}<\log_q n} (1-1/|\mathfrak{p}|) \\
&\ge (1-1/\log_q n)\Theta(1/\lfloor \log_q n\rfloor) \quad \text{(by (6))} \\
&= \Theta(1/\log n) \\
&= \Theta(1/\log\log_q|\mathfrak{m}|) \\
&= \Theta(1/\log\log|\mathfrak{m}|),
\end{aligned}$$

which proves that the lim inf is positive. $\square$

Corollary 1. *For each A, there is a constant $c > 0$ such that*

$$|\mathfrak{m}| \le c\,\varphi_A(\mathfrak{m})\log\log\varphi_A(\mathfrak{m})$$

for every ideal $\mathfrak{m}$ of A.

Proof of Theorem 8. Fix a sign-function, and let H_A^+ be the corresponding normalizing field for rank 1 Drinfeld A-modules, which is the minimal field of definition for each sign-normalized Drinfeld A-module. (See [9] for definitions.) Suppose ϕ is a rank 1 Drinfeld A-module over L, and $[L:K]=d$. By Theorem 12.3 in [9], ϕ is isomorphic to some sign-normalized Drinfeld module ψ, which is defined over H_A^+. Let E be a compositum of L and H_A^+ in some algebraic closure of K. Then ϕ and ψ are twists over E, and they become isomorphic over a field extension F obtained by adjoining a single n-th root, where n (as in the proofs of Section 2) equals $\#\operatorname{Aut}(\phi)=q-1$, by Corollary 5.14 in [9]. In particular,

$$({}^{\phi}L)_{\mathrm{tors}} \subset ({}^{\phi}F)_{\mathrm{tors}} \cong ({}^{\psi}F)_{\mathrm{tors}}.$$

Since ψ is of rank 1, $({}^{\psi}F)_{\mathrm{tors}}$ is isomorphic as an A-module to $A/\mathfrak{m}$ for some ideal $\mathfrak{m}$ of A. Let $K_{\mathfrak{m}}$ be the narrow ray class field, which is the field generated over H_A^+ by the $\mathfrak{m}$-torsion of ψ. Section 16 of [9] gives us an isomorphism from $\operatorname{Gal}(K_{\mathfrak{m}}/H_A^+)$ to $(A/\mathfrak{m})^*$, so

$$\begin{aligned}
\varphi_A(\mathfrak{m}) &= \#\operatorname{Gal}(K_{\mathfrak{m}}/H_A^+)\\
&= [K_{\mathfrak{m}}:H_A^+]\\
&\le [F:H_A^+]\\
&\le n[E:H_A^+] \quad \text{(by definition of } F)\\
&= n[LH_A^+:KH_A^+]\\
&\le nd.
\end{aligned}$$

Finally

$$\begin{aligned}
\#({}^{\phi}L)_{\mathrm{tors}} &\le \#({}^{\psi}F)_{\mathrm{tors}}\\
&= |\mathfrak{m}|\\
&\le c\varphi_A(\mathfrak{m})\log\log\varphi_A(\mathfrak{m}) \quad \text{(by Corollary 1)}\\
&\le c(nd)\log\log(nd)\\
&\le C\cdot d\log\log d,
\end{aligned}$$

for some constant C depending only on A.

This is best possible, because for the sequence of $\mathfrak{m}$'s which make the lim inf in Lemma 3 small, if ϕ is a sign-normalized Drinfeld A-module over the narrow ray class field $K_{\mathfrak{m}}$, then

$$d=[K_{\mathfrak{m}}:K]=[K_{\mathfrak{m}}:H_A^+][H_A^+:K]=O(\varphi_A(\mathfrak{m}))=O(|\mathfrak{m}|/\log\log|\mathfrak{m}|)$$

while

$$\#({}^{\phi}L)_{\mathrm{tors}} \ge |\mathfrak{m}|.$$

□

5. Examples

Theorem 2 tells us in particular that over $K=\mathbb{F}_q(T)$, there are only finitely many rank 1 Drinfeld $\mathbb{F}_q[T]$-modules that have nonzero torsion. Here we list them explicitly.

Theorem 9. *Let $A=\mathbb{F}_q[T]$ and $K=\mathbb{F}_q(T)$. Let ϕ be a rank 1 Drinfeld A-module over K.*

Case 1: $q=2$

In this case ϕ is isomorphic to the Carlitz module $\phi_T(x) = Tx + x^2$ over K. For the Carlitz module, $({}^\phi K)_{tors} = \mathbb{F}_2 + \mathbb{F}_2 \cdot T$, and the torsion is isomorphic to $\mathbb{F}_2[T]/(T^2+T)$ as an $\mathbb{F}_2[T]$-module.

Case 2: $q > 2$

If $\phi_T(x) = Tx - (T+c)x^q$ for some $c \in \mathbb{F}_q$, then the torsion submodule $({}^\phi K)_{tors}$ equals $\mathbb{F}_q \subset {}^\phi K$ and is isomorphic to $\mathbb{F}_q[T]/(T+c)$ as an $\mathbb{F}_q[T]$-module. If ϕ is not isomorphic over K to such a Drinfeld module, then $({}^\phi K)_{tors} = 0$.

We will specialize the second proof of Theorem 4, since it is the only one that does not require that we work within field extensions larger than K. The fact that K has class number 1 will simplify matters greatly.

Proof. Let v_g denote the $\mathbb{Z}$-valued discrete valuation on K associated with an irreducible element g of $\mathbb{F}_q[T]$. The only nontrivial valuation not of this form is the one at ∞, the degree function deg.

We have

$$\phi_T(x) = Tx - fx^q$$

for some $f \in \mathbb{F}_q(T)$. Since ϕ is isomorphic over K to any Drinfeld module ψ with

$$\psi_T(x) = Tx - u^{q-1}fx^q$$

for $u \in K^*$, we may assume without loss of generality that $f \in \mathbb{F}_q[T]$. Also, since $\mathbb{F}_q[T]$ is a UFD, we may assume that $v_g(f) < q-1$ for each irreducible $f \in \mathbb{F}_q[T]$. (When $q = 2$, this means that $f = 1$ and ϕ is the Carlitz module.) The set $S \cup T$ in the second proof of Theorem 2 for us is just $\{\infty\}$. Then that proof gives $v_g(\alpha) \geq 0$ for all irreducible g in $\mathbb{F}_q[T]$. In other words, $({}^\phi K)_{\text{tors}} \subset \mathbb{F}_q[T]$.

Suppose $\alpha \subset \mathbb{F}_q[T]$ is of degree at least 1 if $q \neq 2$, and at least 2 if $q = 2$. Then $\deg \alpha^{q-1} \geq 2$, so

$$\begin{aligned}
\deg(f\alpha^q) &> \deg(T\alpha) \\
\deg(\phi_T(\alpha)) &= \deg(f\alpha^q) > \deg \alpha \\
\deg(\phi_{T^n}(\alpha)) &\to \infty
\end{aligned}$$

as n goes to ∞. This implies that α is not a torsion element, because a torsion element has finite orbit under iteration ϕ_T. Thus $({}^\phi K)_{\text{tors}} \subset \mathbb{F}_q$ if $q \neq 2$, and $({}^\phi K)_{\text{tors}} \subset \mathbb{F}_2 + \mathbb{F}_2 \cdot T$ if $q = 2$.

For $q = 2$ (and $f = 1$),

$$\begin{aligned}
\phi_{T+1}(1) &= T \\
\phi_T(T) &= 0
\end{aligned}$$

so $({}^\phi K)_{\text{tors}} = \mathbb{F}_2 + \mathbb{F}_2 \cdot T$ and it is a cyclic module generated by 1 and isomorphic to $\mathbb{F}_2[T]/(T^2+T)$.

For $q > 2$, $({}^\phi K)_{\text{tors}} \subset \mathbb{F}_q$. If $f = T + c$ with $c \in \mathbb{F}_q$, then $\phi_{T+c}(1) = 0$, so it is clear that $({}^\phi K)_{\text{tors}} = \mathbb{F}_q$, and that it is isomorphic to $\mathbb{F}_q[T]/(T+c)$ as an $\mathbb{F}_q[T]$-module. Otherwise $\phi_T(1) = T - f \notin \mathbb{F}_q$, so $1 \notin ({}^\phi K)_{\text{tors}}$, and $({}^\phi K)_{\text{tors}} = 0$. □

6. Uniform bounds for Drinfeld modules of higher rank

In this section we will first explain why the methods of the previous three section fail to prove Conjectures 1 or 2 in general for Drinfeld modules of rank $r \geq 2$, and then prove Theorem 6, which is the only result beyond Theorem 5 that we have in this situation. If we work over a local field (the completion of the global function field at a prime not above ∞), we still have finiteness of the torsion submodule for each individual Drinfeld module by Proposition 1, but on the other hand we will be able to exploit the Tate uniformization Drinfeld modules in the next proposition to construct examples where the torsion submodule over the local field can be arbitrarily large. Let H_A denote the Hilbert class field of A, which is the maximal unramified abelian extension of K in which ∞ splits completely. (See Section 15 of [9].)

Proposition 2. *Let L be a finite extension of the completion of H_A at a place not above ∞. Then for each $r \geq 2$ and nonzero $a \in A$, there exists a rank r Drinfeld module ϕ over L with a torsion element of order a.*

Proof. There exists a rank 1 Drinfeld A-module ψ over L, since the minimal field of definition for any rank 1 Drinfeld A-module is H_A. (See [9].) By replacing ψ with an isomorphic Drinfeld module, we may assume the coefficients of ψ_a for all a lie in the valuation ring O of L. Then O and L both inherit A-module structures from ϕ, and the quotient ${}^{\phi}L/{}^{\phi}O$ as an A-module is isomorphic to the direct sum of a free module of rank $\aleph_0$ with a finite torsion module, by Theorem 2 in [17]. Let $\lambda_1, \lambda_2, \ldots, \lambda_{r-1}$ be elements of ${}^{\phi}L$ whose images in ${}^{\phi}L/{}^{\phi}O$ are A-independent. The A-module Λ generated by the λ_i is discrete since its intersection with ${}^{\phi}O$ is trivial. Let $\phi_a(\Lambda)$ denote the submodule generated by $\phi_a(\lambda_1), \phi_a(\lambda_2), \ldots, \phi_a(\lambda_{r-1})$. Then the quotient of ψ by $\phi_a(\Lambda)$ can be given the structure of a rank r Drinfeld module over L, as in Section 7 of [4] on Tate uniformization, and the image of λ_1 in this quotient has order a. $\square$

The adelic parallelotope method fails when $r \geq 2$, simply because the volume of the parallelotope needed to contain the torsion can be arbitrarily large. For example, suppose $A = \mathbb{F}_q[T]$, $L = K = \mathbb{F}_q(T)$, V is the sub-$\mathbb{F}_q$-vector space of K with basis $\lambda_1, \ldots, \lambda_r$, and ϕ is the rank r Drinfeld A-module with $\ker \phi_T = V$. Then it is not hard to show that the smallest parallelotope of the adeles $\mathbb{A}_K$ containing the T-torsion submodule V has volume $q^{h((\lambda_1:\cdots:\lambda_r))}$, where $h(P)$ denotes the logarithmic Weil height of a point $P \in \mathbb{P}^{r-1}(K)$, and this height can be arbitrarily large.

We cannot apply the method of Section 4 to obtain uniform bounds for torsion of Drinfeld modules of rank $r \geq 2$ until we have more information about the Galois representations arising from such Drinfeld modules. It is perhaps reasonable to expect that the index of the image of the representation is finite for rank r Drinfeld modules ϕ with $\operatorname{End}\phi = A$, but to use this to obtain uniform boundedness of torsion, it would probably be necessary to bound the index uniformly over Drinfeld modules of a given rank. Not much is known regarding uniform boundedness of the index in the classical case either, for the image of Galois for non-CM elliptic curves.

Let us now give the proof of Theorem 6. Manin's proof of the number field analogue required an application of the Mordell conjecture, which had not been proved at the time, but he was able to verify the conjecture in the cases he needed. Similarly, we will need the Mordell conjecture over characteristic p function fields, which was proved by Samuel [21]. I thank Ernst-Ulrich Gekeler for explaining that the necessary hypotheses for the application of the Mordell conjecture (genus at least 2, and non-isotriviality) were essentially known.

Proof of Theorem 6. By Corollary 2.20 in [7], if $n \geq 4$, the genus of the Drinfeld modular curve $X_0(\mathfrak{p}^n)$ exceeds 2, and then the same will hold for the covering $X_1(\mathfrak{p}^n)$. In order to apply the characteristic p Mordell conjecture, we also need to know that $X_1(\mathfrak{p}^n)$ is non-isotrivial; i.e. that it cannot be defined over a finite field, even after base change. Let J be the Jacobian of $X_1(\mathfrak{p}^n)$ for some $n \geq 4$. By [8], J has multiplicative reduction at ∞. Then the criterion of Ogg-Néron-Shafarevich implies that J cannot be defined over a finite field, and so neither can $X_1(\mathfrak{p}^n)$.

By the Mordell conjecture for characteristic p function fields (Theorem 4 in [21]), $X_1(\mathfrak{p}^n)$ has only finitely many L-rational points. In particular, there are only finitely many $j \in L$ for which there might exist a rank 2 Drinfeld module (of that j-invariant) with a $\mathfrak{p}^n$-torsion point. Hence it will suffice to prove that for fixed $j \in L$, there is a uniform bound for the $\mathfrak{p}$-primary torsion of Drinfeld modules of that j-invariant. All rank 2 Drinfeld modules of a given j-invariant are twists of one another, so their torsion is uniformly bounded by Theorem 3. ☐

Theorem 6 could probably be generalized to general A. This would involve calculating the genus of the Drinfeld modular curves for these A, or at least verifying that the genus is eventually at least 2. Such a calculation can be done by starting with the genus formula for $X(1)$ (VI 5.8 in [5]), and applying the Hurwitz formula, using the computation of the contributions of the ramified points in [6].

Finally, it should be mentioned that Tamagawa [20] has developed a theory for the rank 2 case over $A = \mathbb{F}_q[T]$ analogous to Mazur's theory of Eisenstein ideals for modular curves over $\mathbb{Q}$. In particular, he has succeeded in defining the Eisenstein quotient of the Drinfeld modular curves $X_0(\mathfrak{n})$ over K, and has proved the finiteness of the Mordell-Weil group and the prime-to-q part of the Shafarevitch-Tate group for the "minus part" of this Eisenstein quotient. It is not yet clear whether this will lead to information on rational points on the Drinfeld modular curves themselves, which is what is needed to verify the uniform boundedness conjecture for rank 2 Drinfeld $\mathbb{F}_q[T]$-modules. Perhaps it will be necessary to construct analogues of the "winding quotient," which is used in [14] for the classical case.

Acknowledgements

I thank Dan Abramovich for suggesting that I try to prove Theorem 5. I thank J. Felipe Voloch for correcting my history, and for helping me find references for the characteristic p Mordell conjecture. Finally, thanks go to Ernst-Ulrich Gekeler for explaining the other results needed in the proof of Theorem 6.

References

[1] Abramovich, D., Formal finiteness and the torsion conjecture on elliptic curves, to appear in *Astérisque* **228** (1995).

[2] Artin, E. and Whaples, G., Axiomatic characterization of fields by the product formula for valuations, *Bull. AMS* **51** (1945), 469–492.

[3] Denis, L., Hauteurs canoniques et modules de Drinfeld, *Math. Ann.* **294** (1992), 213–223.

[4] Drinfeld, V., Elliptic modules, *Math. USSR Sb.*, **23** (1974), 561–592.

[5] Gekeler, E.-U., *Drinfeld Modular Curves*, Lecture Notes in Math. 1231, Springer-Verlag, 1986.

[6] Gekeler, E.-U., Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern, *Bonner Math. Schriften* **119**, 1980.
[7] Gekeler, E.-U., Fundamental domains of some arithmetic groups over function fields, preprint, 1995.
[8] Gekeler, E.-U. and Reversat, M., Some results on the Jacobians of Drinfeld modular curves, *The Arithmetic of Function Fields*, ed. D. Goss, D. R. Hayes, and M. I. Rosen, de Gruyter, Berlin, 1992.
[9] Hayes, D., A brief introduction to Drinfeld modules, *The Arithmetic of Function Fields*, ed. D. Goss, D. R. Hayes, and M. I. Rosen, de Gruyter, Berlin, 1992.
[10] Kamienny, S. and Mazur, B., Rational torsion of prime order in elliptic curves over number fields, to appear in *Astérisque* **228** (1995), 81–100.
[11] Levi, B., Sull'equazione indeterminata del 3° ordine, *Atti del IV Congresso Internazionale dei matematici, Roma 1908* **2**, 175–177.
[12] Manin, J. The p-torsion of elliptic curves is uniformly bounded, *Math. USSR - Izvestija* **3** (1969), 433–438.
[13] Mazur, B., Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47** (1977), 33–186.
[14] Merel, L., Existence d'une borne uniforme pour les nombres premiers de torsion des courbes elliptiques sur les corps de nombres, preprint, 1994.
[15] Nagell, T., Problems in the theory of exceptional points on plane cubics of genus one, *Den 11te Skandinaviske Matematikerkongress*, Trondheim 1949, Oslo (J. Grundt Tanums Forlag), 71–76.
[16] Ogg, A., Rational points of finite order on elliptic curves, *Inv. Math.* **12** (1971), 105–111.
[17] Poonen, B., Local height functions and the Mordell-Weil theorem for Drinfeld modules, to appear in *Compositio Math.*
[18] Rosen, M., A generalization of Mertens' Theorem, preprint, 1995.
[19] Schappacher, N. and Schoof, R., Beppo Levi and the arithmetic of elliptic curves, preprint, 1995.
[20] Tamagawa, A. The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve, to appear in *Publ. RIMS. Kyoto Univ.*
[21] Samuel, P., Compléments à un article de Hans Grauert sur la conjecture de Mordell, *I.H.E.S. Publ. Math.* **29** (1966), 55–62.

Mathematical Sciences Research Institute, Berkeley, CA 94720-5070, USA
E-mail address: poonen@msri.org