DRINFELD MODULES WITH NO SUPERSINGULAR PRIMES

BJORN POONEN

ABSTRACT. We give examples of Drinfeld modules ϕ of rank 2 and higher over $\mathbf{F}_q(T)$ that have no primes of supersingular reduction. The idea is to construct ϕ so that the associated mod ℓ representations are incompatible with the existence of supersingular primes. We also answer a question of Elkies by proving that such obstructions cannot exist for elliptic curves over number fields.

Elkies [El1] proved that if E is an elliptic curve over $\mathbf{Q}$, then there are infinitely many primes p for which the mod p reduction of E is supersingular. Later [El3] he extended his argument to prove the analogous statement for elliptic curves over number fields having a real place. But over other number fields the question is still open.[1] In this note, we show that the analogous statement for Drinfeld modules over $\mathbf{F}_q(T)$ is *false*: we exhibit Drinfeld modules having no primes of supersingular reduction. The obstruction is obtained from the mod ℓ representations associated to a Drinfeld module. The final section, which may be read independently of the rest of the paper, proves that such obstructions cannot exist for elliptic curves over number fields.

1. Drinfeld modules

The following definitions are to remain in force for the rest of the paper, except for the final section. Let p be a prime, and let q be a power of p. Let $A = \mathbf{F}_q[T]$ and $K = \mathbf{F}_q(T)$. Let L be an A-field; i.e., a field equipped with a ring homomorphism $\iota : A \to L$. The ring of $\mathbf{F}_q$-linear endomorphisms over L of the additive group scheme over L can be described explicitly as the ring of $\mathbf{F}_q$-linear polynomials; i.e., polynomials $f(x) \in L[x]$ satisfying the polynomial identities $f(x+y) = f(x) + f(y)$ and $f(\epsilon x) = \epsilon f(x)$ for all $\epsilon \in \mathbf{F}_q$. We identify this ring with the ring $L\{\tau\}$ of twisted polynomials over L, where τ (which we think of as the q-th power Frobenius operator) satisfies $\tau\alpha = \alpha^q\tau$ for $\alpha \in L$. The identification will be written as follows: if $f \in L\{\tau\}$, then $f(x)$ will denote the $\mathbf{F}_q$-linear polynomial obtained by "applying the operator f to x."

A Drinfeld module over L is a ring homomorphism

$$\begin{aligned} \phi : A &\to L\{\tau\} \\ a &\mapsto \phi_a \end{aligned}$$

Date: December 23, 1997.

Much of this research was done while the author was supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship at Princeton University. This paper has appeared in *Internat. Math. Res. Notices* **1998**, no. 3, 151–159.

[1] As Elkies explains, there is reason to believe that handling the case of elliptic curves over totally imaginary number fields may be genuinely more difficult: heuristics predict far fewer supersingular primes for certain elliptic curves over these fields.

such that for all $a \in A$ the coefficient of τ^0 in ϕ_a is $\iota(a)$, and such that for some $a \in A$, $\phi_a \neq \iota(a) \in L\{\tau\}$. The rank r of ϕ is the exponent of the highest power of τ that appears in ϕ_T. (See [DH], [Ge2], [Go], or [Ha] for an introduction to Drinfeld modules.)

Now temporarily suppose that L is a finite A-field of order q^m. The kernel of ι is generated by an irreducible element $\mathfrak{p} \in A$. The q^m-th power Frobenius acts on the Tate modules of a rank r Drinfeld module ϕ over L, and the characteristic polynomial $P(X)$ of the action is a polynomial of degree r with coefficients in A, whose constant term is necessarily divisible by $\mathfrak{p}$. The Drinfeld module ϕ is said to be *ordinary* if the linear coefficient of $P(X)$ is nonzero modulo $\mathfrak{p}$. At the other extreme, ϕ is said to be *supersingular* if $P(X)$ is congruent to X^r modulo $\mathfrak{p}$. (See [Ge] or [Go] for other equivalent characterizations of supersingularity.)

Remarks. If $r = 1$, then ϕ is both ordinary and supersingular. If $r = 2$, then ϕ is either ordinary or supersingular (but not both), depending on whether the "trace of Frobenius" is divisible by $\mathfrak{p}$. If $r \geq 3$, then ϕ may be ordinary, supersingular, or something in between: there is a range of possibilities corresponding to the various shapes that the $\mathfrak{p}$-adic Newton polygon of $P(X)$ can take.

Now suppose instead that L is a finite extension of K considered as an A-field with ι being the inclusion, that ϕ is a rank r Drinfeld module over L, and that $\mathfrak{q}$ is a prime of L. If the coefficients of ϕ_T are integral at $\mathfrak{q}$ and if the leading coefficient is a $\mathfrak{q}$-adic unit, then we may "reduce ϕ modulo $\mathfrak{q}$" in order to obtain a rank r Drinfeld module over the residue field $\mathbf{F}_\mathfrak{q}$. One says that ϕ has *good reduction* at $\mathfrak{q}$ if there exists a Drinfeld module ψ isomorphic[2] to ϕ over L that can be reduced in this way; otherwise ϕ has *bad reduction* at $\mathfrak{q}$. Any given ϕ will have good reduction except at finitely many primes of L. If ϕ has good reduction at $\mathfrak{q}$, then we say that $\mathfrak{q}$ is an ordinary (or supersingular) prime of ϕ if the reduction is ordinary (resp. supersingular). Our convention will be that if ϕ has bad reduction at $\mathfrak{q}$, then $\mathfrak{q}$ is neither ordinary nor supersingular.

Finally, if $\mathfrak{p}$ is a prime of a global field L, then $\mathrm{Frob}_\mathfrak{p}$ will denote a Frobenius element of the absolute Galois group $\mathrm{Gal}(L^{\mathrm{sep}}/L)$.

2. A simple example

The following will be the prototype for our constructions. Despite its simplicity, many features of the general construction are already present here, and the reader would be well-advised to understand this example thoroughly before proceeding.

Proposition 1. *Suppose that q is odd. Let ϕ be the rank 2 Drinfeld module over K with*

$$\phi_T = T(1-\tau)^2 = T - 2T\tau + T\tau^2.$$

Then ϕ has no primes of supersingular reduction.

Proof. Since the T-adic valuation of the leading coefficient of ϕ_T is not divisible by $q^2 - 1$, ϕ has bad reduction at (T). Let $\mathfrak{p}$ be a finite prime of K other than (T). The T-torsion of ϕ is the 2-dimensional $\mathbf{F}_q$-vector space $\ker((1-\tau)^2)$, which lies in $\overline{\mathbf{F}}_q$ and has a basis $\{1, \alpha\}$ where $\alpha^q - \alpha = 1$. The action of $x \mapsto x^q$ on this basis is given by $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \in GL_2(\mathbf{F}_q)$. The action of $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$ on the same space is the $(\deg \mathfrak{p})$-th power of $x \mapsto x^q$, so it is represented by a matrix of the form $\left[\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right]$. Thus the characteristic polynomial of $\mathrm{Frob}_\mathfrak{p}$ is congruent to $(X-1)^2$ modulo T. In particular, its linear coefficient a is nonzero. But it

[2] A morphism between Drinfeld modules is an $\mathbf{F}_q$-linear polynomial that respects the A-module structures; see [Go].

follows from part 5 of Theorem 4.12.8 in [Go] that a is an element of A of degree at most $(\deg \mathfrak{p})/2$, so a cannot be divisible by $\mathfrak{p}$. Hence ϕ is ordinary at $\mathfrak{p}$. □

Remark. When considered over $\mathbf{F}_q(T^{1/(q^2-1)})$, ϕ acquires good reduction at the place above (T), and the reduction is supersingular.

Remarks. The j-invariant of ϕ in Proposition 1 is $4T^q$, so this example contradicts the main theorem (1.1.6) of [Br]. This is due only to a minor miscalculation in the proof of Lemma (4.1.2) in [Br]: the exponent of $(-\omega(\pi))$ in the right hand side of (4.1.4) and also (4.1.3) should be $(\deg b + 1)(q-1)/2$ instead of $(\deg b + (q-1)/2)(q-1)/2$. Redoing the argument shows that (4.1.11) should be replaced by

$$\left(\frac{\pi}{N_\pi}\right) = \left(\frac{\pi, Tf}{\infty}\right) \prod_{\mathfrak{p}\in S} \left(\frac{\pi}{\mathfrak{p}}\right),$$

so that the "exceptional j-invariants" f for which the method of [Br] does not apply directly are those for which Tf is a square in $\mathbf{F}_q((1/T))$. A similar correction must be made to [Da], but only because that paper makes use of [Br].

Remark. It is impossible to construct a rank 2 Drinfeld module over $\mathbf{F}_q(T)$, q odd, with good ordinary reduction everywhere. A rank 2 Drinfeld module over $\mathbf{F}_q(T)$ with good reduction everywhere is isomorphic to one of the form

$$\phi_T = T + a\tau + b\tau^2$$

with $b \in \mathbf{F}_q^*$. The T^{-1}-adic valuation of $j(\phi) = a^{q+1}/b$ is then even, so ϕ has infinitely many supersingular primes by Brown's theorem (as modified above).

3. More general examples

In this section, we present more examples of Drinfeld modules having no primes of supersingular (or non-ordinary) reduction. It is not our intention to list *all* possibilities in which some mod I representation is incompatible with the existence of supersingular (resp. non-ordinary) primes. Instead the point we make here is simply that there are *many*.

Lemma 2. *Let $a_1, a_2, \ldots, a_r$ be elements of K^*, and ϕ be the rank r Drinfeld module over K with*

$$\phi_T = T(1 - a_1\tau)(1 - a_2\tau)\cdots(1 - a_r\tau).$$

If ϕ has good reduction at (T), then the reduction is ordinary.

Proof. Let v be the discrete valuation on $\mathcal{O} := \mathbf{F}_q[[T]]$. If ϕ has good reduction at (T), then for some $u \in K^*$, the isomorphic Drinfeld module ψ with

$$\psi_T = u^{-1}\phi_T u = T(1 - u^{q-1}a_1\tau)(1 - u^{q-1}a_2\tau)\cdots(1 - u^{q-1}a_r\tau) \tag{1}$$

has coefficients in $\mathcal{O}$ and leading coefficient in $\mathcal{O}^*$. Let $V = \{\, \alpha \in \ker(\psi_T) \mid v(\alpha) > 0 \,\}$, which is an $\mathbf{F}_q$-subspace of $\ker(\psi_T)$. Since the T-adic valuation of the linear coefficient of $\psi_T(x)$ is 1, the theory of Newton polygons implies that $\prod_{\alpha\in V, \alpha\neq 0}(x-\alpha)$ is a nontrivial irreducible factor of $\psi_T(x)$ over $\mathcal{O}$. In particular, V is an irreducible representation of the decomposition group D at (T). But the factorization (1) of ψ_T gives a full flag in $\ker(\psi_T)$ that is D-stable (even $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-stable), so the composition factors of $\ker(\psi_T)$ as D-module are 1-dimensional over $\mathbf{F}_q$. Hence $\dim_{\mathbf{F}_q} V = 1$, and this is equivalent to ψ being ordinary at (T). □

Theorem 3. *Suppose $r \geq 2$, and write $r = r_0 p^k$ with $\gcd(r_0, p) = 1$. Suppose that m is a positive divisor of $q-1$ such that $r_0 m$ does not divide $q-1$. Let $a_1, a_2, \ldots, a_r$ be elements of K^* such that a_i/a_1 is an m-th power in K for each i. Let ϕ be the rank r Drinfeld module over K with*

$$\phi_T = T(1 - a_1\tau)(1 - a_2\tau)\cdots(1 - a_r\tau).$$

Then ϕ has no primes of supersingular reduction.

Proof. By Lemma 2, ϕ cannot be supersingular at (T). The action of Galois on $\ker(1 - a_i\tau)$ is given by a character $\chi_i : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathbf{F}_q^*$ mapping σ to ${}^\sigma\beta_i/\beta_i$ where $\beta_i \in K^{\mathrm{sep}}$ satisfies $\beta_i^{q-1} = a_i^{-1}$. The semisimplification of the mod T representation ρ of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ associated to ϕ is the direct sum of the χ_i.

If $\mathfrak{p} \neq (T)$ is a prime of good reduction for ϕ, then ρ is unramified at $\mathfrak{p}$. Hence each χ_i is unramified at $\mathfrak{p}$. The characteristic polynomial

$$P(X) := X^r + b_1 X^{r-1} + b_2 X^{r-2} + \cdots + b_r \qquad \in A[x]$$

of $\mathrm{Frob}_\mathfrak{p}$ is congruent to $\prod_{i=1}^r (X - \chi_i(\mathrm{Frob}_\mathfrak{p}))$ modulo T.

If in addition ϕ is supersingular at $\mathfrak{p}$, then for $0 < j \leq r$ the coefficient b_j is divisible by $\mathfrak{p}$. But part 5 of Theorem 4.12.8 in [Go] implies that $\deg b_j$ is at most $(j/r)\deg \mathfrak{p}$, so $b_j = 0$ for $0 < j < r$. There exist two roots of the polynomial $X^r + b_r$ modulo T whose ratio is a primitive r_0-th root of unity $\zeta \in \overline{\mathbf{F}}_q$, so we have $\chi_i(\mathrm{Frob}_\mathfrak{p})/\chi_j(\mathrm{Frob}_\mathfrak{p}) = \zeta$ for some i and j. In particular, r_0 divides the order of the character χ_i/χ_j. On the other hand, a_i/a_j is an m-th power in K^*, so the order of χ_i/χ_j divides $(q-1)/m$. Thus r_0 divides $(q-1)/m$, which contradicts the hypothesis. □

Remark. For any $c \in \mathbf{F}_q$ one can easily create similar examples in which it is the action of Galois on the $(T+c)$-torsion that is incompatible with the existence of supersingular primes.

Remark. Naïve heuristics (counting for each $\mathfrak{p}$ the supersingular characterstic polynomials as a fraction of the number of all possible characteristic polynomials) suggest that if $r \geq 4$, then any rank r Drinfeld module ϕ over K with $\mathrm{End}(\phi) = A$ will have at most finitely many supersingular primes. More sophisticated heuristics (analogous to those in [LT]) seem likely to suggest the same. Recent results of Pink [Pi] determine, for any Drinfeld module (having any endomorphism ring), the *density* of primes for which the Newton polygon of the characteristic polynomial of Frobenius assumes a given shape. (But of course, [Br] shows that the set of primes in question can be infinite even when the density is zero.)

Theorem 4. *Let $a_1, a_2, \ldots, a_r$ be elements of K^*. Let ϕ be the rank r Drinfeld module over K with*

$$\phi_T = T(1 - a_1\tau)(1 - a_2\tau)\cdots(1 - a_r\tau).$$

If $\sum_{i=1}^r \eta(a_i)$ is nonzero for every homomorphism $\eta : K^* \to \mathbf{F}_q^*$, then ϕ has ordinary reduction at every prime $\mathfrak{p}$ of good reduction.

Proof. We retain the notation of the proof of Theorem 3. Lemma 2 handles the case $\mathfrak{p} = (T)$, so suppose $\mathfrak{p}$ is a prime of good reduction for ϕ other than (T). By Kummer theory, the condition on the a_i is equivalent to $\sum_{i=1}^r \chi_i(\sigma) \neq 0 \in \mathbf{F}_q$ for all $\sigma \in \mathrm{Gal}(K^{\mathrm{sep}}/K)$. Applying this to $\sigma = \mathrm{Frob}_\mathfrak{p}^{-1}$ and multiplying by $\prod_{i=1}^r \chi_i(\mathrm{Frob}_\mathfrak{p}) \in \mathbf{F}_q^*$, we deduce that the linear coefficient b_{r-1} of the characteristic polynomial $P(X)$ of $\mathrm{Frob}_\mathfrak{p}$ is nonzero modulo T. As before, it follows that b_{r-1} is nonzero modulo $\mathfrak{p}$, so ϕ has ordinary reduction at $\mathfrak{p}$. □

Remark. The condition on the a_i in Theorem 4 is automatically satisfied if $\gcd(r,p)=1$ and a_i/a_1 is a $(q-1)$-th power for each i. In particular, for each $r \geq 2$ and q with $\gcd(r,q)=1$ we obtain infinitely many non-$\overline{K}$-isomorphic examples.

4. Open questions

Suppose that I is a nonzero ideal of A, and that ϕ is a Drinfeld module over K. We will say that the associated mod I representation

$$\rho_I : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to GL_r(A/I)$$

is *compatible* with the existence of infinitely many supersingular (or non-ordinary) primes if there are infinitely many primes $\mathfrak{p}$ of K for which $\rho_I(\mathrm{Frob}_{\mathfrak{p}})$ is conjugate to the action of Frobenius on the I-torsion of a supersingular (resp. non-ordinary) Drinfeld module over the residue field $k_{\mathfrak{p}}$. The examples we have given in previous sections of Drinfeld modules with no supersingular (or non-ordinary) primes had the property that their mod T representations were incompatible with the existence of supersingular (resp. non-ordinary) primes. We can ask if the only obstructions are of this type:

Question 1. Let ϕ be a Drinfeld module over K. If for every nonzero ideal I of A, the mod I representation associated to ϕ is compatible with the existence of infinitely many non-ordinary primes, then does ϕ necessarily have infinitely many non-ordinary primes?

In the analogous question for supersingularity, we should restrict the rank, because of the heuristics mentioned in the previous section.

Question 2. Let ϕ be a Drinfeld module over K of rank $r \leq 3$. If for every nonzero ideal I of A, the mod I representation associated to ϕ is compatible with the existence of infinitely many supersingular primes, then does ϕ necessarily have infinitely many supersingular primes?

The heuristics suggest a positive answer to the following, at least once the rank is allowed to be at least 4.

Question 3. Does there exist a Drinfeld module ϕ over K whose mod I representations are all compatible with the existence of infinitely many supersingular primes, but which nevertheless has only finitely many supersingular primes?

In cases where obstructions exist, we can ask whether they can always be found at a uniformly bounded level:

Question 4. Fix q and r. Does there exist a nonzero ideal I_0 of A with the following property: if ϕ is a rank r Drinfeld module over K, and if for some I the associated mod I representation is incompatible with the existence of infinitely many supersingular (or non-ordinary) primes, then the same is true for the mod I_0 representation?

Finally, it would of course be possible to study similar problems for Drinfeld modules over finite extensions of K.

5. The lack of obstruction for elliptic curves

In light of the examples of this paper, an obvious question is whether there exist elliptic curves over number fields for which one of the associated mod n representations creates an obstruction to the existence of infinitely many supersingular primes. Elkies raised this question already in [El2] (see question 2 on page 35). We prove in Theorem 6 below that there are no elliptic curves for which such obstructions exist. But first we need a lemma

saying that certain mod n representations that "look supersingular" actually come from supersingular elliptic curves.

Lemma 5. *Suppose $n > 0$ and $8|n$. Let p be a prime with $p \equiv -1 \pmod{n}$, and let $q = p^d$ for some $d \geq 1$. If d is even, let M be the identity $I \in GL_2(\mathbf{Z}/n\mathbf{Z})$. If d is odd, let M be any element of $GL_2(\mathbf{Z}/n\mathbf{Z})$ such that $M^2 = I$ and $\det M = -1 \in \mathbf{Z}/n\mathbf{Z}$. Then there exists a supersingular elliptic curve E over $\mathbf{F}_q$ for which the action of Frobenius on $E[n]$ is given by a matrix conjugate to M.*

Proof. First suppose d is even. Let E be any elliptic curve over $\mathbf{F}_p$ with $\#E(\mathbf{F}_p) = p+1$. Then E is supersingular, and the square of the p-th power Frobenius isogeny on E is multiplication by $-p$, which fixes $E[n]$ pointwise, so $E[n] \subset E(\mathbf{F}_q)$, as desired.

If d is odd, the conditions $M^2 = I$ and $\det M = -1$ (and $8|n$) force M to be conjugate to either $A_0 := \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ or $A_1 := \left[\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right]$ in $GL_2(\mathbf{Z}/n\mathbf{Z})$. Let E be an elliptic curve $y^2 = x^3 - cx$ over $\mathbf{F}_p$ with $c \neq 0$. By assumption, $p \equiv -1 \pmod{4}$, so E is supersingular. The action of the q-th power Frobenius on $E[n]$ is represented by a matrix F satisfying $F^2 = I$ and $\det F = q = -1 \in \mathbf{Z}/n\mathbf{Z}$, so F is conjugate to A_0 or A_1. Moreover we can make F conjugate to the desired A_i by choosing c to be a square or not in $\mathbf{F}_p^*$, since this choice determines the conjugacy class of F mod 2. □

Theorem 6. *Suppose that E is an elliptic curve over a number field K. Let*

$$\rho : \mathrm{Gal}(\overline{K}/K) \to GL_2(\mathbf{Z}/n\mathbf{Z})$$

be the associated mod n representation for some fixed $n \geq 1$. Then there exist infinitely many primes $\mathfrak{p}$ of K for which $\rho(\mathrm{Frob}_\mathfrak{p})$ is conjugate to the action of Frobenius on the n-torsion of a supersingular elliptic curve E' over the residue field $k_\mathfrak{p}$.

Proof. We may assume $8|n$. Let L be a Galois extension of $\mathbf{Q}$ containing $K(E[n])$. Fix an embedding $L \hookrightarrow \mathbf{C}$, and let $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$ be the restriction of complex conjugation. By the Chebotarev Density Theorem, there exist infinitely many primes p of $\mathbf{Q}$ for which all of the following hold:

(1) p is unramified in L. (It follows from this that p does not divide n.)
(2) $\mathrm{Frob}_p \in \mathrm{Gal}(L/\mathbf{Q})$ is conjugate to σ. (This condition is the crucial one.[3])
(3) p is not divisible by any prime of bad reduction of E.

We will show that if $\mathfrak{p}$ is any prime of K lying above such p, then $\rho(\mathrm{Frob}_\mathfrak{p})$ is conjugate to the action of Frobenius on the n-torsion of a supersingular elliptic curve E' over the residue field $k_\mathfrak{p}$.

Fix such p and $\mathfrak{p}$, and let d be the degree of $\mathfrak{p}$ over p. The Weil pairing gives a primitive n-th root of unity ζ in L. Since $\zeta^p = \mathrm{Frob}_p(\zeta) = \sigma(\zeta) = \zeta^{-1}$, we find that $p \equiv -1 \pmod{n}$. After replacing σ by a $\mathrm{Gal}(L/\mathbf{Q})$-conjugate if necessary, we have $\sigma^d = \mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$. We obtain the desired E' by applying Lemma 5 to $M = \rho(\mathrm{Frob}_\mathfrak{p})$. □

Remark. It seems that the reason one cannot rule out the existence of supersingular primes based on the mod n representations is that such an argument would also rule out the existence of the primes above infinity, which act as if they were supersingular!

Theorem 6 gives credence to the conjecture that every elliptic curve over a number field has infinitely many supersingular primes.

[3]Interestingly, the same condition appears in Ribet's work on "raising the level" (see [Ri] and [Ri2, Lemma 7.1]) and in Kolyvagin's work.

Acknowledgements

I thank Bruce Jordan for some conversations about the heuristics for the expected number of supersingular primes for Drinfeld modules. I thank also Noam Elkies for providing a copy of his thesis. The final remark of Section 2 arose from a question e-mailed to me by David Goss.

References

[Br] Brown, M. L., Singular moduli and supersingular moduli of Drinfeld modules, *Invent. Math.* **110** (1992), no. 2, 419–439.

[Da] David, C., Supersingular reduction of Drinfel'd modules, *Duke Math. J.* **78** (1995), no. 2, 399–412.

[DH] Deligne, P. and Husemöller, D., Survey of Drinfeld Modules, *Contemp. Math.* **67** (1987), 25–91.

[El1] Elkies, N. D., The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$, *Invent. Math.* **89** (1987), no. 3, 561–567.

[El2] Elkies, N. D., Supersingular primes of a given elliptic curve over a number field, Thesis, Harvard, May 1987.

[El3] Elkies, N. D., Supersingular primes for elliptic curves over real number fields, *Compositio Math.* **72** (1989), no. 2, 165–172.

[Ge] Gekeler, E.-U., On Finite Drinfeld Modules, *J. of Algebra* **141** (1991), 187–203.

[Ge2] Gekeler, E.-U., *Drinfeld Modular Curves*, Lecture Notes in Math. **1231**, Springer-Verlag, Berlin, 1986.

[Go] Goss, D., *Basic structures of function field arithmetic*, Springer-Verlag, Berlin, 1996.

[Ha] Hayes, D. R., A brief introduction to Drinfeld modules, in: *The Arithmetic of Function Fields*, eds. D. Goss, D. R. Hayes, and M. I. Rosen, de Gruyter, Berlin, 1992.

[LT] Lang, S. and Trotter, H., *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Math. **504**, Springer-Verlag, Berlin, 1976.

[Pi] Pink, R., The Mumford-Tate conjecture for Drinfeld modules, to appear in *Publ. Res. Inst. Math. Sci.*

[Ri] Ribet, K., Raising the levels of modular representations, *Séminaire de Théorie des Nombres, Paris 1987–88*, 259–271, *Progr. Math.* **81**, Birkhäuser Boston, Boston, MA, 1990.

[Ri2] Ribet, K., On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu