Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint Nr. 131

On the torsion of optimal elliptic curves over function fields

Mihran Papikian

Saarbrücken 2005

Fachrichtung 6.1 – Mathematik
Universität des Saarlandes

Preprint No. 131
submitted: March 13, 2005

On the torsion of optimal elliptic curves over function fields

Mihran Papikian

Department of Mathematics
Stanford University
Stanford
CA 94305
USA
papikian@math.stanford.edu

Edited by
FR 6.1 – Mathematik
Universität des Saarlandes
Postfach 15 11 50
66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-Mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

ON THE TORSION OF OPTIMAL ELLIPTIC CURVES OVER FUNCTION FIELDS

MIHRAN PAPIKIAN

ABSTRACT. For an optimal elliptic curve E over $\mathbb{F}_q(t)$ of conductor $\mathfrak{p}\cdot\infty$, where $\mathfrak{p}$ is prime, we show that $E(F)_{\mathrm{tor}}$ is generated by the image of the cuspidal divisor group.

1. INTRODUCTION

Let $\mathbb{F}_q$ denote the finite field of q elements. We let p be the characteristic of $\mathbb{F}_q$ (so q is a power of p). Let $F = \mathbb{F}_q(t)$ be the field of rational functions on $\mathbb{P}^1_{\mathbb{F}_q}$, and let $A = \mathbb{F}_q[t]$ be the subring of F consisting of functions which are regular away from $\infty := 1/t$.

Let $\mathfrak{p}$ be a fixed prime ideal of A. Denote by $Y_0(\mathfrak{p})$ the coarse moduli scheme of pairs (D, Z), where D is a rank-2 Drinfeld A-module of general characteristic, and Z is a $\mathfrak{p}$-cyclic subgroup of D; for the definitions see, for example, [3]. The scheme $Y_0(\mathfrak{p})$ is a smooth affine geometrically irreducible curve defined over F. Denote by $X_0(\mathfrak{p})$ the unique smooth compactification of $Y_0(\mathfrak{p})$ over F. Let J be the Jacobian variety of $X_0(\mathfrak{p})$. The complement of $Y_0(\mathfrak{p})$ in $X_0(\mathfrak{p})$ consists of two F-rational points; these are called the *cusps* of $X_0(\mathfrak{p})$. The divisor on $X_0(\mathfrak{p})$ which is the difference of the two cusps generates a finite cyclic subgroup $\mathcal{C}$ of $J(F)$ called the *cuspidal divisor group*. It is known that $\mathcal{C}$ has order $N(\mathfrak{p})$, where $N(\mathfrak{p}) = \frac{q^d-1}{q-1}$, if $d := \deg(\mathfrak{p})$ is odd, and $N(\mathfrak{p}) = \frac{q^d-1}{q^2-1}$ if d is even.

Let $\mathcal{J}$ be the Néron model of J over $\mathbb{P}^1_{\mathbb{F}_q}$. It is known that J has bad reduction only at two places of $\mathbb{P}^1_{\mathbb{F}_q}$, namely at $\mathfrak{p}$ and ∞. In other words, the v-fibre $\mathcal{J}_{\mathbb{F}_v}$ of $\mathcal{J}$ is not an abelian variety over $\mathbb{F}_v$ only when $v = \mathfrak{p}$ or $v = \infty$; here we denote by $\mathbb{F}_v$ the residue field at the place v. Moreover, it is known that the reduction of J at $\mathfrak{p}$ and ∞ is toric, i.e., the connected component of the identity $\mathcal{J}^0_{\mathbb{F}_v}$ is an algebraic torus over $\mathbb{F}_v$ when $v = \mathfrak{p}, \infty$. We denote $\mathcal{J}_{\mathbb{F}_v}/\mathcal{J}^0_{\mathbb{F}_v}$ by $\Phi_{J,v}$; this is a finite abelian group called the *group of connected components of* $\mathcal{J}$ *at* v. By what was said, the groups $\Phi_{J,v}$ are trivial if v is not $\mathfrak{p}$ or ∞. Taking the schematic closure of $\mathcal{C}$ in $\mathcal{J}$ and then specializing to the $\mathfrak{p}$-fibre, we get a natural homomorphism $\mathcal{C} \to \Phi_{J,\mathfrak{p}}$. Gekeler proved [2] that this is an isomorphism. More recently, Pál proved [7] that the inclusion $\mathcal{C} \subset J(F)_{\mathrm{tor}}$ is in fact an equality. These results are the function field analogues of some of the results of Mazur in his celebrated paper [5].

The aim of the present article is to show that for certain one-dimensional quotients of J the F-rational torsion is again cuspidal, i.e., is generated by the image of $\mathcal{C}$. Let E be an elliptic curve over F. We say that E is *optimal* if there is a

Key words and phrases. Elliptic curves, Drinfeld modular curves, cuspidal divisor group.
Supported by a fellowship from the European Postdoctoral Institute.

homomorphism $J \to E$ with connected and smooth kernel (i.e., the kernel is an abelian subvariety of J). An equivalent condition is that E is isomorphic to an abelian subvariety of J. If E is optimal then it has conductor $\mathfrak{p}\cdot\infty$ and the reduction of E at $\mathfrak{p}$ (resp. ∞) is multiplicative (resp. split multiplicative). For E we adopt notations similar to that for J, so, for example, $\mathcal{E}$ will be the Néron model of E over $\mathbb{P}^1_{\mathbb{F}_q}$ and $\Phi_{E,v}$ will be the v-fibre component group of $\mathcal{E}$. The main result is the following:

Theorem 1.1. *Let E be an optimal elliptic curve.*

(1) *The specialization map $E(F)_{\mathrm{tor}} \to \Phi_{E,\mathfrak{p}}$ is an isomorphism. In particular, $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$ acts trivially on $\Phi_{E,\mathfrak{p}}$.*
(2) *The homomorphism $J(F)_{\mathrm{tor}} \to E(F)_{\mathrm{tor}}$, induced from the quotient map $J \to E$, is surjective. In particular, $E(F)_{\mathrm{tor}}$ is generated by the image of the cuspidal divisor group $\mathcal{C}$ in E.*
(3) *$E(F)_{\mathrm{tor}} = \mathbb{Z}/n\mathbb{Z}$ for some $1 \leq n \leq 5$ coprime to p.*
(4) *The order of $\Phi_{E,\mathfrak{p}}$ divides the order of $\Phi_{E,\infty}$.*

This theorem is the function field analogue of a result over $\mathbb{Q}$ due to Mestre and Oesterlé [6]. Emerton [1] generalized Mestre-Oesterlé theorem from elliptic curves to arbitrary abelian subvarieties of the classical modular Jacobians. Both [6] and [1] extensively use in their proofs the results of Mazur [5] and Ribet [10]. One feature which is significantly different in our proof is that we completely avoid using any "level-lowering" results, and from the Eisenstein ideal theory essentially only need Pál's theorem $J(F)_{\mathrm{tor}} = \mathcal{C}$.

Example 1.2. It is remarkable that the possibilities for $E(F)_{\mathrm{tor}}$ in Theorem 1.1(3) exactly match the possibilities for the rational torsion of optimal elliptic curves over $\mathbb{Q}$ of prime conductor (aside from the requirement that n is coprime to p, of course). In fact, Mestre and Oesterlé show that $E(\mathbb{Q})_{\mathrm{tor}} = \mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 5$, and moreover give examples where all the cases occur. Unfortunately, at present we are unable to show that all the possibilities for $E(F)_{\mathrm{tor}}$ actually occur. This is due to lack of many examples of optimal elliptic curves over F. But at least there is an example due to Gekeler, which shows that $E(F)_{\mathrm{tor}}$ is not always trivial. Let $F = \mathbb{F}_7(t)$, and $E/F:\ y^2 = x^3+ax+b$, where $a = -3t(t^3+2)$ and $b = -2t^6+3t^3+1$. Then E is an optimal elliptic curve of conductor $(t^3-2)\cdot\infty$. One easily shows that $\#E(F)_{\mathrm{tor}} = \#\Phi_{E,\mathfrak{p}} = \#\Phi_{E,\infty} = 3$.

The quotient $\#\Phi_{E,\infty}/\#\Phi_{E,\mathfrak{p}}$ is an integer by Theorem 1.1(4), but it can be strictly larger than 1. Here is another example due to Gekeler. Let $F = \mathbb{F}_2(t)$ and $E/F:\ y^2 + txy + y = x^3 + x^2$. Then E is an optimal curve of conductor $(t^4+t^3+1)\cdot\infty$. By computing the j-invariant $j_E = t^{12}/(t^4+t^3+1)$ we conclude that $\Phi_{E,\mathfrak{p}} = 1$ but $\Phi_{E,\infty} = \mathbb{Z}/8\mathbb{Z}$.

The requirement on E being optimal in Theorem 1.1 is necessary. One way to see this is to recall that the rational torsion of elliptic curves over F is universally bounded, whereas the orders of component groups can be made arbitrarily large by taking the Frobenius conjugates of an elliptic curve.

In [9] we gave a formula for the variation of the orders of Tate-Shafarevich groups $Ш(E/K)$ of E over certain quadratic extensions K of F, under the assumption that E/K has analytic rank 0. One of the factors which appears in that formula is the fraction $\#E(F)_{\mathrm{tor}}/\#\Phi_{E,\mathfrak{p}}$. By Theorem 1.1 this fraction is always equal to 1, and hence can be omitted from the formula for $\#Ш(E/K)$. This was our initial motivation for considering the problem of the present article.

Acknowledgement. I thank the Department of Mathematics of University of Saarlandes for its hospitality during the Winter semester of 2004.

2. Proof of the main theorem

Aside from the notation used in the introduction, we will also use the following notation and terminology: For a field L we will denote its algebraic closure by $\bar{L}$, and the separable closure by L^{sep}. By a finite flat group scheme over the base scheme S we always mean a finite flat *commutative* S-group scheme. We say that the finite flat group scheme G over $\mathbb{P}^1_{\mathbb{F}_q}$ is *constant* if it is étale and the action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on $G_F(\overline{F})$ is trivial. We say that G is *μ-type* if its Cartier dual $G^\vee$ is constant. Given an abelian variety B, its dual abelian variety will be denoted by $\hat{B}$. As in [7], let $\mathfrak{E}$ be the *Eisenstein ideal* of the Hecke algebra $\mathbb{T}$, i.e., the ideal generated by the elements $T_\mathfrak{q} - q^{\deg(\mathfrak{q})} - 1$, where $\mathfrak{q} \neq \mathfrak{p}$ is any prime in A. We write $J[\mathfrak{E}]$ for the group of points in $J(\overline{F})$ which are killed by all elements of $\mathfrak{E}$. Let $\widetilde{F} := \overline{\mathbb{F}}_q(t)$. This is the maximal unramified extension of F.

Before giving the proof of Theorem 1.1, we need a preliminary lemma.

Lemma 2.1. *There is an inclusion $J(\widetilde{F})_{\mathrm{tor}} \subset J[\mathfrak{E}]$.*

Proof. Let $G = J(\widetilde{F})_{\mathrm{tor}}$. Since J is not isotrivial, G is finite. We claim that G has order coprime to p. To see this, fix a prime $\mathfrak{P}$ in $\widetilde{A} := \overline{\mathbb{F}}_q[t]$ over $\mathfrak{p}$. Let $k = \widetilde{A}/\mathfrak{P}$. Since $\widetilde{F}/F$ is unramified at $\mathfrak{p}$, the Néron model $\widetilde{\mathcal{J}}$ of $\widetilde{J} := J_{\widetilde{F}}$ over $\widetilde{A}_\mathfrak{P}$ is isomorphic to the base change of $\mathcal{J}$ to the strict henselization of $A_\mathfrak{p}$. In particular, $\Phi_{J,\mathfrak{p}} = \Phi_{\widetilde{J},\mathfrak{P}}$. Suppose G has non-trivial p-torsion. Fix a subgroup $G' \subset G$ of order p. By taking the schematic closure of G' in $\widetilde{\mathcal{J}}_{\widetilde{A}_\mathfrak{P}}$, we get a finite flat group scheme $\mathcal{G}'$ extending G over $\widetilde{A}_\mathfrak{P}$. If $\widetilde{\mathcal{J}}^0_k \cap \mathcal{G}'_k$ is non-trivial, then $\mathcal{G}'_k = \mu_p$ (as $\widetilde{\mathcal{J}}^0_k$ is a torus). This is impossible, since otherwise $(\mathcal{G}')^\vee$ has étale closed fibre but connected generic fibre (μ_p is connected in characteristic p). Hence we get a natural injection $G' \hookrightarrow \Phi_{J,\mathfrak{p}}$. This latter group is known to have no p-torsion, and we get a contradiction.

Next, we claim that G is an extension of a constant group scheme by a μ-type étale group scheme. Since G has order coprime to the characteristic of F (and hence also coprime to the characteristics all residue fields) and is unramified at all places, it extends to a finite étale group scheme $\mathcal{G}$ over $\mathbb{P}^1_{\mathbb{F}_q}$, cf. [4, §2]. It is easy to see that $\mathcal{G}$ is the schematic closure of G in $\mathcal{J}$. So we are reduced to studying the $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-structure of G. The action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on G factors through $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. By fixing a decomposition subgroup D_∞ of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ at ∞, we get a canonical inclusion $\mathrm{Gal}(\overline{\mathbb{F}}_\infty/\mathbb{F}_\infty) \to \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. This latter map is an isomorphism as $\deg(\infty) = 1$. The specialization map $\mathcal{G} \to \mathcal{G}_{\mathbb{F}_\infty}$ commutes with the action of $\mathrm{Gal}(\overline{\mathbb{F}}_\infty/\mathbb{F}_\infty)$, so we are reduced to showing that $\mathcal{G}_{\mathbb{F}_\infty}$ is an extension of a constant group scheme over $\mathbb{F}_\infty$ by a μ-type étale group scheme. On the one hand, Drinfeld modular curves are totally degenerate at infinity, so $\mathcal{J}^0_{\mathbb{F}_\infty}$ is a split torus and by [4, §11] $\Phi_{J,\infty}$ is constant. On the other hand, $\mathcal{G}_{\mathbb{F}_\infty} \hookrightarrow \mathcal{J}_{\mathbb{F}_\infty}$. The claim follows.

Let $\mathcal{S}$ be the maximal μ-type étale subgroup of J. It is clear that $\mathcal{S} \subset G$. We claim that $\mathcal{L} := G/\mathcal{S}$ is a constant group scheme. Indeed, by what we have proved, we can write G as an extension of a constant group scheme by a μ-type étale group scheme. Since $\mathcal{S}$ is the maximal μ-type étale subgroup scheme of J, the group $\mathcal{L}$ must be constant.

It is clear that $\mathcal{S}$ and G are $\mathbb{T}$-modules, and they are also $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-invariant. Hence $\mathcal{L}$ is equipped with a commuting actions of $\mathbb{T}$ and the absolute Galois group, which satisfy the Eichler-Shimura congruence relations. We claim that the extension of $\mathbb{T}$-modules

$$0 \to \mathcal{S} \to G \to \mathcal{L} \to 0$$

in fact splits. The action of $\mathbb{T}$ uniquely extends by the universal property of Néron models to $\mathcal{J}$. Hence we get a natural map $\mathbb{T} \to \mathrm{End}_{\mathbb{F}_\mathfrak{p}}(\mathcal{J}_{\mathbb{F}_\mathfrak{p}})$, which is injective since $\mathcal{J}$ has toric reduction at $\mathfrak{p}$. Since the action of $\mathbb{T}$ on $\mathcal{J}_{\mathbb{F}_\mathfrak{p}}$ is continuous, it preserves $\mathcal{J}^0_{\mathbb{F}_\mathfrak{p}}$. Thus, $\Phi_{J,\mathfrak{p}}$ is naturally a $\mathbb{T}$-module. It is enough to show that the specialization of G to the $\mathfrak{p}$-fibre splits. This specialization provides a map $G \to \Phi_{J,\mathfrak{p}}$, and by restricting to $\mathcal{S}$, a map $\mathcal{S} \to \Phi_{J,\mathfrak{p}}$. This latter homomorphism is an isomorphism by Proposition 8.18 in [7], so the sequence splits as we have produced a $\mathbb{T}$-equivariant retraction $G \to \mathcal{S}$, cf. [5, p.142].

Now it is easy to see that G is annihilated by the Eisenstein ideal. Indeed, as a $\mathbb{T}$-module $G = \mathcal{S} \oplus \mathcal{L}$, and both summands are killed by $T_\mathfrak{q} - q^{\deg(\mathfrak{q})} - 1$, $\mathfrak{q} \neq \mathfrak{p}$, according to the Eichler-Shimura congruence relations. □

Proof of Theorem 1.1. The dual of the optimal quotient map $\pi : J \to E$ is the closed immersion $\hat{\pi} : \hat{E} \hookrightarrow \hat{J}$, which, using the canonical self-duality of E and J, can be identified with a closed immersion $E \hookrightarrow J$. First, we claim that the functorially-induced homomorphism on component groups $\hat{\pi}_\Phi : \Phi_{E,\mathfrak{p}} \to \Phi_{J,\mathfrak{p}}$ is injective. It is enough to show that $\Phi_{E,\mathfrak{p}}[\ell] \to \Phi_{J,\mathfrak{p}}[\ell]$ is injective for any prime ℓ. Moreover, by Corollary 3.4 in [8] we can assume $\ell \neq p$. Suppose $\Phi_{E,\mathfrak{p}}[\ell]$ is nontrivial. Then by [4, §2] the ℓ-torsion of E is unramified at $\mathfrak{p}$. Indeed, according to *loc. cit.* $E[\ell]^{I_\mathfrak{p}}$ is isomorphic to $\mathcal{E}_{\mathbb{F}_\mathfrak{p}}[\ell]$, where $I_\mathfrak{p}$ is the inertia group at $\mathfrak{p}$. Our assumption implies that $\dim_{\mathbb{F}_\ell}(\mathcal{E}_{\mathbb{F}_\mathfrak{p}}[\ell]) = 2$, hence $E[\ell]^{I_\mathfrak{p}} = E[\ell]$ as $\dim_{\mathbb{F}_\ell}(E[\ell]) = 2$. We claim that $E[\ell]$ is in fact everywhere unramified. Since E has good reduction away from $\mathfrak{p}$ and ∞, using the Néron-Ogg-Shafarevich criterion, it is enough to show that $E[\ell]$ is unramified at ∞. It is even enough to show that $E[\ell]$ is at most tamely ramified at ∞. Indeed, $E[\ell]$ is a $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-module as E is defined over F. On the other hand, using Hurwitz genus formula, it is easy to see that F has no extensions ramified exactly at ∞ such that the ramification is tame. Since E has split multiplicative reduction at ∞, we can use Tate's uniformization of E to conclude that $F_\infty(E[\ell]) \subseteq F_\infty(\mu_\ell, \wp_E^{1/\ell})$, where $\wp_E$ is the Tate period of E at ∞. This latter extension of F_∞ is clearly at most tamely ramified. Hence $E[\ell] \subset E(\widetilde{F})$. Since E is an abelian subvariety of J, we have the inclusion $E(\widetilde{F}) \subset J(\widetilde{F})$. Using Lemma 2.1, we get $E[\ell] \subseteq D[\ell]$, where $D[\ell]$ denotes the ℓ-torsion subgroup of $J[\mathfrak{C}]$. According to [7, §§10-11], $\dim_{\mathbb{F}_\ell}(D[\ell]) = 2$, so $E[\ell] = D[\ell]$. There results a commutative functorial diagram

$$\begin{array}{ccc} E[\ell] & \longrightarrow & \Phi_{E,\mathfrak{p}}[\ell] \\ \| & & \downarrow \\ D[\ell] & \longrightarrow & \Phi_{J,\mathfrak{p}}[\ell]. \end{array}$$

The image of $D[\ell]$ in $\Phi_{J,\mathfrak{p}}[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ by Proposition 8.18 in [7] and the description of $D[\ell]$ in Sections 10 and 11 of *loc. cit.* The elliptic curve E has multiplicative reduction at $\mathfrak{p}$, so $\Phi_{E,\mathfrak{p}}$ is cyclic. In particular, $\Phi_{E,\mathfrak{p}}[\ell] \cong \mathbb{Z}/\ell\mathbb{Z}$. Now it is easy to see from the above diagram that $\Phi_{E,\mathfrak{p}}[\ell] \to \Phi_{J,\mathfrak{p}}[\ell]$ must be injective, as we claimed.

Next, we claim that the functorially-induced homomorphism $\pi_\Phi : \Phi_{J,\mathfrak{p}} \to \Phi_{E,\mathfrak{p}}$ is surjective. For an abelian variety B over a local field Grothendieck defined a bifunctorial pairing [4, §1.2]: $\Phi_B \times \Phi_{\hat{B}} \to \mathbb{Q}/\mathbb{Z}$, which is perfect when B is semi-stable; see [4, §11]. Applied to our situation, this pairing induces a canonical isomorphism between $\mathrm{coker}(\pi_\Phi)$ and the Pontrjagin dual of $\ker(\hat{\pi}_\Phi)$. We showed that this latter group is trivial, so π_Φ is indeed surjective.

Consider the functorial commutative diagram arising from the immersion $E \to J$:

$$\begin{array}{ccc} E(F)_{\mathrm{tor}} & \longrightarrow & \Phi_{E,\mathfrak{p}} \\ \big\downarrow & & \big\downarrow \\ J(F)_{\mathrm{tor}} & \xrightarrow{\sim} & \Phi_{J,\mathfrak{p}}. \end{array}$$

The left vertical arrow is obviously injective, and we know that the lower horizontal arrow is an isomorphism. Hence the homomorphism $E(F)_{\mathrm{tor}} \to \Phi_{E,\mathfrak{p}}$ is injective. There is a similar commutative diagram arising from the quotient map $J \to E$:

$$\begin{array}{ccc} J(F)_{\mathrm{tor}} & \xrightarrow{\sim} & \Phi_{J,\mathfrak{p}} \\ \big\downarrow & & \big\downarrow \\ E(F)_{\mathrm{tor}} & \longrightarrow & \Phi_{E,\mathfrak{p}}. \end{array}$$

We showed that the left vertical arrow is surjective. Hence $E(F)_{\mathrm{tor}} \to \Phi_{E,\mathfrak{p}}$ must be surjective, and since it is also an injection, we get the isomorphism $E(F)_{\mathrm{tor}} \cong \Phi_{E,\mathfrak{p}}$ of part (1). Now the same diagram also implies that $J(F)_{\mathrm{tor}} \to E(E)_{\mathrm{tor}}$ is surjective. This proves (2).

We turn to the proof of (3). Suppose $E(F)$ has an element of order n. We know that n is coprime to p, and also $E(F)[n] \cong \Phi_{E,\mathfrak{p}}[n] \cong \mathbb{Z}/n\mathbb{Z}$. The argument at the beginning of the proof can be used to show that $E[n]$ is everywhere unramified, so $E[n] \subset E(\widetilde{F})$. Thus $E/\widetilde{F}$ is a non-isotrivial elliptic curve over $\mathbb{P}^1_{\overline{\mathbb{F}}_q}$ with constant n-torsion. This implies that there is a non-constant morphism $\mathbb{P}^1_{\overline{\mathbb{F}}_q} \to X(n)_{\overline{\mathbb{F}}_q}$, where $X(n)$ is the moduli scheme of elliptic curves with full n-torsion. Since n is coprime to p, $X(n)_{\overline{\mathbb{F}}_q}$ is an irreducible smooth projective curve over $\overline{\mathbb{F}}_q$. We conclude that the genus of $X(n)_{\overline{\mathbb{F}}_q}$ must be 0. On the other hand, the genus of $X(n)_{\overline{\mathbb{F}}_q}$ is equal to the genus of $X(n)_{\mathbb{C}}$. Using the formula for the genus of $X(n)_{\mathbb{C}}$, we see that $n \leq 5$.

The proof of (4) is implicit in the previous paragraph. Indeed, suppose $\Phi_{E,\mathfrak{p}} = \mathbb{Z}/n\mathbb{Z}$. Then $E[n]$ is everywhere unramified, so $\mathcal{E}_{\mathbb{F}_\infty}[n]$ must be of rank two over $\mathbb{Z}/n\mathbb{Z}$. Since $\mathcal{E}^0_{\mathbb{F}_\infty}[n]$ has order n, this forces $\Phi_{E,\infty}[n] = \mathbb{Z}/n\mathbb{Z}$. □

References

[1] M. Emerton, *Optimal quotients of modular Jacobians*, Math. Ann. **327** (2003), 429–458.
[2] E.-U. Gekeler, *Über Drinfeldsche Modulkurven vom Hecke-Typ*, Compositio Math. **57** (1986), 219–236.

[3] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. **476** (1996), 27–93.
[4] A. Grothendieck, *Modèles de Néron et monodromie*, SGA 7, Exposé IX, 1972.
[5] B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.
[6] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math. **400** (1989), 173–184.
[7] A. Pál, *On the torsion of the Mordell-Weil group of the Jacobians of Drinfled modular curves*, Documenta Mathematica, to appear.
[8] M. Papikian, *Abelian subvariaties of Drinfeld Jacobians and congruences modulo the characteristic*, preprint.
[9] M. Papikian, *On the variation of Tate-Shafarevich groups of elliptic curves over hyperelliptic curves*, J. Number Theory, to appear.
[10] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.

Department of Mathematics, Stanford University, Stanford, CA 94305
E-mail address: papikian@math.stanford.edu