Math. Res. Lett. **13** (2006), *no.* 2, 321–331

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. We also show that $E(F)_{\mathrm{tor}} \cong \mathbb{Z}/n\mathbb{Z}$ for some n, $1 \leq n \leq 3$, and that n divides $(q-1)$ and $\deg(\mathfrak{p})$.

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, [6]. 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 [4] 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 [4] that this is an isomorphism. More

Received by the editors April 4, 2005.

Key words and phrases. Elliptic curves, Drinfeld modular curves, cuspidal divisor group.

The author's research was supported by Institut Post-Doctoral Européen.

recently, Pál proved [10] 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 [8].

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 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 notation 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 $\mathcal{E}$. We denote by $n(\mathfrak{p})$ the greatest common divisor of $N(\mathfrak{p})$ and $(q-1)$. The main result is the following:

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

1. *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.*
2. *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 $\Phi_{E,\mathfrak{p}}$.*
3. *$E(F)_{\mathrm{tor}} \cong \mathbb{Z}/n\mathbb{Z}$ for some $1 \leq n \leq 3$ dividing $n(\mathfrak{p})$.*

Remark 1.2. According to part (1) of the theorem, $E(F)_{\mathrm{tor}}$ has a natural generator, namely the image of the cuspidal divisor. In part (3), the condition that n divides $n(\mathfrak{p})$, can be equivalently stated as follows: If $n = 3$, then 3 divides $(q-1)$ and d; if $n = 2$ then q is odd and d is divisible by 4. This easily follows from the formula for $N(\mathfrak{p})$.

This theorem is the function field analogue of a result over $\mathbb{Q}$ due to Mestre and Oesterlé [9]. Emerton [3] generalized Mestre-Oesterlé theorem from elliptic curves to arbitrary abelian subvarieties of the classical modular Jacobians. Both [9] and [3] extensively use in their proofs the results of Mazur [8] and Ribet [13]. One feature which is significantly different in our proof is that we completely avoid using any "level-lowering" results. From the Eisenstein ideal theory we need the Gorensteinness property of the completion of the Hecke algebra at the Eisenstein maximal ideals and the fact that $\mathcal{C} = J(F)_{\mathrm{tor}}$, both proven by Pál in [10].

Lemma 1.3. *If we allow both q and $\mathfrak{p}$ to vary then Theorem 1.1 (3) is the best possible result, in the sense that there are optimal elliptic curves with $E(F)_{\mathrm{tor}} \cong \mathbb{Z}/2\mathbb{Z}$ and there are also optimal elliptic curves with $E(F)_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$.*

Proof. There is an example due to Gekeler, which shows that $E(F)_{\mathrm{tor}} \cong \mathbb{Z}/3\mathbb{Z}$ occurs. 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 $\#E(F) = \#\Phi_{E,\mathfrak{p}} = 3$.

Andreas Schweizer in his Ph.D. thesis considered the curve

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

over $\mathbb{F}_3(t)$. This curve has conductor $(t^4 - t^2 - 1) \cdot \infty$, split multiplicative reduction at ∞, and $E(F) \cong \mathbb{Z}/2\mathbb{Z}$. It is not optimal according to Theorem 1.1, since $\Phi_{E,\mathfrak{p}}$ is trivial. Let E' be the curve obtained from E by the isogeny having kernel $E(F)$. By Theorem 4.1 and its proof, E' must be optimal and $\Phi_{E',\mathfrak{p}} \cong \mathbb{Z}/2\mathbb{Z}$. Again using Theorem 1.1, we get $E'(F) \cong \mathbb{Z}/2\mathbb{Z}$. □

Note that the proof of this lemma also shows that the requirement on E being optimal in Theorem 1.1 is necessary. Another 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.

Remark 1.4. One could ask whether Theorem 1.1 (3) is the best possible result when we *fix* q and vary only $\mathfrak{p}$. For example, for any q not congruent to 1 modulo 3 the only possibility for $E(F)_{\text{tor}}$ is $\mathbb{Z}/2\mathbb{Z}$. This is similar to the situation over $\mathbb{Q}$, where one knows that aside from finitely many (explicitly known) examples of optimal curves with prime conductor the only possibility for the rational torsion of such curves is $\mathbb{Z}/2\mathbb{Z}$. Moreover, a curve with non-trivial 2-torsion must be a Setzer-Neumann curve; see [9, §5]. It seems like an interesting problem to try to give such a complete classification over function fields too. (The only q for which our theorem gives such a complete answer is $q = 2$: the optimal curves over $\mathbb{F}_2(t)$ cannot have any rational torsion at all.)

In [11] 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. One of the factors which appears in that formula is the fraction $\#E(F)_{\text{tor}}/\#\Phi_{E,\mathfrak{p}}$. 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. Following the suggestion of the referee, we include the statement of this result.

Let $S := \{x_1, x_2, \ldots, x_n\}$ be the set of isomorphism classes of super-singular Drinfeld modules over $\overline{\mathbb{F}}_{\mathfrak{p}}$. Let $\mathcal{M}$ denote the free $\mathbb{Z}$-module on the set S, and $\deg : \mathcal{M} \to \mathbb{Z}$ denote the $\mathbb{Z}$-linear map obtained by sending each $x_i \in S$ to $1 \in \mathbb{Z}$, and let $\mathcal{M}^0$ denote the kernel of deg. Define a symmetric, bilinear, $\mathbb{Z}$-valued pairing on $\mathcal{M}$ by the formula $\langle x_i, x_j \rangle = \#\text{Isom}(x_i, x_j)/(q-1)$. It is known that the character group $\text{Hom}_{\overline{\mathbb{F}}_{\mathfrak{p}}}(\mathcal{J}^0_{\overline{\mathbb{F}}_{\mathfrak{p}}}, \mathbb{G}_{m,\overline{\mathbb{F}}_{\mathfrak{p}}})$ is canonically isomorphic to $\mathcal{M}^0$, and the pairing $\langle \cdot, \cdot \rangle$ restricted to $\mathcal{M}^0$ is Grothendieck's monodromy pairing discussed in [7]. From the optimal quotient map $J \to E$ one obtains a canonical element $H_E \in \mathcal{M}^0$ corresponding to E. Now let $\mathfrak{d}$ be an irreducible polynomial in A of odd degree. Let $K = F(\sqrt{\mathfrak{d}})$. Let $\mathcal{O}$ be the integral closure of A in K. If we assume that the ideal $(\mathfrak{p})$ remains prime in $\mathcal{O}$ then the endomorphism rings of

some super-singular Drinfeld modules x_i contain $\mathcal{O}$ as a subring. There results an action of $\mathrm{Pic}(\mathcal{O})$ on a subset of S, which produces an element $H_K \in \mathcal{M}$ depending only on K. Theorem 1.1 combined with [11, Thm. 1.2] give the following formula:

Theorem 1.5. *If* $\langle H_E, H_K\rangle \neq 0$ *then*

$$\#Ш(E/K) = \left(\langle H_E, H_K\rangle \cdot q^{(\deg \Omega^1_{\mathcal{E}}|_O - 1)}\right)^2,$$

where $\Omega^1_{\mathcal{E}}|_O$ *is the pullback of* $\Omega^1_{\mathcal{E}}$ *along the relative zero section.*

2. The kernel of the Eisenstein ideal

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 [10], 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 $J[\mathfrak{E}]$, respectively $J[\mathfrak{E}, \ell]$, for the group of points in $J(\overline{F})$, respectively in $J(\overline{F})[\ell]$, which are killed by all elements of $\mathfrak{E}$. Denote $\widetilde{F} := \overline{\mathbb{F}}_q(t)$. This is the maximal unramified extension of F.

Before giving the proof of Theorem 1.1, we need few preliminary facts. The purpose of this section is to describe the kernel of the Eisenstein ideal $J[\mathfrak{E}]$ as a Galois submodule of J. This result seems to be of independent interest. Some of our arguments are motivated by [8] and [14].

Lemma 2.1. *Let* V *be a* $\mathrm{Gal}(F^{\mathrm{sep}}/F)$*-submodule of* $J(\overline{F})$ *of finite cardinality coprime to* p*. If* V *is unramified at* $\mathfrak{p}$*, then it is everywhere unramified, i.e.,* $V \subset J(\widetilde{F})$*.*

Proof. Since J has good reduction away from $\mathfrak{p}$ and ∞, using the Néron-Ogg-Shafarevich criterion, it is enough to show that V is unramified at ∞. It is even enough to show that V is at most tamely ramified at ∞. Indeed, V is a $\mathrm{Gal}(F^{\mathrm{sep}}/F)$-module by assumption, and it is easy to see (for example, by using Hurwitz genus formula) that F has no extensions ramified exactly at ∞ such that the ramification is tame. We can assume $\#V = \ell^n$ for some prime $\ell \neq p$. Choose an inertia group $I_\infty \subset \mathrm{Gal}(F^{\mathrm{sep}}/F)$ at ∞. The reduction of J at ∞ is toric, in particular semi-abelian, so I_∞ acts on $J[\ell^n]$ through its maximal pro-ℓ quotient, which is procyclic; see [7, Prop. 3.5]. In particular, I_∞ acts on V through its pro-ℓ quotient, so V is at most tamely ramified at ∞. □

Proposition 2.2. *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. [7, §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 [7, §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 [10], so the sequence splits as we have produced a $\mathbb{T}$-equivariant retraction $G \to \mathcal{S}$, cf. [8, 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. □

Lemma 2.1 and Proposition 2.2, combined with the results in [10], are actually sufficient for the proof of Theorem 1.1, but for the sake of completeness we show that the inclusion in Proposition 2.2 is in fact an equality.

The maximal ideals of $\mathbb{T}$ which contain the Eisenstein ideal $\mathfrak{E}$ will be called *Eisenstein maximal ideals*. By Proposition 7.11 and the proof of Corollary 11.8 in [10] we have $\mathbb{T}/\mathfrak{E} = \mathbb{Z}/N(\mathfrak{p})\mathbb{Z}$. Hence for a maximal Eisenstein ideal $\mathfrak{M}$ the quotient field $\mathbb{T}/\mathfrak{M}$ has characteristic dividing $N(\mathfrak{p})$, in particular it is coprime to p. For a maximal ideal $\mathfrak{M} \lhd \mathbb{T}$ denote by $\mathbb{T}_{\mathfrak{M}}$ the completion of $\mathbb{T}$ at $\mathfrak{M}$.

The character group $\mathcal{X} = \mathrm{Hom}_{\overline{\mathbb{F}}_{\mathfrak{p}}}(\mathcal{J}^0_{\overline{\mathbb{F}}_{\mathfrak{p}}}, \mathbb{G}_{m,\overline{\mathbb{F}}_{\mathfrak{p}}})$ is a free $\mathbb{Z}$-module of rank $\dim(J)$ which is equipped with compatible actions of $\mathbb{T}$ and $\mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$. Moreover, $\mathbb{T}$ acts faithfully on $\mathcal{X}$.

Lemma 2.3. *If the maximal ideal $\mathfrak{M} \lhd \mathbb{T}$ is Eisenstein then $\mathcal{X}_{\mathfrak{M}} = \mathcal{X} \otimes_{\mathbb{T}} \mathbb{T}_{\mathfrak{M}}$ is free of rank one over $\mathbb{T}_{\mathfrak{M}}$.*

Proof. Let $k = \mathbb{T}/\mathfrak{M}$, and let ℓ be the characteristic of k. An argument similar to the one in [14, Thm. 2.3] shows that there is an inclusion

$$\mathrm{Hom}(\mathcal{X}/\mathfrak{M}\mathcal{X}, \mu_\ell) \hookrightarrow J[\mathfrak{M}].$$

On the other hand, from [10, §§10-11] we know that $\dim_{\mathbb{F}_\ell} J[\mathfrak{M}] = 2$ and the image of $J[\mathfrak{M}]$ in $\Phi_{J,\mathfrak{p}}$ is non-trivial. Since $\mathrm{Hom}(\mathcal{X}/\mathfrak{M}\mathcal{X}, \mu_\ell) \subset \mathcal{J}^0_{\mathbb{F}_{\mathfrak{p}}}[\mathfrak{M}]$, we conclude that $\dim_k(\mathcal{X}/\mathfrak{M}\mathcal{X}) \leq 1$. By Nakayama's lemma $\mathcal{X}_{\mathfrak{M}}$ is a cyclic $\mathbb{T}_{\mathfrak{M}}$-module.

Using [16, Prop. 4.2], it is easy to see that $\mathbb{T}_{\mathfrak{M}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is a commutative semi-simple algebra of the same dimension as $\mathcal{X}_{\mathfrak{M}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Since $\mathbb{T}$ acts faithfully on $\mathcal{X}$, we get that $\mathcal{X}_{\mathfrak{M}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ is free of rank one over $\mathbb{T}_{\mathfrak{M}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. Combined with the previous paragraph, this implies that $\mathcal{X}_{\mathfrak{M}}$ is indeed a free rank one $\mathbb{T}_{\mathfrak{M}}$-module. □

Proposition 2.4. *There is an inclusion $J[\mathfrak{E}] \subset J(\widetilde{F})$.*

Proof. Let $n = N(\mathfrak{p})$. As we already mentioned, $\mathbb{T}/\mathfrak{E} = \mathbb{Z}/n\mathbb{Z}$, so every element of $J[\mathfrak{E}]$ is killed by n. From [10, §§10-11] we also have $\dim_{\mathbb{F}_\ell} J[\mathfrak{E}, \ell] = 2$, for any prime ℓ dividing n. Therefore, $\#J[\mathfrak{E}] \leq n^2$.

Fix a decomposition group $D_{\mathfrak{p}} \subset \mathrm{Gal}(\mathbb{F}^{\mathrm{sep}}/F)$ at $\mathfrak{p}$. Using the quotient map $D_{\mathfrak{p}} \to \mathrm{Gal}(\overline{\mathbb{F}}_{\mathfrak{p}}/\mathbb{F}_{\mathfrak{p}})$, we view $\mathcal{X}$ as a $\mathbb{T}[D_{\mathfrak{p}}]$-module. For any natural number m coprime to p, the finite multiplicative group $\mathcal{J}^0_{\mathbb{F}_{\mathfrak{p}}}[m]$ canonically lifts to a $\mathbb{T}[D_{\mathfrak{p}}]$-submodule of $J[m](\overline{F}_{\mathfrak{p}})$, cf. [7, §2]. Now $\mathcal{J}^0_{\mathbb{F}_{\mathfrak{p}}}[m]$ is the Cartier dual of $\mathcal{X}/m\mathcal{X}$.

We thus obtain a $\mathbb{T}[D_{\mathfrak{p}}]$-equivariant injection

$$\mathrm{Hom}(\mathcal{X}/m\mathcal{X}, \mu_m) \hookrightarrow J[m](\overline{F}_{\mathfrak{p}}).$$

Taking $m = n$ and applying $\mathrm{Hom}_{\mathbb{T}}(\mathbb{T}/\mathfrak{E}, -)$, we get a canonical injection

$$\mathrm{Hom}(\mathcal{X}/\mathfrak{E}\mathcal{X}, \mu_n) \hookrightarrow J[\mathfrak{E}].$$

By combining this injection with the inclusion of $\mathcal{C}$ in $J[\mathfrak{E}]$, we obtain a map of $D_{\mathfrak{p}}$-modules

$$\mathcal{C} \oplus \mathrm{Hom}(\mathcal{X}/\mathfrak{E}\mathcal{X}, \mu_n) \to J[\mathfrak{E}]. \tag{2.1}$$

The sum is direct and the map is injective since $\mathcal{C}$ maps isomorphically onto $\Phi_{J,\mathfrak{p}}$, whereas $\mathrm{Hom}(\mathcal{X}/\mathfrak{E}\mathcal{X}, \mu_n)$ lies in $\mathcal{J}^0_{\mathbb{F}_{\mathfrak{p}}}$ by construction. By Lemma 2.3, $\mathcal{X}/\mathfrak{E}\mathcal{X} = \mathbb{T}/\mathfrak{E} = \mathbb{Z}/n\mathbb{Z}$, and since $\mathcal{C} = \mathbb{Z}/n\mathbb{Z}$, we get $\#J[\mathfrak{E}] \geq n^2$. On the other hand, we already showed $\#J[\mathfrak{E}] \leq n^2$, so (2.1) is an isomorphism of $D_{\mathfrak{p}}$-modules. The left hand-side of (2.1) is clearly unramified. Thus, $J[\mathfrak{E}]$ is unramified at $\mathfrak{p}$, and the inclusion $J[\mathfrak{E}] \subset J(\widetilde{F})$ follows from Lemma 2.1. □

Theorem 2.5. *There is an equality $J[\mathfrak{E}] = J(\widetilde{F})_{\mathrm{tor}}$. Moreover, $J[\mathfrak{E}] \subset J[n]$ and there is a short exact sequence of group schemes*

$$0 \to \mu_n \to J[\mathfrak{E}] \to \mathbb{Z}/n\mathbb{Z} \to 0,$$

where $n = N(\mathfrak{p})$.

Proof. The first sentence is an immediate consequence of Proposition 2.2 and Proposition 2.4. To see the second part, recall that in the proof of Proposition 2.2 we showed that $J(\widetilde{F})_{\mathrm{tor}}$ is an extension of a constant group scheme $\mathcal{L}$ by the maximal μ-type étale subgroup $\mathcal{S}$ of J. According to [10], $\mathcal{S} = \mu_n$. On the other hand, in the proof of Proposition 2.4 we showed that $J[\mathfrak{E}]$ as an abelian group is $(\mathbb{Z}/n\mathbb{Z})^2$. Thus, $\mathcal{L} = \mathbb{Z}/n\mathbb{Z}$ and the second claim follows. □

We conclude this section by giving a representation-theoretic description of the Eisenstein maximal ideals. Note that Theorem 2.7 is the function field analogue of Ribet's "level-lowering theorem" [13, Thm. 1.1] in the special case of prime level.

Proposition 2.6. *Let $\mathfrak{M} \lhd \mathbb{T}$ be a maximal ideal such that the characteristic of $\mathbb{T}/\mathfrak{M}$ is different from p. There is a unique semi-simple representation*

$$\rho_{\mathfrak{M}} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{GL}_2(\mathbb{T}/\mathfrak{M}),$$

which is unramified away from $\mathfrak{p}$ and ∞, and such that for all places $v \neq \mathfrak{p}, \infty$ the following relations hold:

$$\mathrm{Tr}(\rho_{\mathfrak{M}}(\mathrm{Frob}_v)) = T_v (\mathrm{mod}\ \mathfrak{M}), \quad \det(\rho_{\mathfrak{M}}(\mathrm{Frob}_v)) = q^{\deg(v)} (\mathrm{mod}\ \mathfrak{M}).$$

Proof. The proof of this proposition is very similar to the proof of the corresponding fact over $\mathbb{Q}$, as is given, for example, in [13, Prop. 5.1]. One only needs to replace [13, (10)] by [5, Thm. 3.17], and needs to replace [1, Thm. 6.1] by Drinfeld's Theorem 2 in [2]. □

In analogy with the terminology for residual representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, for a place v of A we say that $\rho_{\mathfrak{m}}$ is *finite* at v if there is finite flat $\mathbb{T}/\mathfrak{M}$-vector space scheme H over A_v for which the action of $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ on the $\mathbb{T}/\mathfrak{M}$-vector space $H(\overline{F})$ gives $\rho_{\mathfrak{m}}$.

Theorem 2.7. *The following three conditions are equivalent:*

(1) *The representation $\rho_{\mathfrak{m}}$ is reducible;*
(2) *The representation $\rho_{\mathfrak{m}}$ is finite at $\mathfrak{p}$;*
(3) *The maximal ideal $\mathfrak{M}$ is Eisenstein.*

Proof. That (1) and (3) are equivalent follows from the same argument as in [8, Prop. 14.1]. To show that (2) and (3) are equivalent, first observe that since $\ell \neq p$ the representation $\rho_{\mathfrak{m}}$ is finite at $\mathfrak{p}$ if and only if it is unramified at $\mathfrak{p}$. Now the claim easily follows from Lemma 2.1 and Theorem 2.5. □

3. Cuspidal torsion

Proof of parts (1) and (2) 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 Theorem 6.1 in [12] $\Phi_{E,\mathfrak{p}}[p] = 1$, so we can assume $\ell \neq p$. Suppose $\Phi_{E,\mathfrak{p}}[\ell]$ is non-trivial. Then by [7, §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 $\dim_{\mathbb{F}_\ell}(E[\ell]) = 2$. Since E is an abelian subvariety of J defined over F, $E[\ell]$ is a Galois submodule of $J(\overline{F})$, so $E[\ell]$ is in everywhere unramified by Lemma 2.1. Hence $E[\ell] \subset J(\widetilde{F})$. Using Theorem 2.5, we get $E[\ell] = J[\mathfrak{E}, \ell]$. There results a commutative functorial diagram

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

Since $\mathcal{C} \xrightarrow{\sim} \Phi_{J,\mathfrak{p}}$, the image of $J[\mathfrak{E}, \ell]$ in $\Phi_{J,\mathfrak{p}}[\ell]$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$. 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 [7, §1.2]: $\Phi_B \times \Phi_{\hat{B}} \to \mathbb{Q}/\mathbb{Z}$, which is perfect when B is semi-stable; see [7, §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 $E \to J$:

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

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 $J \to E$:

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

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 (2). Now the same diagram also implies that $J(F)_{\mathrm{tor}} \to E(E)_{\mathrm{tor}}$ is surjective. This proves (1). □

4. Rational isogenies

Theorem 4.1 (A. Schweizer)**.** *Let E be an elliptic curve over F with conductor $\mathfrak{p} \cdot \infty$. ($E$ is not necessarily optimal and the multiplicative reduction at ∞ is not necessarily split.) Then E has at most one prime-to-p isogeny over F, and this isogeny (if it exists) is either a 2-isogeny or a 3-isogeny.*

Proof. We can assume that E is not a Frobenius conjugate of another curve over F, so j_E is not a p-th power. Denote $m := \#\Phi_{E,\mathfrak{p}}$ and $n := \#\Phi_{E,\infty}$. By Ogg's formula $md + n = c_2$, where c_2 is the second Chern number of E. Let ℓ be a prime different from p, and let $\phi : E \to E'$ be a cyclic F-isogeny of degree ℓ. Such an isogeny changes n and m either by multiplying or dividing them by ℓ; this is easy to see by looking at the Tate curves corresponding to E. On the other hand, c_2 is invariant under prime-to-p isogenies; cf. [15]. By possibly looking at the dual of ϕ, thus interchanging the roles of E and E', we can assume $\#\Phi_{E',\infty} = n/\ell$ (note that $\phi^\vee$ is also defined over F and is cyclic of order ℓ). Write $n = \ell u$. Then $md + \ell u = \ell md + u$. This implies $u = md$, so $n = \ell md$. We get $c_2 = (\ell + 1)md$. On the other hand, from the Pesenti-Szpiro inequality we have $c_2 < 6d$. Thus $\ell \leq 4$.

Next, we claim that E can have at most one F-rational ℓ-isogeny. Of the $\ell+1$ cyclic ℓ-isogenies of E (over a suitable extension of the base field) exactly one multiplies the order of a component group by ℓ, and all the others divide that order by ℓ; this is again easy to see by looking at the local Tate model of E. Suppose E has two F-rational ℓ-isogenies. Then one of these isogenies divides n by ℓ and multiplies m by ℓ, and the other acts in the opposite way. Repeating

the argument in the first paragraph, we get $(\ell+1)\ell d \leq c_2 < 6d$. This is a contradiction.

Finally, E cannot have a F-rational cyclic ℓ^2-isogeny. Indeed, suppose E has such an isogeny. Let E'' be the image under this isogeny, and let E' be the image under the cyclic ℓ-isogeny. Then E' has two distinct F-rational ℓ-isogenies - one with image E and the other with image E''. This we already ruled out. Combing all the previous facts, the theorem follows. □

Proof of part (3) of Theorem 1.1. From Theorem 4.1 we know $E(F)_{\mathrm{tor}} \cong \mathbb{Z}/n\mathbb{Z}$ for some $n \leq 3$. It remains to show that n divides $n(\mathfrak{p})$. That n divides $N(\mathfrak{p})$ follows from the injection $E(F)_{\mathrm{tor}} \hookrightarrow J(F)_{\mathrm{tor}} \cong \mathcal{C}$. Denote $T := E(F)_{\mathrm{tor}}$. This is a constant group subscheme of E. Consider the Zariski closure $\mathcal{T}$ of T in $\mathcal{E}$. We know that the specialization of $\mathcal{T}$ at $\mathfrak{p}$ injects into $\Phi_{E,\mathfrak{p}}$. Thus, the isogeny $E \to E/T$ divides the order of the component group at $\mathfrak{p}$ by n; this is easy to see by looking at the morphism induced on the closed fibres of Néron models at $\mathfrak{p}$. Hence, by the invariance of c_2 as in the proof of Theorem 4.1, the specialization of $\mathcal{T}$ at ∞ must inject into $\mathcal{E}^0_{\mathbb{F}_\infty}(\mathbb{F}_\infty)$. This last group has order $q-1$, which implies that n divides $q-1$. □

Remark 4.2. A weaker result about the rational torsion of optimal curves can be obtained from the following argument. 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 of Theorem 1.1 (2) 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 $n \leq 5$.

Acknowledgements

I am very grateful to Andreas Schweizer for his useful remarks on an earlier version of this paper, especially for communicating to me the fact in Theorem 4.1. It allowed to improve my initial result on the rational torsion of optimal curves. I thank Universität des Saarlandes and IHÉS for their hospitality.

References

[1] P. Deligne and J.-P. Serre, *Formes modulaires de poinds 1*, Ann. Sci. École Norm. Sup. (4) **7** (1975) 507–530.
[2] V. Drinfeld, *Elliptic modules*, Mat. Sb. (N.S.) **94** (1974) 594–627.
[3] M. Emerton, *Optimal quotients of modular Jacobians*, Math. Ann. **327** (2003) 429–458.

[4] E.-U. Gekeler, *Über Drinfeldsche Modulkurven vom Hecke-Typ*, Compositio Math. **57** (1986) 219–236.
[5] ———, *Analytic construction of Weil curves over function fields*, J. Théor. Nombres Bordeaux **7** (1995), 27–49.
[6] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. **476** (1996) 27–93.
[7] A. Grothendieck, *Modèles de Néron et monodromie*, SGA 7, Exposé IX, 1972.
[8] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977) 33–186.
[9] 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.
[10] A. Pál, *On the torsion of the Mordell-Weil group of the Jacobians of Drinfled modular curves*, Doc. Math. **10** (2005) 131–198.
[11] M. Papikian, *On the variation of Tate-Shafarevich groups of elliptic curves over hyperelliptic curves*, J. Number Theory, to appear.
[12] ———, *Pesenti-Szpiro inequality for optimal elliptic curves*, J. Number Theory **114** (2005) 361–393.
[13] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990) 431–476.
[14] ———, *Torsion points on* $J_0(N)$ *and Galois representations*, Lecture Notes in Math. **1716** (1999), 145–166.
[15] T. Shioda, *Some remarks on elliptic curves over function fields*, Astérisque **209** (1992), 99–114.
[16] A. Tamagawa, *The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve*, Publ. RIMS, Kyoto Univ. **31** (1995), 204–246.

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