Journal of Number Theory 131 (2011) 285–299

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Strong Weil curves over $\mathbb{F}_q(T)$ with small conductor

Andreas Schweizer

Institute of Mathematics, Academia Sinica, 6F, Astronomy–Mathematics Building, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan

ARTICLE INFO

Article history:
Received 15 May 2010
Revised 24 August 2010
Accepted 30 August 2010
Available online 16 October 2010
Communicated by David Goss

MSC:
primary 11G05
secondary 11G09, 14J27

Keywords:
Elliptic curve
Drinfeld modular curve
Strong Weil uniformization
Frobenius isogeny
Bruhat–Tits tree
Rational elliptic surface

ABSTRACT

We continue work of Gekeler and others on elliptic curves over $\mathbb{F}_q(T)$ with conductor $\infty\cdot\mathfrak{n}$ where $\mathfrak{n}\in\mathbb{F}_q[T]$ has degree 3. Because of the Frobenius isogeny there are infinitely many curves in each isogeny class, and we discuss in particular which of these curves is the strong Weil curve with respect to the uniformization by the Drinfeld modular curve $X_0(\mathfrak{n})$. As a corollary we obtain that the strong Weil curve $E/\mathbb{F}_q(T)$ always gives a rational elliptic surface over $\overline{\mathbb{F}_q}$.

0. Introduction

The first paper that systematically used Drinfeld modular curves and the Bruhat–Tits tree in order to classify elliptic curves over a function field was [Ge1].

With an eye towards feasibility of practical calculations, what we are talking about here are elliptic curves over a rational function field $\mathbb{F}_q(T)$ and Drinfeld modular curves $X_0(\mathfrak{n})$ for $\mathfrak{n}\in\mathbb{F}_q[T]$. Every elliptic curve over $\mathbb{F}_q(T)$ that is modular, that is, covered by some $X_0(\mathfrak{n})$, must have split multiplicative reduction at the place ∞ (= pole divisor of T). Conversely, every elliptic curve over $\mathbb{F}_q(T)$ with conductor $\infty\cdot\mathfrak{n}$ and split multiplicative reduction at ∞ is an isogeny factor of the Jacobian of $X_0(\mathfrak{n})$.

E-mail address: schweizer@math.sinica.edu.tw.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.08.007

It is known that there are no such elliptic curves if $deg(\mathfrak{n}) \leqslant 2$. So elliptic curves with conductor $\infty \cdot \mathfrak{n}$ where $deg(\mathfrak{n}) = 3$ represent the case with the smallest possible conductor. When considered as elliptic surfaces over the algebraic closure of $\mathbb{F}_q$ they give so-called extremal elliptic surfaces, which means that they are supersingular (in the sense of surface theory) and their Mordell–Weil groups are finite even over $\overline{\mathbb{F}_q}(T)$ (compare [Shi]).

Now let $\mathcal{T}$ be the Bruhat–Tits tree of $GL_2(\mathbb{F}_q((\frac{1}{T})))$. Then the homology of the quotient graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ encodes the splitting of the Jacobian of $X_0(\mathfrak{n})$. So it plays the same role as the space of cusp forms of weight 2 for $\Gamma_0(N)$ in the theory of elliptic curves of conductor N over $\mathbb{Q}$.

In [Ge1] the structure of the quotient graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ is determined for $deg(\mathfrak{n}) = 3$. Then the splitting of the Jacobian is calculated for $q \leqslant 16$. For elliptic curves with certain conductors explicit equations are given uniformly in q. In [Lei] these calculations were extended and further uniform explicit equations of elliptic curves were given.

Other papers have used Drinfeld modular curves to explicitly determine all elliptic curves over $\mathbb{F}_q(T)$ with conductors $\infty \cdot \mathfrak{n}$ of high degree but only few places of bad reduction: [Ge4] for q a power of 2 and $\mathfrak{n} = T^n$; [Ge5] ditto for q a power of 3; and [Sch5] for q even and $\mathfrak{n} = T^n(T-1)$.

However, although one of the subjects of [Ge2] is the characterization of the strong Weil curve, up to now the only explicit calculations of strong Weil curves seem to be three examples in [Ge2], the case $q = 2$, $deg(\mathfrak{n}) = 4$ treated in Chapter 4 of [Sch1] (the results are also listed in [Sch2]), and unpublished computer calculations by Udo Nonnengardt from around 1995 for $q = 2$, $\mathfrak{n} = T^n$ with $n \leqslant 10$.

In contrast to the classical situation of modular elliptic curves over $\mathbb{Q}$, each $\mathbb{F}_q(T)$-isogeny class contains infinitely many non-isomorphic curves. More precisely, they are obtained from finitely many curves by repeated application of the Frobenius isogeny. Papikian [Pa1,Pa2] has shown that in certain situations the strong Weil curve is not the Frobenius of another curve over $\mathbb{F}_q(T)$, but from examples it is known that this is not a general phenomenon.

The Frobenius isogeny is more problematic than the other ones, for example in the following context. By the two-dimensional Lüroth theorem, the image of a rational elliptic surface under a separable isogeny is again a rational elliptic surface. But the Frobenius of a rational elliptic surface need not be a rational surface. For example, the Frobenius of a semistable rational elliptic surface is never a rational surface (although it is of course a unirational surface).

Now Frobenius minimal extremal elliptic surfaces were proved to be rational surfaces in [Ito] for characteristic $p \geqslant 5$ and in [Sch6] for characteristics 2 and 3. Moreover, extremal rational elliptic surfaces have been explicitly classified in [La1] and [La2]. This invites of course the question where the strong Weil curves of conductor $\infty \cdot \mathfrak{n}$ with $deg(\mathfrak{n}) = 3$ are standing in this respect.

This question will be answered quite explicitly in this paper. The main reason why this can be done for all q, not just for specific instances, is that for $deg(\mathfrak{n}) = 3$ the corresponding quotient graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ can be described uniformly in q and the necessary calculations and arguments can be carried out more or less generically.

1. Basic facts

For an elliptic curve E over any field K of characteristic p we write $E^{(p)}$ for the image of E under the Frobenius isogeny. Since $E^{(p)}$ is obtained by raising the coefficients in a Weierstraß equation of E to the p-th power, we have $j(E^{(p)}) = (j(E))^p$. Conversely, if $j(E) \in (K^*)^p$, then $E \cong \tilde{E}^{(p)}$ for some $\tilde{E}$ over K.

If $p \geqslant 5$, then $Y^2 = X^3 + a_4X + a_6$ is isomorphic over K to

$$Y^2 = X^3 + a_4^{p^2}X + a_4^{\frac{3(p^2-1)}{2}}a_6$$

and from the formula for the j-invariant we see that if $j(E)$ is a p-th power, then $a_4^{\frac{3(p^2-1)}{2}}a_6$ also is.

Analogous arguments work in characteristic 3, where E has a normal form $Y^2 = X^3 + a_2X^2 - \frac{a_2^3}{j(E)}$ with $a_2 \neq 0$ (see [Si, Appendix A]) and in characteristic 2, where $Y^2 + XY = X^3 + a_2X^2 + \frac{1}{j(E)}$ is isomorphic over K to $Y^2 + XY = X^3 + a_2^2X^2 + \frac{1}{j(E)}$ (also [Si, Appendix A]).

Somewhat similar arguments show that an elliptic curve with j-invariant 0 always is the Frobenius of some elliptic curve over the same field.

We are in particular interested in elliptic curves over the rational function field $\mathbb{F}_q(T)$ where $\mathbb{F}_q$ is the finite field with q elements and characteristic p. By the above, such a curve E over $\mathbb{F}_q(T)$ with $j(E) \notin \mathbb{F}_q$ is **Frobenius minimal**, i.e. not the Frobenius of another elliptic curve over $\mathbb{F}_q(T)$, if and only if $j(E)$ is not a p-th power in $\mathbb{F}_q(T)$.

Now let us fix the polynomial ring $\mathbb{F}_q[T]$ and hence the place ∞ (the pole divisor of T). Then it is known that the elliptic curves over $\mathbb{F}_q(T)$ that are modular, i.e. that are images of a Drinfeld modular curve $X_0(\mathfrak{n})$ under a nonconstant $\mathbb{F}_q(T)$-rational morphism, are exactly the ones that have split multiplicative reduction at ∞. See [GeRe] for a thorough treatment (over any congruence function field), and [Ge2] or [Ge3] for less technical accounts over $\mathbb{F}_q(T)$.

As in the classical situation of elliptic curves over $\mathbb{Q}$, in every $\mathbb{F}_q(T)$-isogeny class of modular elliptic curves of conductor $\infty \cdot \mathfrak{n}$ there exists a unique curve E that is "closest to $X_0(\mathfrak{n})$" in the sense that every morphism $X_0(\mathfrak{n}) \to E'$ where E' is in the given isogeny class factors over E [GeRe, Section 8.4]. Equivalently, E is a subvariety of the Jacobian of $X_0(\mathfrak{n})$, not just an isogeny factor. To see this, note that since the map $X_0(\mathfrak{n}) \to E$ does not factor over an elliptic curve, Picard functoriality induces an embedding of $E \cong Jac(E)$ into $Jac(X_0(\mathfrak{n}))$. For the converse we are using that $Jac(X_0(\mathfrak{n}))$ contains only one abelian subvariety isogenous to E. This elliptic curve E is called the **strong Weil curve** (or optimal elliptic curve in [Pa1]).

Note however that the notion of strong Weil curve and the degree of the strong Weil uniformization $\pi : X_0(\mathfrak{n}) \to E$ also depend on q. The base change of the strong Weil curve E over $\mathbb{F}_q(T)$ to $\mathbb{F}_{q^n}(T)$ is not necessarily the strong Weil curve in its $\mathbb{F}_{q^n}(T)$-isogeny class; and even if it is, the degree of the strong Weil uniformization might not be the same. This comes from the simple fact that every q has its own Drinfeld modular curves. No useful relation is known between the curves $X_0(\mathfrak{n})$ for the same $\mathfrak{n}$ but different q of the same characteristic.

Naively, one would perhaps guess that the strong Weil curve is always Frobenius minimal. This is true for example if $\mathfrak{n}$ is irreducible [Pa1, Theorem 1.2] but not in general [GeRe, Examples 9.7.2 and 9.7.3] or equivalently [Ge2, Examples 4.2 and 4.3].

In practice, strong Weil curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$ can be determined by diagonalizing Hecke operators on the homology $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$ of the (essentially finite) quotient graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$. Here $\mathcal{T}$ is the Bruhat–Tits tree of $GL_2(\mathbb{F}_q((\frac{1}{T})))$ and $\Gamma_0(\mathfrak{n})$ is a Hecke subgroup of $GL_2(\mathbb{F}_q[T])$. One obtains a bijection between their $\mathbb{F}_q(T)$-isogeny classes (and hence their strong Weil curves) and certain one-dimensional simultaneous eigenspaces in $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$.

We suppress discussing the somewhat involved general details [GeRe,Ge2,Ge3] and concentrate on the case of interest to us, that is, the case $deg(\mathfrak{n}) = 3$. Up to affine transformation $T \mapsto aT + b$ with $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$, there are 5 different cases, namely

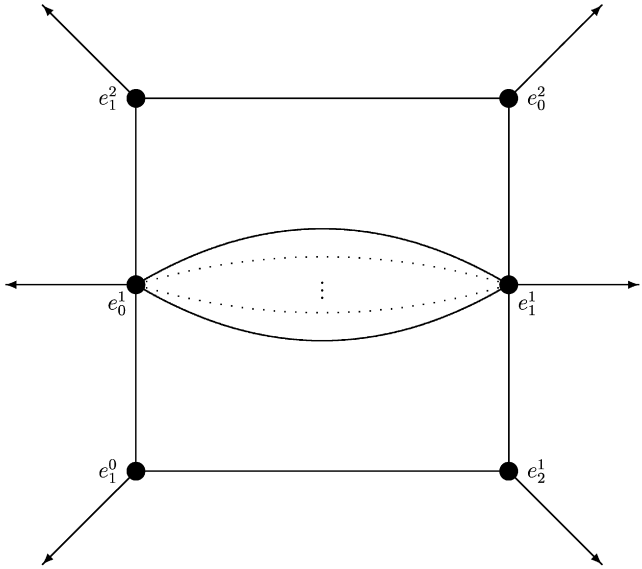
$\mathfrak{n} = T^3$ (in this case elliptic curves exist only in characteristics 2 and 3);
$\mathfrak{n} = T^2(T-1)$;

and the three semistable cases

$$\mathfrak{n} = T(T-1)(T-c),\ \mathfrak{n} = T\mathfrak{p}_2,\ \mathfrak{n} = \mathfrak{p}_3$$

where $1 \neq c \in \mathbb{F}_q^*$ and $\mathfrak{p}_i \in \mathbb{F}_q[T]$ is irreducible of degree i.

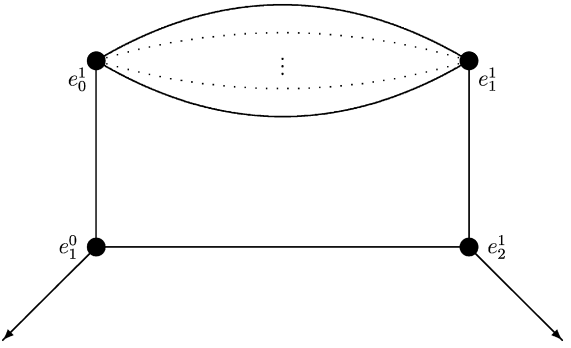
The corresponding quotient graphs have already been calculated in [Ge1]. For example, the graph $\Gamma_0(T^2(T-1)) \setminus \mathcal{T}$ looks as follows.



Here the dotted lines mean that there are $q-2$ different edges between the vertices e_0^1 and e_1^1. The (in English) somewhat unfortunate choice of the letter e for the labeling of the vertices originates from [Ge1] being written in German. The 6 arrows in the picture represent so-called cusps, that is half-lines consisting of infinitely many edges.

For general $\mathfrak{n} \in \mathbb{F}_q[T]$ of degree 3 the graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ looks somewhat similar and can be precisely described as follows: There are two vertices e_0^1 and e_1^1 of valency $q+1$. So the edges attached to e_0^1 can be parametrized by $\mathbb{P}^1(\mathbb{F}_q)$. Of these edges the ones that directly connect e_0^1 and e_1^1 are those corresponding to the $a \in \mathbb{F}_q$ with $(T-a) \nmid \mathfrak{n}$. If $\mathfrak{n}$ has a multiple zero, there is a cusp attached to each of e_0^1 and e_1^1, otherwise not. Finally, for each simple zero of $\mathfrak{n}$ in $\mathbb{F}_q$ and for ∞ there is a three edge path between e_0^1 and e_1^1 with two cusps attached to it (as in the above picture the upper and the lower part of the graph, belonging to 0 respectively ∞).

So for example, if $\mathfrak{n} \in \mathbb{F}_q[T]$ is irreducible of degree 3, the quotient graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ is



where the dotted lines now represent q different edges in total between e_0^1 and e_1^1.

Although we don't need it in the sequel we mention that in our description of the graphs the full Atkin–Lehner involution is the reflection at the vertical axis whereas in [Ge1] they are printed in a way that shows how they project onto the quotient graph $GL_2(\mathbb{F}_q[T]) \setminus \mathcal{T}$. Note however that Figs. 3 and 5 in [Ge1] have unfortunately been interchanged.

In particular, for $deg(\mathfrak{n}) = 3$ the structure of the graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ depends only on the splitting type of $\mathfrak{n}$ and can be uniformly described in q, whereas matters are (much) more complicated for $deg(\mathfrak{n}) \geqslant 4$ [GeNo].

The homology $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$ of the graph $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ is the $\mathbb{Z}$-module of all $\mathbb{Z}$-valued functions ψ on the oriented edges of $\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}$ that satisfy the following three conditions:

(i) $\psi(\bar{e}) = -\psi(e)$ where $\bar{e}$ is the edge e with reversed orientation.
(ii) (harmonicity) $\sum_{t(e)=v} \psi(e) = 0$ for every vertex v. Here $t(e)$ denotes the terminal vertex of the edge e.
(iii) ψ has finite support. Because of the harmonicity this means that ψ vanishes on the cusps.

The above description shows that every $\psi \in H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$ is completely determined by the values it takes on the edges terminating in the vertex e_0^1. Writing $\psi(a)$ for the value of ψ on the edge corresponding to $a \in \mathbb{P}^1(\mathbb{F}_q)$ establishes a $\mathbb{Z}$-module isomorphism between $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$ and the $\mathbb{Z}$-valued functions ψ on $\mathbb{P}^1(\mathbb{F}_q)$ whose values sum up to 0 (harmonicity at e_0^1), subject to the additional condition $\psi(0) = 0$ in case $\mathfrak{n}$ has a multiple zero, which we place at 0.

In particular, the dimension of $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$, which is also the genus of $X_0(\mathfrak{n})$, is q if $\mathfrak{n}$ is square-free, and $q-1$ if not.

Theorem 1.1. *(See [Ge1,Ge2].) Let E be a strong Weil curve over $\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$ where $deg(\mathfrak{n}) = 3$. Let φ be the primitive cycle in $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$ belonging to E. Scaling to $\varphi(\infty) = -1$ we have*

$$\varphi(a) = \begin{cases} -\lambda_a & \text{if } E \text{ has good reduction at } T-a, \\ -1 & \text{if } E \text{ has split multiplicative reduction at } T-a, \\ 1 & \text{if } E \text{ has non-split multiplicative reduction at } T-a, \\ 0 & \text{if } E \text{ has additive reduction at } T-a. \end{cases}$$

(Recall that $\lambda_a = q + 1 - \#E(\mathbb{F}_q[T]/(T-a))$ for $(T-a) \nmid \mathfrak{n}$.) Moreover,

$$-v_\infty\big(j(E)\big) = \min\big\{\langle\varphi, \psi\rangle > 0\colon\ \psi \in H_1\big(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z}\big)\big\}$$

where the scalar product is given by

$$\langle\varphi, \psi\rangle = \sum_{a \in \mathbb{P}^1(\mathbb{F}_q)} w_a \varphi(a) \psi(a)$$

with $w_a = q+1$ if E has multiplicative reduction at $a \in \mathbb{P}^1(\mathbb{F}_q)$, and $w_a = 1$ otherwise. The degree of the strong Weil uniformization $\pi : X_0(\mathfrak{n}) \to E$ is

$$deg(\pi) = \frac{\langle\varphi, \varphi\rangle}{-v_\infty(j(E))}.$$

Proof. The calculation of φ is done in [Ge1, Satz 9.1 and p. 141]. In particular, $\varphi(a)$ is the negative of the eigenvalue of φ under the Hecke operator H_{T-a}. In order to maintain compatibility with the examples in [Ge1] and [Lei] we have refrained from scaling the minus sign away. Also note that the harmonicity of φ at the vertex e_0^1 corresponds to the fact that the linear coefficient of the L-polynomial of E is 0.

For the scalar product see [Ge1, Bemerkung 6.9]. The factor $w_a = q+1$ comes from the fact that the middle edge of each three edge path between e_0^1 and e_1^1 carries weight $q-1$. Compare [GeRe, 3.2.5] and [GeRe, 4.8].

The formulas for $-v_\infty(j(E))$ [Ge2, Corollary 3.19] and $deg(\pi)$ [Ge2, Corollary 3.20] hold for all $\mathfrak{n} \in \mathbb{F}_q[T]$, but in general the scalar product is more complicated and there is no explicit formula for φ. □

Theorem 1.1 shows that for $deg(\mathfrak{n}) = 3$ the eigenform φ corresponding to a strong Weil curve E, and hence also $-v_\infty(j(E))$ and the degree of the strong Weil uniformization, are completely determined by the number of points of the reduction at the linear places. We make this explicit.

Corollary 1.2. *Let E be a strong Weil curve over $\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$ where $deg(\mathfrak{n}) = 3$. For every $a \in \mathbb{F}_q$ such that $(T-a) \nmid \mathfrak{n}$ let $\#_a$ be the number of $\mathbb{F}_q$-rational points of the reduction modulo $T-a$ of E (or of any other elliptic curve in the same isogeny class). Let N be the greatest common divisor of all these $\#_a$.*

(a) *If E has no linear places of non-split multiplicative reduction, then the pole order of $j(E)$ at the place ∞ is N.*
(b) *If E has at least one linear place of non-split multiplicative reduction, then $-v_\infty(j(E)) = \gcd(N, 2q+2)$.*

Proof. We write $\delta_a - \delta_\infty$ for the cycle taking the value 1 on the edge corresponding to a, the value -1 on the edge corresponding to ∞, and the value 0 on the other edges terminating in e_0^1. Obviously

$$\{\delta_a - \delta_\infty \colon a \in \mathbb{F}_q \text{ and } (T-a)^2 \nmid \mathfrak{n}\}$$

is a $\mathbb{Z}$-basis of $H_1(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T}, \mathbb{Z})$ and thus

$$-v_\infty\big(j(E)\big) = \gcd\big\{\langle \varphi, \delta_a - \delta_\infty\rangle \colon a \in \mathbb{F}_q \text{ and } (T-a)^2 \nmid \mathfrak{n}\big\}.$$

By Theorem 1.1 we have

$$\langle \varphi, \delta_a - \delta_\infty\rangle = \begin{cases} \#_a & \text{if } E \text{ has good reduction at } T-a, \\ 0 & \text{if } E \text{ has split multiplicative reduction at } T-a, \\ 2q+2 & \text{if } E \text{ has non-split multiplicative reduction at } T-a. \end{cases}$$ □

In particular, if there exists a linear place of good, supersingular reduction, then the strong Weil curve is Frobenius minimal. The same holds if q is odd and E has a linear place of non-split multiplicative reduction.

For convenient use later on we prove the following, presumably well-known facts.

Lemma 1.3.

(a) *An elliptic curve E over a perfect field k of characteristic 2 has a k-rational 2-torsion point if and only if it has a model $Y^2 + XY = X^3 + a_2X^2 + a_6$ with $a_6 \neq 0$. Moreover, this model has a k-rational 4-torsion point if and only if $a_2 = b^2 + b$ for some $b \in k$, that is, if it can be transformed over k into $Y^2 + XY = X^3 + \frac{1}{j(E)}$.*
(b) *An elliptic curve E over a perfect field k of characteristic 3 has a k-rational 3-torsion point if and only if it has a model $Y^2 = X^3 + X^2 + a_6$ with $a_6 \neq 0$. Furthermore, this model has a k-rational 9-torsion point if and only if $a_6 = u^3 - u$ with $u \in k \setminus \mathbb{F}_3$.*
(c) *An elliptic curve E over a perfect field k of characteristic 5 has a k-rational 5-torsion point if and only if it has a model $Y^2 = X^3 + 3X + a_6$ with $a_6 \neq \pm 1$.*

Proof. (a) If E has a 2-torsion point, it is not supersingular. So $j(E) \neq 0$, and there exists a change of coordinates over k that brings E into the desired form (cf. [Si, Appendix A]). With the duplication formula [Si, p. 59] one easily checks that $(0, \sqrt{a_6})$ is a 2-torsion point of the above equation, and that the 4-torsion points are $(\sqrt[4]{a_6}, \sqrt{a_6} + b\sqrt[4]{a_6})$ and $(\sqrt[4]{a_6}, \sqrt{a_6} + (b+1)\sqrt[4]{a_6})$ with $b^2 + b = a_2$.

(b) As before, if E has a 3-torsion point, it is not supersingular, i.e. $j(E) \neq 0$, and by [Si, Appendix A] there exists a model $Y^2 = X^3 + a_2X^2 + a_6$. With the duplication formula [Si, p. 59] one easily verifies that the 3-torsion points of this equation are $(-\sqrt[3]{a_6}, \pm\sqrt{a_2}\sqrt[3]{a_6})$. But if a_2 is a square in k, we can scale X and Y over k to get the desired form (with new a_6).

After some tedious calculation using the addition formulas [Si, p. 59] one obtains that in characteristic 3 the triplication formula for the X-coordinate of a point $P = (x, y)$ on the curve $Y^2 = X^3 + X^2 + a_6$ is

$$x[3]P = \frac{x^9 - a_6x^3 + a_6^3}{(x^3 + a_6)^2}.$$

So if δ is the X-coordinate of the 3-torsion point (and hence $a_6 = -\delta^3$), then η is the third power of the X-coordinate of a 9-torsion point if and only if

$$\eta^3 + \delta^3\eta - \delta^9 = \delta\big(\eta - \delta^3\big)^2.$$

Elementary transformations show that this equation is equivalent to $\delta = \lambda - \lambda^3$ with

$$\lambda = \frac{\delta^2}{\eta + \delta^2 - \delta^3} \quad \text{and} \quad \eta = \frac{\delta^2}{\lambda} + \delta^3 - \delta^2.$$

This proves that the X-coordinate of the 9-torsion point is k-rational if and only if $a_6 = u^3 - u$ (with $u = \lambda^3$). Then the Y-coordinate is automatically k-rational. Otherwise there would be an element in $Gal(\bar{k}/k)$ that maps the 9-torsion point to its inverse. But then it would also map the (k-rational!) 3-torsion point to its inverse, contradiction.

(c) The condition $a_6 \neq \pm 1$ is equivalent to $\Delta \neq 0$. The Hasse invariant of a Weierstraß equation $Y^2 = X^3 + AX + B$ in characteristic 5 is $H = 2A$. If H is a 4-th power in k^*, then by [Vo, pp. 248/249] the 5-torsion points are k-rational. Conversely, we have to show that if (x_0, y_0) is a k-rational 5-torsion point, then $\sqrt[4]{H} \in k$; then we can carry out the desired transformation.

Now $Q = (x_0\sqrt{H}, y_0\sqrt{H}\sqrt[4]{H})$ is a 5-torsion point of

$$Y^2 = X^3 + 3H^2X + BH\sqrt{H}.$$

Its Hasse invariant H^2 is a 4-th power in $k(\sqrt{H})$, so again by [Vo, pp. 248/249] Q is $k(\sqrt{H})$-rational. Since $y_0 \neq 0$ this means $\sqrt[4]{H} \in k(\sqrt{H})$. If $\sqrt{H} \in k$ we are done. If not, we have $\sqrt[4]{H} = u + v\sqrt{H}$ with $u, v \in k$, and after squaring $0 = u^2 + v^2H$, so $\sqrt{H} = \frac{u\sqrt{-1}}{v} \in k$ quite the same. □

2. The main results

It is well known that elliptic curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot T^3$ can only exist in characteristics 2 and 3. If q is a power of 2 or of 3, then by [Ge5, Corollary 6.4] the Jacobian of the Drinfeld modular curve $X_0(T^3)$ is isogenous to a product of $q - 1$ elliptic curves that are explicitly described in [Ge5]. We prove the following refinement.

Theorem 2.1.

(a) *If q is a power of 2, then the strong Weil curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot T^3$ are*

$$Y^2 + XY = X^3 + \frac{c}{T^4} \quad \textit{with } c \in \mathbb{F}_q^*.$$

(b) *If q is a power of 3, then the strong Weil curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot T^3$ are*

$$Y^2 = X^3 + X^2 - \frac{c}{T^3} \quad \text{with } c \in \mathbb{F}_q^*.$$

Proof. (a) By [Sch7, Theorem 5.1] $Y^2 + XY = X^3 + \frac{c}{T}$ is up to Frobenius the only curve in its isogeny class. So the pole order of the j-invariant of the strong Weil curve at the place ∞ must be a power of 2, and we only have to show that this pole order is divisible by 4 but not by 8.

We use Corollary 1.2. At all places $T-a$ with $a \in \mathbb{F}_q^*$ the reduced curve has an $\mathbb{F}_q$-rational 4-torsion point. But it is well known (see for example [Rü, Theorem 1b]) that there exists an elliptic curve over $\mathbb{F}_q$ with non-zero j-invariant that has a 4-torsion point but no 8-torsion point over $\mathbb{F}_q$. By Lemma 1.3 this curve has an equation $Y^2 + XY = X^3 + a_6$, so it occurs as the reduction at one of the places $T-a$.

(b) The proof is similar to (a). By [Sch6, Proposition 4.3] the strong Weil curve must be $Y^2 = X^3 + X^2 - \frac{c}{T}$ up to Frobenius. So we have to show that the reductions mod $T-a$ with $a \in \mathbb{F}_q^*$ all have 3-torsion points but at least one of them has no 9-torsion points over $\mathbb{F}_q$. This follows again by combining [Rü, Theorem 1b] and Lemma 1.3. □

In Chapter 3 of [Lei] four equations of elliptic curves over $\mathbb{F}_p(T)$ with conductor $\infty \cdot T^2(T-1)$ are given uniformly in $p \geqslant 5$, and by different tricks the curves are shown to be non-isogenous over $\mathbb{F}_p(T)$ at least for the p in certain congruence classes. What seems to have escaped attention is that by the theory of Tate curves one can easily see that these 4 curves are non-isogenous over any field $\mathbb{F}_q(T)$ (of characteristic $\geqslant 5$). More precisely:

Theorem 2.2. *If $\mathrm{char}(\mathbb{F}_q) \geqslant 5$, then there are 4 isogeny classes of elliptic curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot T^2(T-1)$ and split multiplicative reduction at ∞. The Frobenius minimal curves in these classes are given in the table below, with curves in the same horizontal box belonging to the same isogeny class. The numbers (mn), respectively (mno^*), give the pole orders of the j-invariant at the places ∞ and $T-1$ (and T in the class E_1).*

No.		equation	j-invariant
E_1:	(222*)	$Y^2 = X(X+T)(X+T^2)$	$\frac{2^8(T^2-T+1)^3}{T^2(T-1)^2}$
	(114*)	$Y^2 = X^3 - 2T(T-2)X^2 + T^4X$	$\frac{-2^4(T^2-16T+16)^3}{T^4(T-1)}$
	(141*)	$Y^2 = X^3 - 2T(T+1)X^2 + T^2(T-1)^2X$	$\frac{2^4(T^2+14T+1)^3}{T(T-1)^4}$
	(411*)	$Y^2 = X^3 + 2T(2T-1)X^2 + T^2X$	$\frac{2^4(16T^2-16T+1)^3}{T(T-1)}$
E_2:	(12)	$Y^2 = X^3 - 2T^2X^2 + T^3(T-1)X$	$\frac{2^6(T+3)^3}{(T-1)^2}$
	(21)	$Y^2 = X^3 + 4T^2X^2 + 4T^3X$	$\frac{2^6(4T-3)^3}{T-1}$
E_3:	(13)	$Y^2 = X^3 - 27T^3(T+8)X + 54T^4(T^2-20T-8)$	$\frac{3^3T(T+8)^3}{(T-1)^3}$
	(31)	$Y^2 = X^3 - 3T^3(9T-8)X + 2T^4(27T^2-36T+8)$	$\frac{3^3T(9T-8)^3}{T-1}$
E_4:	(11)	$Y^2 = X^3 - 27T^4X + 54T^5(T-2)$	$\frac{2^4\cdot 3^3T^2}{T-1}$

Proof. The strategy is to first find all Frobenius minimal elliptic curves over $\overline{\mathbb{F}_p}(T)$ with conductor $\infty \cdot T^2(T-1)$ where $\overline{\mathbb{F}_p}$ is the algebraic closure of $\mathbb{F}_q$. Such a curve is an elliptic surface over $\overline{\mathbb{F}_p}$; and since the base curve is a projective line and the conductor has degree 4, it is actually an extremal elliptic surface. By [Ito, Theorem 3.1] Frobenius minimal extremal elliptic surfaces are extremal rational elliptic surface, and these have been completely classified in [La1] and [La2]. Most of the equations in the table we essentially got from [Ito] and [Lei]. Note however, that one can apply a Möbius transformation to $\overline{\mathbb{F}_p}(T)$. This means for example that not all authors place the additive fiber at $T=0$, and that the same elliptic surface might give rise to several non-isomorphic elliptic curves over $\overline{\mathbb{F}_p}(T)$. For

example, there are three pairs of curves in the table that are connected by the Möbius transformation $T \mapsto \frac{T}{T-1}$ that fixes 0 and interchanges 1 and ∞. Possibly one has to take an unramified quadratic twist to make the multiplicative reduction at ∞ split. It turns out that for each curve one can find an equation already over $\mathbb{F}_p(T)$.

Now take an equation from the table, consider it as a curve over $\mathbb{F}_q(T)$ and assume there is another curve E' over $\mathbb{F}_q(T)$ that becomes isomorphic to E over $\overline{\mathbb{F}_q}(T)$. Then E' can only be the unramified quadratic twist of E. Hence E' has non-split multiplicative reduction at ∞. This shows that the table is complete.

A curve from the class E_1, having potentially multiplicative reduction at T, cannot be isogenous to a curve from one of the other classes, as those have potentially good reduction at T. For other possible isogenies it suffices if we consider ℓ-isogenies where ℓ is a prime. From the theory of Tate curves we know that at every pole of $j(E)$ under an ℓ-isogeny the pole order will be either multiplied or divided by ℓ (regardless of whether the reduction at this place is split or non-split multiplicative or even additive). This shows that there cannot be isogenies between different E_2, E_3 and E_4.

Each of the three $\mathbb{F}_q(T)$-rational 2-torsion points of (222*) gives rise to a 2-isogeny to another Frobenius minimal elliptic curve in class E_1, that is to one of the other three curves in the box. Similarly, there is a 2-isogeny between (12) and (21) coming from the 2-torsion point $(0,0)$. Finally, the 3-torsion point $(-9T^2, 12T^2(T-1)\sqrt{-3})$ on (13) generates an $\mathbb{F}_q(T)$-rational 3-isogeny to (31). □

Remark 2.3. The equations of the isogeny classes E_1 and E_2 in Theorem 2.2 also make sense in characteristic 3, and indeed, if q is a power of 3, there exist only these two isogeny classes. Compare [Sch6, Proposition 4.2], where one should however replace the second equation by its (-1)-twist to ensure split multiplicative reduction at ∞.

In characteristic 2 there is only one isogeny class, with two Frobenius minimal curves (see [Sch7, Theorem 5.4]). It corresponds to E_3 but, of course, one has to take equations that are not in short Weierstraß form.

Theorem 2.4.

(a) *If q is a power of 2, then the equation of the (unique) strong Weil curve over $\mathbb{F}_q(T)$ with conductor $\infty \cdot T^2(T-1)$ is*

$$Y^2 + XY = X^3 + \frac{1}{T^2}X^2 + \frac{(T-1)^2}{T^8}.$$

(b) *If q is a power of 3, then there are two strong Weil curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot T^2(T-1)$, namely*

$$Y^2 = X^3 + T(T+1)X^2 + T^2X,$$

which is the curve (411) from the table in Theorem 2.2 and represents the isogeny class with supersingular reduction at the place $T+1$; and*

$$Y^2 = X^3 + T^2X^2 + TX,$$

which is the Frobenius of the curve (21) and represents the isogeny class with ordinary reduction at $T+1$.

(c) *If $\mathrm{char}(\mathbb{F}_q) \geqslant 7$, then the last equation in each horizontal box in Theorem 2.2 gives the strong Weil curve of the corresponding isogeny class.*
This also holds in characteristic 5, except for the class E_4 whose strong Weil curve then is

$$Y^2 = X^3 + 3T^4X - T(T-2)^5,$$

which is the image of the last curve under the Frobenius isogeny.

Proof. (a) By [Sch7, Theorem 5.4] there are two Frobenius minimal curves in this isogeny class, namely

$$(13): \quad Y^2 + XY = X^3 + \frac{1}{T}X^2 + \frac{(T-1)^3}{T^4} \quad \text{and}$$
$$(31): \quad Y^2 + XY = X^3 + \frac{1}{T}X^2 + \frac{T-1}{T^4}.$$

The reductions of the second equation modulo $T - a$ with $1 \neq a \in \mathbb{F}_q^*$ inherit the rational 3-torsion point $(\frac{1}{T}, \frac{1}{T^2})$. By Lemma 1.3 they also have a rational 2-torsion point. But for $q > 2$ there exists $a \in \mathbb{F}_q^*$, $a \neq 1$ such that $\frac{1}{a}$ (the coefficient of X^2) is not of the form $b^2 + b$; so by Lemma 1.3 the reduction modulo $T - a$ has no 4-torsion point. In the terminology of Corollary 1.2 we thus have $N = 6$ (except for $q = 2$; then there are no linear places of good reduction).

The multiplicative reduction at $T - 1$ is non-split if and only if q is an odd power of 2. In this case 6 divides $2q + 2$. All in all we obtain $-v_\infty(j(E)) = 6$ (also for $q = 2$). So the strong Weil curve is the Frobenius of the second equation.

(b) We start with the curve (222*) from the table in Theorem 2.2. From the j-invariant we see that the reduction at T is supersingular. Consequently 3 does not divide the pole order of the j-invariant of the strong Weil curve, which therefore has to be Frobenius minimal (cf. Corollary 1.2). On the other hand, the 2-torsion points survive every reduction and $2q + 2$ is divisible by 4. So by Theorem 2.2 and Corollary 1.2 the strong Weil curve is (411*).

For the other isogeny class we have to show $-v_\infty(j(E)) = 6$. We start with Eq. (21). The 2-torsion point $(0, 0)$ survives every reduction. We transform to

$$Y^2 = X^3 + X^2 - \frac{T-1}{T^3}.$$

Then, besides the split multiplicative reduction at $T - 1$, we see by Lemma 1.3 that the reductions at places $T - a$ have a 3-torsion point, and we have to show that at least one has no 9-torsion point over $\mathbb{F}_q$. For $q = 3$ this is clear from the Weil bounds. Writing W for $\frac{1}{T}$, the reductions we get for $q > 3$ are

$$Y^2 = X^3 + X^2 + w^3 - w^2$$

with $1 \neq w \in \mathbb{F}_q^*$. If they all had an $\mathbb{F}_q$-rational 9-torsion point, then by Lemma 1.3 the elliptic curve $U^3 - U = W^3 - W^2$ would have at least $3(q - 2)$ rational points over $\mathbb{F}_q$, which is impossible.

(c) First we use Corollary 1.2 to show that up to Frobenius the strong Weil curve is always the last equation in each horizontal box. Obviously all reductions of (222*) have a full set of rational 2-torsion points and 4 divides $2q + 2$. Similarly with the 2-torsion point of (12). The curve (13) has a 3-torsion point

$$\big(-9T^2, 12T^2(T-1)\sqrt{-3}\big).$$

If $q \equiv 1 \bmod 3$, this gives a rational 3-torsion point on the reductions. Moreover, the harmonicity condition at the vertex e_0^1 of the quotient graph (or equivalently, the fact that the L-polynomial of our curves are constant 1) implies that the multiplicative reduction at $T - 1$ is split. If $q \equiv 2 \bmod 3$, then $2q + 2$ is divisible by 3, but the above point does not give a rational point on the reduced curve $\tilde{E}$. However, it shows that the twist of $\tilde{E}$ has an $\mathbb{F}_q$-rational 3-torsion point. Since the number of rational points on $\tilde{E}$ and its twist add up to $2q + 2$, this shows that $\tilde{E}$ must have (another) rational 3-torsion point.

Now we want to show that the strong Weil curve is Frobenius minimal (at least for $p \geqslant 7$). Let $A_p(T)$ be the Hasse invariant of E. For our curves $A_p(T)$ has degree at most $p - 1$ and is divisible

by T^2. By [Si, pp. 141/142] the number of $\mathbb{F}_q$-rational points on the reduction of E mod $T-a$ is congruent to $1-A_q(a)$ modulo p where

$$A_q(a) = \big(A_p(a)\big)^{\frac{q-1}{p-1}}.$$

Now assume that p divides $v_\infty(j(E))$. Then $A_q(a)=1$ for all $a \in \mathbb{F}_q \setminus \{0,1\}$. With the properties mentioned above one easily shows that then necessarily $A_q(T) = T^{q-1}$ and hence $A_p(T) = cT^{p-1}$ with $c \in \mathbb{F}_p$. This means that for the curve over $\mathbb{F}_p(T)$, i.e. for $q=p$, the values of the corresponding cycle φ on the edges from e_1^1 to e_0^1 are all congruent to c modulo p. By the harmonicity condition this is only possible if either $c=0$ (in which case we are done) or if $c=1$. The latter case means that all reductions $\tilde{E}$ at places $T-a$ with $a \in \mathbb{F}_p \setminus \{0,1\}$ have an $\mathbb{F}_p$-rational p-torsion point. For the classes E_1, E_2 and E_3 the Weil bound then gives

$$2p \leqslant \#\big(\tilde{E}(\mathbb{F}_p)\big) \leqslant p+1+2\sqrt{p},$$

which is only possible for $p \leqslant 5$. Despite first appearance to the contrary, the same argument can be made to work for the curve (11). We transform it into

$$Y^2 = X^3 - 27X + 54\left(1-\frac{2}{T}\right).$$

If $p \geqslant 7$ and X runs through $\mathbb{F}_p$, then X^3-27X takes at least 3 different values. So we can find $a \in \mathbb{F}_p \setminus \{0,1\}$ such that for $T=a$ the cubic polynomial has a zero in $\mathbb{F}_p$. Thus there exists a reduction with an $\mathbb{F}_p$-rational 2-torsion point.

Finally we deal with characteristic 5. Then the curve (222*) has Hasse invariant $T^2(T^2-T+1)$, and the classes E_2 and E_3 have supersingular reduction at $T-2$. Transforming Eq. (11) into

$$Y^2 = X^3 + 3X + \frac{2}{T} - 1$$

we see by Lemma 1.3 that all reductions have a rational 5-torsion point and that all elliptic curves with a 5-torsion point, including those without a 25-torsion point, occur among these reductions. Moreover, the multiplicative reduction at $T-1$ is split. So in this case $-v_\infty(j(E)) = 5$. □

We avoid getting lost in trying to write down equations for the curves with square-free $\mathfrak{n} \in \mathbb{F}_q[T]$ of degree 3.

In the special case of characteristic 2 all these curves have been explicitly determined in Sections 3 and 4 of [Sch7]. In a certain sense the proof in that paper is unnecessarily complicated. As an alternative strategy one can see from Szpiro's conjecture [PeSz] that the Frobenius minimal ones give rational elliptic surfaces, and then one can, as in the proof of Theorem 2.2, determine the forms over $\mathbb{F}_q(T)$ of the equations in [La1] and [La2]. This approach was already outlined in [Ng, Proposition 4]. As one excuse we mention that the complete proof [PeSz] of Szpiro's conjecture in characteristic 2 had not been published yet when [Sch7] was written.

In any case, for any finite field $\mathbb{F}_q$ and any given $\mathfrak{n} \in \mathbb{F}_q[T]$ of degree 3, writing down all elliptic curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$ is (at least in principal) mainly a matter of patience. We content ourselves with the following example.

Example 2.5. Let $\mathfrak{n} \in \mathbb{F}_q[T]$ be a monic irreducible polynomial of degree 3. Then the necessary and sufficient condition for the existence of an elliptic curve $E/\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$ is that by a translation $T \mapsto T+b$ one can bring $\mathfrak{n}$ into the form T^3-c. In particular, such curves exist if and only if $q \equiv 1 \bmod 3$.

Indeed, suppose that $E/\mathbb{F}_q(T)$ is such a curve. We may assume that it is Frobenius minimal. Over $\overline{\mathbb{F}_q}$ its equation gives a rational extremal elliptic surface, whose j-invariant has at least 3 different poles of the same order. Up to affine transformation of T this can only be a surface (3333) or (9111) from [La1]. But these surfaces don't exist in characteristic 3. Hence we can find a translation $T \mapsto T + b$ that transforms $\mathfrak{n}$ into a polynomial $T^3 + c_1 T + c_0$. Since the elliptic curves (3333) and (9111) have conductor $\infty \cdot (T^3 - 1)$ we see that $c_1 = 0$. But irreducible polynomials of the form $T^3 - c$ exist only if $q \equiv 1 \bmod 3$.

Conversely, if $q \equiv 1 \bmod 3$, then $\mathbb{F}_q^*$ contains an element c that is not a third power. Then for example

$$Y^2 = X^3 - 3T\big(T^3 + 8c\big)X - 2\big(T^6 - 20cT^3 - 8c^2\big)$$

has conductor $\infty \cdot (T^3 - c)$. We have taken the (-1)-twist of the curve in [Ge1, Table 9.3] to make sure that the multiplicative reduction at ∞ is split.

Even without the explicit knowledge of the curves we can make the following statement.

Theorem 2.6. *Semistable strong Weil curves $E/\mathbb{F}_q(T)$ of conductor $\infty \cdot \mathfrak{n}$ with $\deg(\mathfrak{n}) = 3$ are Frobenius minimal.*

Proof. We even prove that $v_\infty(j(E))$ is not divisible by p, the characteristic of $\mathbb{F}_q$. For every $a \in \mathbb{F}_q$ we have $\langle \varphi, \delta_a - \delta_\infty \rangle \equiv \varphi(a) - 1 \bmod q$. Thus, if p divides $v_\infty(j(E))$, then all entries of φ must be congruent to 1 mod p. But this contradicts the condition that the sum over these entries has to be 0. □

In characteristic 3 we can prove more. By [Sch6, Proposition 4.1] the elliptic curves with square-free $\mathfrak{n} \in \mathbb{F}_{3^r}[T]$ of degree 3 have two or no linear places of supersingular reduction. Calculating modulo 3 we see $\langle \varphi, \varphi \rangle \not\equiv 0 \bmod 3$. This shows not only that the strong Weil curve is Frobenius minimal, but also that the degree of the strong Weil uniformization is not divisible by 3.

Using additional machinery, Theorem 2.6 can be generalized as follows.

Lemma 2.7. *Semistable strong Weil curves $E/\mathbb{F}_q(T)$ of conductor $\infty \cdot \mathfrak{n}$ where $\mathfrak{n}$ has an irreducible factor $\mathfrak{p}$ with $\deg(\frac{\mathfrak{n}}{\mathfrak{p}}) \leqslant 2$ are Frobenius minimal.*

Proof. If $\mathfrak{n}$ is irreducible, this is [Pa1, Theorem 1.2]. More generally, in the terminology of [Pa2], if E is not Frobenius minimal, then by [Pa2, Theorem 1.1] we have $p \in C(\mathfrak{p})$, but $C(\mathfrak{p}) = \emptyset$ since $S(\mathfrak{n})^{\mathfrak{p}\text{-old}} = 0$. □

Comparing Theorems 2.1, 2.4 and 2.6 with the elliptic surfaces in [La1] and [La2], or alternatively, with the results in [Ito] and [Sch6], we obtain the following fact.

Theorem 2.8. *If $E/\mathbb{F}_q(T)$ is a strong Weil curve with conductor $\infty \cdot \mathfrak{n}$ where $\deg(\mathfrak{n}) = 3$, then the corresponding elliptic surface is a rational surface over $\overline{\mathbb{F}_q}$.*

One might conjecture that the same statement holds for $\deg(\mathfrak{n}) = 4$. This is true at least for $q = 2$ (see the table in [Sch2]) or if $\mathfrak{n}$ is square-free but does not split completely into linear factors. To see the last claim note that for $\deg(\mathfrak{n}) = 4$ in general Szpiro's conjecture [PeSz] still implies that Frobenius minimal elliptic curves $E/\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$ give rational elliptic surfaces over $\overline{\mathbb{F}_q}$, and by Lemma 2.7 those where $\mathfrak{n}$ is square-free of degree 4 but has a non-linear irreducible factor are Frobenius minimal.

In any case, the elliptic surfaces corresponding to the strong Weil curves with $\deg(\mathfrak{n}) = 4$ are at least unirational. This also implies, by the way, that for these elliptic curves the conjecture of Birch and Swinnerton-Dyer holds (see [Shi, Section 3]).

3. Complements

At least in one case we want to make Theorem 2.6 more explicit.

Example 3.1. In characteristic 2, semistable elliptic curves $E/\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$ where $\mathfrak{n}$ is the product of 3 different linear factors exist if and only if q is a power of 4. Moreover, for these curves $\mathfrak{n}$ can be transformed to $(T-1)(T-s)(T-s^2)$ where s is a primitive third root of unity (see Section 3 in [Sch7]). For example,

$$(3333): \quad Y^2 + TXY + Y = X^3 + T^3 + 1$$

is such a curve. Since all its 3-torsion points are rational, one can show by the same arguments as in the previous theorems that the corresponding strong Weil curve is

$$(9111): \quad Y^2 + TXY + Y = X^3.$$

The numbers $(klmn)$ give the pole orders of the j-invariant at the places ∞, 1, s and s^2. There are 3 more isogeny classes with this conductor and their strong Weil curves are

$$(5511): \quad Y^2 + TXY + Y = X^3 + X^2 + T,$$
$$(5115): \quad Y^2 + sTXY + Y = X^3 + X^2 + sT,$$
$$(5151): \quad Y^2 + s^2TXY + Y = X^3 + X^2 + s^2T$$

in the terminology of [Sch7, Theorem 3.2].

If $q = 2^{2n+1}$, the curve (9111) has conductor $\infty \cdot (T-1)(T^2+T+1)$ but in general it will not be the strong Weil curve in this situation. For example if $q = 2$, the strong Weil curve of this class is (3333) (see [GeRe, Example 9.7.4] or [Ge2, Example 4.4] or [Ge3, Example 9.4]).

Proposition 3.2. *If $q = 4$ and $\mathfrak{n}$ is the product of three different linear factors, then the curve $X_0(\mathfrak{n})$ has no $\mathbb{F}_4(T)$-rational points except the 8 cusps.*

Proof. After translation we can suppose $\mathfrak{n} = T(T-1)(T-v)$. From Table 10.2 in [Ge1] we easily calculate that $X_0(T(T-1)(T-v))$ maps with degree 4 to the corresponding strong Weil curves. By the previous example, one of these is a transformation of (9111), which has only 3 rational points. Thus $X_0(\mathfrak{n})$ has at most 12 rational points over $\mathbb{F}_4(T)$.

But at the same time the number of these points is divisible by 8. This follows from the action of the Atkin–Lehner involutions on the rational points. Namely, by the proof of Lemma 12 in [Sch4] the fixed points of these Atkin–Lehner involutions correspond to Drinfeld modules with complex multiplication by orders in $\mathbb{F}_q[\sqrt{T}]$, and by [Sch3, Lemma 4] these Drinfeld modules have j-invariants that are inseparable over $\mathbb{F}_q(T)$. Thus the fixed points are not rational. So the Atkin–Lehner involutions (which form a group of order 8) act freely on the $\mathbb{F}_q(T)$-rational points of $X_0(\mathfrak{n})$. □

By analogous arguments one can show that the curve $X_0(\mathfrak{n})$ has no $\mathbb{F}_q(T)$-rational points outside the cusps for the following values

$$q = 2, \qquad \mathfrak{n} = T^3, T^2(T-1), T\left(T^2+T+1\right),$$
$$q = 3, \qquad \mathfrak{n} = T(T-1)(T+1), T^2(T-1).$$

But for bigger q the attempt is too weak, simply because the degree of the strong Weil uniformization grows with q. More precisely:

Lemma 3.3. *Let $\pi : X_0(\mathfrak{n}) \to E$ be the uniformization of a strong Weil curve E over $\mathbb{F}_q(T)$ of conductor $\infty \cdot \mathfrak{n}$ with $deg(\mathfrak{n}) = 3$. Then*

$$\frac{q}{2} \leqslant deg(\pi) \leqslant -v_\infty\big(j(E)\big)deg(\pi) \leqslant 4q^2 + q + 1.$$

Proof. Let $W_\mathfrak{n}$ be the full Atkin–Lehner involution of $X_0(\mathfrak{n})$. It is well known that in the case $deg(\mathfrak{n}) = 3$ the quotient curve $W_\mathfrak{n} \setminus X_0(\mathfrak{n})$ is rational (cf. [Ge1] or [Sch4]). Applying Castelnuovo's inequality (see for example [Sti, Theorem III.10.3]) to π and the canonical map $\kappa : X_0(\mathfrak{n}) \to W_\mathfrak{n} \setminus X_0(\mathfrak{n})$, we obtain

$$\begin{aligned} g\big(X_0(\mathfrak{n})\big) &\leqslant deg(\pi)g(E) + deg(\kappa)g\big(W_\mathfrak{n} \setminus X_0(\mathfrak{n})\big) + \big(deg(\pi) - 1\big)\big(deg(\kappa) - 1\big) \\ &= 2deg(\pi) - 1. \end{aligned}$$

For $deg(\mathfrak{n}) = 3$ it is also well known that $g(X_0(\mathfrak{n})) = q$ if $\mathfrak{n}$ is square-free, and $g(X_0(\mathfrak{n})) = q - 1$ otherwise.

The upper bound comes from estimating $\langle \varphi, \varphi \rangle$. □

Acknowledgments

This paper was written while I was holding a visiting position at the National Center for Theoretical Sciences (NCTS) in Hsinchu, Taiwan. I want to thank all the people there for their support.

References

[Ge1] E.-U. Gekeler, Automorphe Formen über $\mathbb{F}_q(T)$ mit kleinem Führer, Abh. Math. Sem. Univ. Hamburg 55 (1985) 111–146.
[Ge2] E.-U. Gekeler, Analytical construction of Weil curves over function fields, J. Théor. Nombres Bordeaux 7 (1995) 27–49.
[Ge3] E.-U. Gekeler, Jacquet–Langlands theory over K and relations with elliptic curves, in: E.-U. Gekeler, M. van der Put, M. Reversat, J. Van Geel (Eds.), Drinfeld Modules, Modular Schemes and Applications, Proceedings of a Workshop at Alden Biesen, September 9–14, 1996, World Scientific, Singapore, 1997, pp. 224–257.
[Ge4] E.-U. Gekeler, Highly ramified pencils of elliptic curves in characteristic two, Duke Math. J. 89 (1997) 95–107.
[Ge5] E.-U. Gekeler, Local and global ramification properties of elliptic curves in characteristics two and three, in: B.H. Matzat, G.-M. Greuel, G. Hiß (Eds.), Algorithmic Algebra and Number Theory, Springer, Berlin, Heidelberg, New York, 1998, pp. 49–64.
[GeNo] E.-U. Gekeler, U. Nonnengardt, Fundamental domains of some arithmetic groups over function fields, Internat. J. Math. 6 (1995) 689–708.
[GeRe] E.-U. Gekeler, M. Reversat, Jacobians of Drinfeld modular curves, J. Reine Angew. Math. 476 (1996) 27–93.
[Ito] H. Ito, On unirationality of extremal elliptic surfaces, Math. Ann. 310 (1998) 717–733.
[La1] W. Lang, Extremal rational elliptic surfaces in characteristic p. I: Beauville surfaces, Math. Z. 207 (1991) 429–438.
[La2] W. Lang, Extremal rational elliptic surfaces in characteristic p. II: Surfaces with three or fewer singular fibres, Ark. Mat. 32 (1994) 423–448.
[Lei] R. Leitl, Elliptische Kurven über $\mathbb{F}_q(T)$ mit kleinem Führer, Diplomarbeit, Saarbrücken, 1995.
[Ng] K.V. Nguyen, On families of curves over $\mathbb{P}^1$ with small number of singular fibres, C. R. Acad. Sci. Paris 326 (1998) 459–463.
[Pa1] M. Papikian, Pesenti–Szpiro inequality for optimal elliptic curves, J. Number Theory 114 (2005) 361–393.
[Pa2] M. Papikian, Abelian subvarieties of Drinfeld Jacobians and congruences modulo the characteristic, Math. Ann. 337 (2007) 139–157.
[PeSz] J. Pesenti, L. Szpiro, Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques, Compos. Math. 120 (2000) 83–117.
[Rü] H.G. Rück, A note on elliptic curves over finite fields, Math. Comp. 49 (179) (1987) 301–304.
[Sch1] A. Schweizer Zur Arithmetik der Drinfeld'schen Modulkurven $X_0(\mathfrak{n})$, Dissertation, Saarbrücken, 1996.
[Sch2] A. Schweizer, Modular automorphisms of the Drinfeld modular curves $X_0(\mathfrak{n})$, Collect. Math. 48 (1997) 209–216.
[Sch3] A. Schweizer, On singular and supersingular invariants of Drinfeld modules, Ann. Fac. Sci. Toulouse Math. 6 (1997) 319–334.
[Sch4] A. Schweizer, Hyperelliptic Drinfeld modular curves, in: E.-U. Gekeler, M. van der Put, M. Reversat, J. Van Geel (Eds.), Drinfeld Modules, Modular Schemes and Applications, Proceedings of a Workshop at Alden Biesen, September 9–14, 1996, World Scientific, Singapore, 1997, pp. 330–343.
[Sch5] A. Schweizer, On elliptic curves in characteristic 2 with wild additive reduction, Acta Arith. 91 (1999) 171–180.
[Sch6] A. Schweizer, Extremal elliptic surfaces in characteristic 2 and 3, Manuscripta Math. 102 (2000) 505–521.

[Sch7] A. Schweizer, On elliptic curves over function fields of characteristic two, J. Number Theory 87 (2001) 31–53.
[Shi] T. Shioda, Some remarks on elliptic curves over function fields, Astérisque 209 (1992) 99–114.
[Si] J.H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 106, Springer, Berlin, Heidelberg, New York, 1986.
[Sti] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer, Berlin, Heidelberg, New York, 1993.
[Vo] J.F. Voloch, Explicit p-descent for elliptic curves in characteristic p, Compos. Math. 74 (1990) 247–258.