ACTA ARITHMETICA
XCI.2 (1999)

On elliptic curves in characteristic 2 with wild additive reduction

by

Andreas Schweizer (Montreal)

Introduction. In [Ge1] Gekeler classified all elliptic curves over $\mathbb{F}_{2^r}(T)$ with one rational place of multiplicative reduction (without loss of generality located at ∞), one further rational place of bad reduction (without loss of generality located at 0) and good reduction elsewhere. So these curves have conductor $\infty \cdot T^n$ where n is a natural number (which actually can be arbitrarily large). In [Ge2] he extended his results to characteristic 3. Roughly, his strategy can be divided into four steps:

1. Using Drinfeld modular curves, determine the places of supersingular reduction of the elliptic curves with such a conductor.
2. This gives control over the zeros and poles of the j-invariants of these curves.
3. Use Tate's algorithm to calculate the conductors of the "untwisted" elliptic curves with the possible j-invariants.
4. Control the effect of twisting on the conductor.

In this paper we extend the results in characteristic 2 by allowing one more place of multiplicative reduction, without loss of generality located at $T = 1$.

Actually we first prove a quite general and semi-explicit form of step 1, namely: Given a finite field $\mathbb{F}_q$ (of any characteristic), the places of supersingular reduction of an elliptic curve E over $\mathbb{F}_q(T)$ with multiplicative reduction at ∞ are contained in a finite set $\mathfrak{S}$ that depends only on the support of the conductor of E. The set $\mathfrak{S}$ is given in terms of a Drinfeld modular curve. But it is difficult to make this result really explicit, and even in our simple situation this requires circumstantial arguments and modifications.

The author gratefully acknowledges support from CICMA (Centre Interuniversitaire en Calcul Mathématique Algébrique) in the form of a postdoctoral position at Concordia University and McGill University.

1991 *Mathematics Subject Classification*: 11G05, 11G09.

1. Basic facts. As usual $\mathbb{F}_q$ is a finite field with q elements. We denote by A the polynomial ring $\mathbb{F}_q[T]$ and by K its quotient field $\mathbb{F}_q(T)$. Later we will specialize to the case where the characteristic of $\mathbb{F}_q$ is 2.

We use the symbol ∞ for the place of K corresponding to the degree valuation. In other words, ∞ is the pole divisor of T. All other places of K are written as monic irreducible polynomials $\mathfrak{p} \in A$ and divisors not containing ∞ as monic polynomials $\mathfrak{n} \in A$. The completion of K at the place ∞ is denoted by K_∞. Furthermore C is the completion of an algebraic closure of K_∞ and $\Omega := C - K_\infty$ is the Drinfeld upper half-plane.

It is well known (and easy to prove) that an elliptic curve over $\mathbb{F}_q(T)$ with non-constant j-invariant has only finitely many places of supersingular reduction. The central idea of [Ge1] and [Ge2] is to make this more explicit using Drinfeld modular curves. The following fact is fundamental in this context.

THEOREM 1.1 [G&R]. *Over $\mathbb{F}_q(T)$ every elliptic curve with conductor $\infty \cdot \mathfrak{n}$ and split multiplicative reduction at ∞ is isogenous to a one-dimensional factor of the Jacobian of the Drinfeld modular curve $X_0(\mathfrak{n})$.*

Recall that a (smooth, geometrically connected, projective) curve of genus g over a field of characteristic p is called *ordinary* if the p-rank of its Jacobian is as big as possible, namely g.

All Drinfeld modular curves (i.e. all curves coming from the action of arithmetic subgroups of $\mathrm{GL}_2(A)$ on Ω) are ordinary. This was shown in [G&R] by explicit construction of their Jacobians.

Statements relating ordinarity of a curve to its quotients have been proved (and reproved) in several degrees of generality. We cite the version that is the most convenient for our purposes.

THEOREM 1.2 [Ray]. *For a curve X over a field of characteristic p and a finite p-group G of automorphisms of X the following two conditions are equivalent*:

(a) *X is ordinary*,

(b) *the curve $G\backslash X$ is ordinary and the second ramification groups of the covering $X \to G\backslash X$ are trivial.*

Unfortunately, for $\mathfrak{m} \mid \mathfrak{n}$ the covering $X_0(\mathfrak{n}) \to X_0(\mathfrak{m})$ is in general not Galois except for some special cases for $q = 2$. The idea (due to [Ge1]) is to apply the lemma to a somewhat bigger curve. Let

$$\Gamma_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) : a \equiv d \equiv 1 \bmod \mathfrak{n},\ c \equiv 0 \bmod \mathfrak{n} \right\}.$$

As an algebraic curve the corresponding Drinfeld modular curve $X_1(\mathfrak{n})$ is defined over a finite Galois extension of K depending on $\mathfrak{n}$. Moreover, $X_1(\mathfrak{n})$ has good reduction at all places not dividing $\infty \cdot \mathfrak{n}$.

Theorem 1.3. *Let $\mathbb{F}_q$ be a finite field and let $\mathfrak{B}$ be a finite set of places of $\mathbb{F}_q(T)$ not containing the place ∞. Then there exists a finite set $\mathfrak{S}$ of places of $\mathbb{F}_q(T)$ (depending on q and on $\mathfrak{B}$) such that every elliptic curve over $\mathbb{F}_q(T)$ with multiplicative reduction at ∞ and good reduction outside $\mathfrak{B} \cup \{\infty\}$ has ordinary reduction outside $\mathfrak{S} \cup \mathfrak{B} \cup \{\infty\}$.*

To be more explicit: Let $\mathfrak{m}$ be the product of all $\mathfrak{p} \in \mathfrak{B}$. Then we can take $\mathfrak{S}$ to be the set of all places of K above which there is a place of good and non-ordinary reduction of $X_1(\mathfrak{m})$.

Proof. The quickest way to see that $\mathfrak{S}$ is finite is presumably the following: Since $X_1(\mathfrak{m})$ is ordinary, the determinant of its Hasse–Witt matrix is non-zero. Hence the determinant is non-zero at almost all places of good reduction. Therefore the reduction is ordinary at almost all places.

Now let $\mathfrak{n}$ be a divisor of K whose support is $\mathfrak{B}$. We prove inductively that the curve $X_{1,0}(\mathfrak{m}, \mathfrak{n})$ belonging to the group $\Gamma_1(\mathfrak{m}) \cap \Gamma_0(\mathfrak{n})$ has good and ordinary reduction at all places not lying above the places in $\mathfrak{S} \cup \mathfrak{B} \cup \{\infty\}$. Let $\mathfrak{p} \in \mathfrak{B}$; then $\Gamma_1(\mathfrak{m}) \cap \Gamma_0(\mathfrak{n}\mathfrak{p})$ is a normal subgroup of $\Gamma_1(\mathfrak{m}) \cap \Gamma_0(\mathfrak{n})$ of index $q^{\deg(\mathfrak{p})}$. So we can apply the reasoning of [Ge2, 5.7] to the covering $X_{1,0}(\mathfrak{m}, \mathfrak{n}\mathfrak{p}) \to X_{1,0}(\mathfrak{m}, \mathfrak{n})$. Namely: This covering is unramified outside the cusps. As $X_{1,0}(\mathfrak{m}, \mathfrak{n}\mathfrak{p})$ is ordinary, by Theorem 1.2 the second ramification groups are trivial. Since for a place of good reduction the reduction map is injective on the cusps, we see from the Hurwitz formula that the second ramification groups of the covering of the reductions are also trivial. Thus by Theorem 1.2 the curve $X_{1,0}(\mathfrak{m}, \mathfrak{n}\mathfrak{p})$ has ordinary reduction at all the places where $X_{1,0}(\mathfrak{m}, \mathfrak{n})$ has.

Finally, let E be an elliptic curve with conductor $\infty \cdot \mathfrak{n}$. We may suppose that the multiplicative reduction at ∞ is split. Otherwise we replace E by its unramified quadratic twist, which has the same places of supersingular reduction. Combining the covering $X_{1,0}(\mathfrak{m}, \mathfrak{n}) \to X_0(\mathfrak{n})$ with Theorem 1.1 we see that E is an isogeny factor of the Jacobian of $X_{1,0}(\mathfrak{m}, \mathfrak{n})$, which has good and ordinary reduction outside $\mathfrak{S} \cup \mathfrak{B} \cup \{\infty\}$. ■

Of course, an elliptic curve need not have supersingular reduction at every place in $\mathfrak{S}$. The real strength of Theorem 1.3 lies in characteristic 2 and 3, where the exponent of a place in the conductor is not bounded and hence infinitely many isogeny classes of elliptic curves may share the same places of bad reduction.

Proposition 1.4. *Let $\mathbb{F}_q$ be a finite field of characteristic 2 or 3 and let E be an elliptic curve over $\mathbb{F}_q(T)$. Then $j(E)$ has poles at all places of multiplicative reduction of E and zeros at all places of supersingular reduction. All other poles or zeros of $j(E)$ must be among the places of additive reduction.*

Proof. The proof for characteristic 2 in [Sch2] also holds in characteristic 3. Slightly modified, the proposition would even be true in all characteristics p for which 0 is a supersingular invariant, that is, for all $p \equiv 2 \bmod 3$. ■

As explained in [Si], Appendix A, every elliptic curve E over a field K of characteristic 2 with $j(E) \neq 0$ can be written in normal form

$$E: \quad Y^2 + XY = X^3 + a_2X^2 + a_6$$

with $a_6 = 1/j(E)$ and $a_2 \in K$. The discriminant of this model is $\Delta = a_6$. For $\alpha \in K$ we call

$$E_\alpha: \quad Y^2 + XY = X^3 + (a_2 + \alpha)X^2 + a_6$$

the *α-twist* of E. Both curves become isomorphic over the quadratic extension $K(\beta)$ with $\beta^2 + \beta = \alpha$. The conductor of $K(\beta)$ is also called the conductor of the twist α. For every field k of characteristic 2 we write $\wp(k)$ for the image of k under the additive map $x \mapsto x^2 + x$. The above procedure puts the K-isomorphism classes of elliptic curves with the same non-zero j-invariant into bijection with $K/\wp(K)$.

Theorem 1.5 [Ge1]. *Let $K = \mathbb{F}_q(T)$ be of characteristic* 2.

(a) *The exponents $f(E)$, $f(\alpha)$, and $f(E_\alpha)$ of a place in the conductors of the elliptic curve E, the quadratic twist α, and the twisted curve E_α are related by*

$$f(E_\alpha) \leq \max\{f(E), 2f(\alpha)\},$$

with equality in case $f(E) \neq 2f(\alpha)$.

(b) *The quadratic twists α that are unramified outside the place T are represented by the unramified quadratic twist $\alpha \in \mathbb{F}_q - \wp(\mathbb{F}_q)$ and by the twists*

$$\alpha = \alpha_0 + \alpha_1T^{-1} + \alpha_3T^{-3} + \ldots + \alpha_{2d-1}T^{-(2d-1)}$$

with $\alpha_i \in \mathbb{F}_q$ and $\alpha_{2d-1} \neq 0$. These twists have conductor T^{2d}.

From an elliptic curve over K (of characteristic 2) one can obtain a K-isogenous one by simply squaring the coefficients of the equation. This Frobenius isogeny obviously commutes with quadratic twists. Since $Y^2 + XY = X^3 + a_2X^2 + 1/j(E)$ and $Y^2 + XY = X^3 + a_2^2X^2 + 1/j(E)$ are isomorphic over K, we see that a curve is "Frobenius-minimal" if and only if $j(E)$ is not a square in K.

2. A special Drinfeld modular curve.

On first view the previous section looks like an effective method to classify elliptic curves with given places of bad reduction. It is a slightly generalized version of Gekeler's strategy in [Ge1] and [Ge2], where he classified elliptic curves with conductor $\infty \cdot T^n$.

The next conductors to treat would be $\infty \cdot T^n(T-1)^m$. But here we run already into a problem. If we want to classify elliptic curves with these conductors over all fields $\mathbb{F}_q(T)$ with $\mathrm{char}(\mathbb{F}_q) = 2$ say, then we have to control the places of non-ordinary reduction of infinitely many different curves $X_1(T(T-1))$. Namely, for every field $\mathbb{F}_q$ the curve $X_1(T(T-1))$ has genus $(q-2)^2$ ([G&N], Corollary 5.7). So these curves are not related in an easy way, and especially the curve for $\mathbb{F}_{q^r}(T)$ is not a base change of the one for $\mathbb{F}_q(T)$.

Actually the determination of $\mathfrak{S}$ seems to be the main difficulty in the whole business. For conductors $\infty \cdot T^n$ this was so to say for free since $X_1(T)$ has genus 0 (and hence $\mathfrak{S}$ is empty) for all q.

Faute de mieux we compromise somewhat and restrict the third place of bad reduction of our elliptic curves to be of multiplicative type, that is, we treat elliptic curves with conductor $\infty \cdot T^n(T-1)$. Then we can carry out the induction of Theorem 1.3 with a smaller curve, namely with the curve

$$X_{(n)} = X_{1,0}(T, T^n(T-1))$$

belonging to the group

$$\begin{aligned} \Gamma_{(n)} &= \Gamma_1(T) \cap \Gamma_0(T^n(T-1)) \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(A) : a \equiv d \equiv 1 \bmod T,\ c \equiv 0 \bmod T^n(T-1) \right\}. \end{aligned}$$

Lemma 2.1. *The genus of* $X_{(1)}$ *is at most* $q-2$.

Proof. The curve $X_0(T(T-1))$ has genus 0 and 4 cusps. Since the covering $X_{(1)} \to X_0(T(T-1))$ is abelian of degree $q-1$ and unramified outside the cusps, the Hurwitz formula yields the claimed bound. ∎

A closer examination would reveal that the four cusps are indeed totally ramified and hence $g(X_{(1)}) = q-2$. We will obtain this as a by-product in the next lemma.

The points of $X_{(1)}$ over C which are not cusps (i.e. the elements of $\Gamma_{(1)}\backslash\Omega$) are in bijection with the isomorphism classes of quadruples (ϕ, u, P_1, P_2) consisting of a rank 2 Drinfeld module ϕ over C, a cyclic $(T-1)$-isogeny u of ϕ, a primitive T-torsion point P_1 of ϕ, and a primitive point P_2 on the quotient of the T-torsion by $\langle P_1\rangle$. Two quadruples (ϕ, u, P_1, P_2) and (ϕ', u', P_1', P_2') are isomorphic if there exists an isomorphism from ϕ to ϕ' that maps (u, P_1, P_2) to (u', P_1', P_2').

Of course (ϕ, u) describes the moduli problem for $X_0(T-1)$, and the one for $X_1(T)$ is given by (ϕ, P_1, P_2). This might be surprising when compared with the classical modular curve $X_1(N)$ which parametrizes elliptic curves with a primitive N-torsion point. The explanation is that when working with $\mathrm{SL}_2(\mathbb{Z})$ one of the conditions $a \equiv 1 \bmod N$ and $d \equiv 1 \bmod N$ in the definition of $\Gamma_1(N)$ is redundant.

We also hasten to remark that for $\deg(\mathfrak{n}) > 1$ the moduli problem for $X_1(\mathfrak{n})$ is not the obvious generalization of our description for $X_1(T)$.

From now on we restrict to the case $\mathrm{char}(\mathbb{F}_q) = 2$.

On $X_{(1)}$ we have at our disposal the Atkin–Lehner involution W_{T-1} given by the action of the matrix $\left(\begin{smallmatrix} T-1 & 1 \\ T^2-T & T-1 \end{smallmatrix}\right)$ on the upper half-plane. In terms of the moduli interpretation W_{T-1} maps the quadruple (ϕ, u, P_1, P_2) to $(\psi, u^t, u(P_1), u(P_2))$ where ψ is the image of ϕ under the isogeny u and u^t is the dual isogeny.

Lemma 2.2. (a) *The curve* $W_{T-1}\backslash X_{(1)}$ *has genus* 0.

(b) *The curve* $X_{(1)}$ *has genus* $q-2$ *and is hyperelliptic for* $q \geq 4$.

Proof. The restriction of W_{T-1} to the rational curve $X_0(T-1)$ has one fixed point. As explained in [Sch1], this fixed point can be represented by the tuple (ϕ, λ) where ϕ is the Drinfeld module with complex multiplication by $\mathbb{F}_q[\sqrt{T}]$ and $\lambda \in \mathrm{End}(\phi)$ with $\lambda^2 = T-1$.

Let P_1 be a non-zero point in the kernel of the endomorphism $\sqrt{T}$. Obviously P_1 is a T-torsion point and $\lambda P_1 = P_1$. For every T-torsion point P_2 which is not contained in $\langle P_1 \rangle$ we have $\lambda P_2 = \sqrt{T} P_2 + P_2$ with $\sqrt{T} P_2 \in \langle P_1 \rangle$. Thus for every choice of P_1 and P_2 mod $\langle P_1 \rangle$ the quadruple $(\phi, \lambda, P_1, P_2)$ is fixed under the involution W_{T-1}. Still $\mathrm{Aut}(\phi) = \mathbb{F}_q^\times$ acts on these quadruples. Fixing P_1 we obtain representatives of the $q-1$ fixed points of W_{T-1} on $X_{(1)}$.

Now the Hurwitz formula implies $g(W_{T-1}\backslash X_{(1)}) = 0$ and also $g(X_{(1)}) \geq q-2$. ∎

Remark. We point out that in odd characteristic there exist at least two different involutions on $X_{(1)}$ which restrict to the usual Atkin–Lehner involution on $X_0(T-1)$. They differ by certain minus-signs in the matrix and in the moduli interpretation. One has no fixed points on $X_{(1)}$, the other has $2(q-1)$. Therefore Lemma 2.2(b) is also true in odd characteristic.

Lemma 2.3. *In characteristic* 2 *the curves* $X_{(n)}$ *have good and ordinary reduction outside* $\infty \cdot T(T-1)$.

Proof. It suffices to prove the statement for $X_{(1)}$. Then for $X_{(n)}$ we can perform the same induction as in the proof of Theorem 1.3.

Fix a place $\wp$ lying above a place $\mathfrak{p}$ of K not dividing $\infty \cdot T(T-1)$. The curve $W_{T-1}\backslash X_{(1)}$ has genus 0 and hence ordinary reduction mod $\wp$. We want to lift this property to $X_{(1)}$ by using Theorem 1.2. As in the proof of Theorem 1.3 we only have to show that the fixed points of W_{T-1} on $X_{(1)}$ do not fall together modulo $\wp$.

Upon reduction the Drinfeld module ϕ becomes supersingular, that is, the endomorphism ring of the reduced Drinfeld module $\bar{\phi}$ is a maximal order $\mathcal{O}$ in the quaternion algebra over K ramified at $\mathfrak{p}$ and ∞. Moreover $\mathrm{End}(\phi)$ embeds into $\mathrm{End}(\bar{\phi})$. Clearly the quadruples $(\bar{\phi}, \lambda, \overline{P}_1, \overline{P}_2)$ are distinct, but we have to show that they are not isomorphic.

An automorphism of $(\bar{\phi}, \lambda)$ is a unit in $\mathcal{O}$ that commutes with λ. Hence it must be an element of $\mathbb{F}_q[\sqrt{T}]^\times = \mathbb{F}_q^\times$. So the reductions of the $q-1$ fixed points are indeed distinct. ∎

3. Elliptic curves with conductor $\infty \cdot T^n(T-1)$. We maintain the restriction $\mathrm{char}(\mathbb{F}_q) = 2$.

We want to classify elliptic curves over $K = \mathbb{F}_q(T)$ with two places of multiplicative and one place of additive reduction where all these places are assumed to be $\mathbb{F}_q$-rational.

After a Möbius transformation $T \mapsto (\alpha T+\beta)/(\gamma T+\delta)$ with $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$ and $\alpha\delta \neq \beta\gamma$, we may suppose that the three places of bad reduction are ∞, 0, and 1 and that the additive reduction is located at 0.

PROPOSITION 3.1. *Every elliptic curve E over K which has conductor $\infty \cdot T^n(T+1)$ must have invariant*

$$j(E) = \varepsilon \frac{T^k}{(T+1)^l}$$

with $\varepsilon \in \mathbb{F}_q^\times$ and $k > l > 0$.

Proof. As in Theorem 1.3 we may suppose that E is modular. Then Lemma 2.3 tells us that E has no places of supersingular reduction. So by Proposition 1.4 the support of the divisor of $j(E)$ is contained in $\infty \cdot T(T+1)$. Furthermore $j(E)$ has poles at ∞ and 1. Hence it must vanish at $T = 0$. ∎

Obviously, such a curve is Frobenius-minimal if and only if at least one of k and l is odd. In the next two lemmas we treat curves with slightly more general j-invariants.

LEMMA 3.2. *Let $k, l \in \mathbb{Z}$, not both even, with $k + l > 0$ and let $\varepsilon \in \mathbb{F}_q^\times$. The standard curve*

$$Y^2 + XY = X^3 + \frac{\varepsilon}{T^k(T+1)^l}$$

has split multiplicative reduction at ∞ and conductor $\infty \cdot T^n(T+1)^m$ with

$$n = \begin{cases} 0 & \text{if } k = 0, \\ 1 & \text{if } k < 0, \\ k+2 & \text{if } 2 \nmid k \text{ and } k > 0, \\ k & \text{if } 2 \mid k \text{ and } k > 3, \\ 3 & \text{if } k = 2, \end{cases}$$

and analogously for m.

Proof. This is a straightforward application of Tate's algorithm ([Ta]). The cases $l = 0$ resp. $l < 0$ are already in [Ge1] resp. [Sch2]. ∎

LEMMA 3.3. *Let E be an elliptic curve as in Lemma* 3.2 *with $k \equiv 0$* mod 4 *(and hence $2 \nmid l$). Let further $\delta \in \mathbb{F}_q^\times$.*

(a) *For $k > 4$ the exponent of T in the conductor of the twisted curve*

$$E_\alpha : \quad Y^2 + XY = X^3 + \frac{\delta}{T^{k/2-1}}X^2 + \frac{\varepsilon}{T^k(T+1)^l}$$

is

$$\operatorname{ord}_T(\operatorname{cond}(E_\alpha)) = \begin{cases} k-1 & \textit{if } \delta^2 = \varepsilon, \\ k & \textit{if } \delta^2 \neq \varepsilon. \end{cases}$$

(b) *The exponent of T in the conductor of the curve*

$$Y^2 + XY = X^3 + \frac{\delta}{T}X^2 + \frac{\varepsilon}{T^4(T+1)^l}$$

is

$$\operatorname{ord}_T(\operatorname{cond}(E_\alpha)) = \begin{cases} 2 & \textit{if } \delta^2 = \varepsilon = 1, \\ 3 & \textit{if } \delta^2 = \varepsilon \neq 1, \\ 4 & \textit{if } \delta^2 \neq \varepsilon. \end{cases}$$

Proof. For $l < 0$ this was shown in [Sch2]. The general proof is exactly the same. ∎

We summarize:

Theorem 3.4. *Every elliptic curve over K with conductor $\infty \cdot T^n(T+1)$ is Frobenius isogenous to a curve*

$$Y^2 + XY = X^3 + \alpha X^2 + \varepsilon\frac{(T+1)^l}{T^k}$$

where $k > l > 0$, not both even, $\varepsilon \in \mathbb{F}_q^\times$ and the twist α is unramified outside $T = 0$.

Conversely, every curve of this form has conductor $\infty \cdot T^n(T-1)$ and n can be easily determined by means of Lemmas 3.2 and 3.3 and Theorem 1.5. In particular all $n \geq 2$ occur.

Making the equations integral, we can also say: The elliptic curves over K with conductor $\infty \cdot T^n(T+1)$ are the ones of the form

$$Y^2 + T^dXY = X^3 + P(T)X^2 + \varepsilon T^e(T+1)^l$$

with $e \in \mathbb{N}_0$, $d \in \mathbb{N}$, $0 < l < 6d - e$, $\varepsilon \in \mathbb{F}_q^\times$, and $P(T) \in \mathbb{F}_q[T]$ of degree at most $2d$.

Corollary 3.5. *Elliptic curves over K with conductor $\infty^n\mathfrak{p}$ where $\mathfrak{p}$ is a prime divisor of degree 2 exist only for $n = 3$ and for even $n > 2$.*

Proof. Suppose E is such a curve. Over the quadratic constant field extension $\mathbb{F}_{q^2}(T)$ the place $\mathfrak{p}$ splits into two rational places at which $j(E)$ has the same pole order. Using a Möbius transformation of $\mathbb{F}_{q^2}(T)$ we can change these two places to ∞ and 1 and the place ∞ to 0. Then $j(E)$ is as in Proposition 3.1 with $l = k - l$. If moreover E is Frobenius minimal, then

l must be odd and hence $k \equiv 2 \bmod 4$. This restricts n to the possibilities mentioned above.

On the other hand, for odd l the curve $Y^2+XY = X^3+\varepsilon\mathfrak{p}^l$ has conductor $\infty^n\mathfrak{p}$ with $n = 3$ for $l = 1$ and $n = 2l$ for $l \geq 3$. The values $n \equiv 0 \bmod 4$ can be realized by twisting. ∎

4. Some further results. We recall that the curve $X_1(T(T-1))$ has genus $(q-2)^2$. Analogously to W_{T-1} which is an involution on $X_1(T(T-1))$ we can define the involution $W_T = \left(\begin{smallmatrix} T^2 & 1 \\ T^2-T & T \end{smallmatrix}\right)$ on $X_1(T(T-1))$. The two commute and their product is the full Atkin–Lehner involution $W_{T^2-T} = \left(\begin{smallmatrix} 0 & 1 \\ T^2-T & 0 \end{smallmatrix}\right)$.

LEMMA 4.1. *If $q \in \{2,4\}$, then the Drinfeld modular curve $X_1(T(T-1))$ has good and ordinary reduction outside $\infty \cdot T(T-1)$.*

Proof. For $q = 2$ this is trivial because then the curve has genus 0.

So let $q = 4$. We fix a place not dividing $\infty \cdot T(T-1)$ and denote the reduction at this place by a tilde. W_{T-1} has 3 fixed points on $\widetilde{X}_{(1)}$. Over each of these there lies at least one fixed point on $(X_1(T(T-1)))^{\sim}$. Analogously W_T has at least 3 fixed points on $(X_1(T(T-1)))^{\sim}$ and W_{T^2-T} has at least one (lying over the unique fixed point on the rational curve $(X_0(T(T-1)))^{\sim}$). So the Hurwitz formula shows that the curve $\langle W_T, W_{T-1}\rangle\backslash(X_1(T(T-1)))^{\sim}$ has genus 0 and that the second ramification groups are trivial. Thus $(X_1(T(T-1)))^{\sim}$ is ordinary by Theorem 1.2. ∎

Combining the previous lemma with Theorem 1.3 and Proposition 1.4 we obtain

PROPOSITION 4.2. *Let $q \in \{2,4\}$. Then every elliptic curve over $\mathbb{F}_q(T)$ with conductor $\infty \cdot T^n(T+1)^m$ is Frobenius isogenous to a quadratic twist, unramified outside $T(T+1)$, of a standard curve from Lemma* 3.2. *The pairs (m,n) that occur are exactly the ones where at least one of m,n is incongruent to* 2 mod 4 *and greater than* 2.

Similarly to Corollary 3.5 we can conclude from this that elliptic curves over $\mathbb{F}_2(T)$ with conductor $\infty \cdot (T^2+T+1)^n$ exist if and only if $3 \leq n \not\equiv 2 \bmod 4$. But this could also be obtained directly from [Ge2].

If the j-invariant of an elliptic curve E over K has a pole at a place $\mathfrak{p}$, then there exists a quadratic twist α, unramified outside $\mathfrak{p}$, such that the twisted curve E_α has multiplicative reduction at $\mathfrak{p}$ (compare the proof of Proposition 2.1 in [Ge1]). Using this and the previous results we obtain

PROPOSITION 4.3. *If* $\mathrm{char}(\mathbb{F}_q) = 2$, *there are three types of elliptic curves E over $\mathbb{F}_q(T)$ with conductor $\infty^e \cdot T^n(T-1)^m$:*

(a) *$j(E)$ is not constant. Without loss of generality* (*i.e. after a Möbius transformation*) *$j(E)$ has a pole at ∞. If $q \in \{2,4\}$, then E is of the form*

$$Y^2 + XY = X^3 + \alpha X^2 + \frac{\varepsilon}{T^k(T+1)^l}$$

where $k+l > 0$ *and* $\varepsilon \in \mathbb{F}_q^\times$ *and the twist* α *is unramified outside* $\infty \cdot T(T+1)$. (*It is quite likely that this holds for all even* q.) *Moreover*, *in this case* $e \equiv 0 \bmod 4$ *unless* $e = 1$.

(b) $j(E) \in \mathbb{F}_q^\times$. *Then* E *is of the form*

$$Y^2 + XY = X^3 + \alpha X^2 + \varepsilon$$

where $\varepsilon \in \mathbb{F}_q^\times$ *and the twist* α *is unramified outside* $\infty \cdot T(T+1)$. *Necessarily* $e \equiv n \equiv m \equiv 0 \bmod 4$.

(c) $j(E) = 0$. *In this case* E *is of the form*

$$Y^2 + \varepsilon T^k(T+1)^l Y = X^3 + a_4 X + a_6$$

with $k, l \in \mathbb{N}_0$, $\varepsilon \in \mathbb{F}_q^\times$ *and* $a_4, a_6 \in \mathbb{F}_q[T]$.

References

[Ge1] E.-U. Gekeler, *Highly ramified pencils of elliptic curves in characteristic two*, Duke Math. J. 89 (1997), 95–107.

[Ge2] —, *Local and global ramification properties of elliptic curves in characteristics two and three*, in: Algorithmic Algebra and Number Theory, B. H. Matzat, G.-M. Greuel and G. Hiß (eds.), Springer, 1998, 49–64.

[G&N] E.-U. Gekeler and U. Nonnengardt, *Fundamental domains of some arithmetic groups over function fields*, Internat. J. Math. 6 (1995), 689–708.

[G&R] E.-U. Gekeler and M. Reversat, *Jacobians of Drinfeld modular curves*, J. Reine Angew. Math. 476 (1996), 27–93.

[Ray] M. Raynaud, *Mauvaise réduction des courbes et p-rang*, C. R. Acad. Sci. Paris 319 (1994), 1279–1282.

[Sch1] A. Schweizer, *Hyperelliptic Drinfeld modular curves*, in: Drinfeld Modules, Modular Schemes and Applications, E.-U. Gekeler, M. van der Put, M. Reversat and J. Van Geel (eds.), World Sci., Singapore, 1997, 330–343.

[Sch2] —, *On elliptic curves over function fields of characteristic two*, submitted.

[Si] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[Ta] J. Tate, *Algorithm for determing the type of a singular fiber in an elliptic pencil*, in: Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer, 1975, 33–52.

CICMA, Department of Mathematics
Concordia University
1455 Boulevard de Maisonneuve Ouest
Montreal, Quebec H3G 1M8
Canada
E-mail: schweiz@cicma.concordia.ca

Received on 7.12.1998 (3524)