Journal of Number Theory **87**, 31–53 (2001)
doi:10.1006/jnth.2000.2582, available online at http://www.idealibrary.com on IDEAL®

On Elliptic Curves over Function Fields of Characteristic Two

Andreas Schweizer

Institute of Mathematics, Academia Sinica, Nankang, Taipei, Taiwan
E-mail: schweiz@math.sinica.edu.tw

Communicated by David Goss

Received March 22, 1999; published online January 26, 2001

and describe explicitly all elliptic curves over $\mathbb{F}_{2^r}(T)$ having a conductor of degree 4. Our results also imply that extremal elliptic surfaces over the algebraic closure of $\mathbb{F}_2$ are unirational. © 2001 Academic Press

0. INTRODUCTION

It is well known that the conductor of a non-constant elliptic curve over a rational function field $\mathbb{F}_q(T)$ is a divisor of degree at least 4.

In this paper we classify explicitly all elliptic curves over $\mathbb{F}_{2^r}(T)$ with a conductor of degree 4.

Since in characteristic 2 (and 3) the exponent of a prime divisor in the conductor can be bigger than 2, there are 11 possibilities for the decomposition of such a conductor into prime divisors of $\mathbb{F}_{2^r}(T)$. Namely, there are 5 semistable (i.e. square-free) types, 3 types without multiplicative reduction, and 3 mixed types.

The curves without multiplicative reduction (treated in Section 6) are different from the others as they turn out to be twisted constant curves.

The classification of the curves with a place of multiplicative reduction is carried out in Sections 3 to 5. To find their equations we apply the same strategy that was used in [Ge3] and [Ge4] to classify elliptic curves in characteristics 2 and 3 with conductors $\infty \cdot T^n$:

(1) Find the places of supersingular reduction of the elliptic curves with such a conductor.

0022-314X/01 $35.00

(2) This restricts the possible prime divisors of the j-invariants of these curves.

(3) Use Tate's algorithm to determine the conductors of the "untwisted" elliptic curves with the possible j-invariants.

(4) Describe the effect of twisting on the conductor.

(5) Divide the curves with the wanted conductor into isogeny classes.

The first step relies on the fact that these elliptic curves are isogeny factors of the Jacobian of a Drinfeld modular curve (at least after a suitable constant field extension and a suitable transformation of T). It is clearly the key step. In order to make it work for our conductors we have to refine the method by taking into consideration the Atkin–Lehner involution of the Drinfeld modular curve (Section 2). In view of Theorem 1.5 this restricts us to characteristic 2, in contrast to the experience that this characteristic usually causes the most problems.

Many of our results, for example Proposition 2.3 and the numbers of isogeny classes, have first been guessed from the tables (for $q \leqslant 16$) in [Ge1].

An elliptic curve E over $\mathbb{F}_q(T)$ can also be interpreted as an elliptic surface over $\mathbb{F}_q$. Here by an elliptic surface we mean an elliptic fibration $S \rightarrow C$ with a base curve C and a section. Recall that over an algebraically closed field of positive characteristic an elliptic surface which has at least one bad fiber is called extremal if its Picard number ρ equals its second Betti number b_2 and its Mordell-Weil rank r is 0.

If the conductor of $E/\mathbb{F}_q(T)$ has degree 4, the corresponding elliptic surface will be extremal; and conversely, every extremal elliptic surface over the algebraic closure of a finite field is obtained in this way. This results from the formula

$$r + b_2 - \rho = 4g(C) - 4 + deg(conductor),$$

valid also in characteristic 2 and 3. (Compare Proposition 4.2 in [Ito] and Section 1 of [Sh]).

In [La1] and [La2] W. Lang has determined all extremal rational elliptic surfaces in all positive characteristics. It turns out that in our situation every Frobenius isogeny class contains at least one curve such that the corresponding elliptic surface over $\overline{\mathbb{F}_2}$ is listed in [La1] or [La2]. Thus our results also provide a partial answer to Problem 3.4 in [Ito]:

PROPOSITION. *Every extremal elliptic surface over the algebraic closure of $\mathbb{F}_2$ is unirational.*

1. BASIC FACTS

Throughout this paper $\mathbb{F}_q$ will be a finite field of characteristic 2 with q elements. We denote by A the polynomial ring $\mathbb{F}_q[T]$ and by K its quotient field $\mathbb{F}_q(T)$.

The choice of T distinguishes a place ∞ of K corresponding to the degree valuation. The places of K different from ∞ correspond to the monic irreducible polynomials in A, which we will occasionally also call primes. Often we will refer to a K-rational place $T-t$ simply as the place t.

Also, for the decomposition type of a divisor we use a notation that should be self-explaining; for example the divisor $\infty \cdot T^3(T^2+T+1)$ of $\mathbb{F}_2(T)$ is of type $(1, 1^3, 2)$.

We will quite frequently use the fact that $Aut(K/\mathbb{F}_q)$ is isomorphic to $PGL_2(\mathbb{F}_q)$, where a matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ acts on K by the Möbius transformation $T \mapsto \frac{aT+b}{cT+d}$.

In characteristic 2 the well-known formulas for the discriminant and the j-invariant of an elliptic curve E in long Weierstraß form

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6$$

simplify to

$$\Delta = a_1^6 a_6 + a_1^5 a_3 a_4 + a_1^4 a_2 a_3^2 + a_1^4 a_4^2 + a_3^4 + a_1^3 a_3^3$$

and

$$j(E) = a_1^{12}/\Delta.$$

Depending on the j-invariant we can find shorter normal forms.

Proposition 1.1. *Let E be an elliptic curve over K with $j(E)=0$. Then there exist $a_3, a_4, a_6 \in A$ and $d \in \mathbb{N}_0$ such that*

$$Y^2 + a_3 Y = X^3 + a_4 X + a_6$$

is a model of E which is minimal at all places different from ∞ and

$$Y^2 + \frac{a_3}{T^{3d}}\, Y = X^3 + \frac{a_4}{T^{4d}} X + \frac{a_6}{T^{6d}}$$

is minimal at ∞.

The discriminant of the above model over A is a_3^4.

Proof. Since A is a principal ideal domain, there exists a long Weierstraß form over A which outside ∞ is a minimal model for E. Furthermore $j=0$ is equivalent to $a_1=0$.

A closer look at the transformations in Tate's algorithm ([Ta] or [Si2]) that are necessary to make the model minimal at ∞ shows that these can be carried out on the equation over A without destroying the minimality at the finite primes.

Finally, by the shift $X \mapsto X + a_2$ we can get rid of a_2. ∎

Elliptic curves E over K with $j(E) \neq 0$ can be written in normal form

$$Y^2 + XY = X^3 + a_2 X^2 + a_6,$$

where $a_6 = \frac{1}{j(E)}$ and $a_2 \in K$ (compare [Si1] Appendix A). Then $\Delta = a_6$.

If $j(E) \neq 0$, then every elliptic curve over K with the same j-invariant is a quadratic twist of E. Indeed, replacing a_2 in the above normal form by $a_2 + \alpha$ with $\alpha \in K$ corresponds to twisting E by the extension $L = K(\beta)$ with $\beta^2 + \beta = \alpha$. The conductor of L 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 $x \mapsto x^2 + x$.

Thus replacing a_2 by $a_2 + \alpha$ with $\alpha \in \wp(K)$ doesn't change the curve. Replacing a_2 by $a_2 + \alpha$ with $\alpha \in \mathbb{F}_q - \wp(\mathbb{F}_q)$ means twisting E by the quadratic constant field extension $\mathbb{F}_{q^2}(T)$ of K. This twist changes neither the conductor nor the type of reduction (supersingular, additive, multiplicative) but it multiplies the values $\delta_{\mathfrak{p}}$ by $(-1)^{deg(\mathfrak{p})}$ where we use the convention $\delta_{\mathfrak{p}} = 1$ (resp. $\delta_{\mathfrak{p}} = -1$) if the multiplicative reduction at $\mathfrak{p}$ is split (resp. non-split).

More generally, we have

Theorem 1.2 [Ge3].

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

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

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

(b) *Modulo the trivial twists $\wp(K)$ and modulo the twist by the constant field extension, the quadratic twists that are unramified outside the place T are the ones of the form*

$$\alpha = \alpha_1 T^{-1} + \alpha_3 T^{-3} + \cdots + \alpha_{2d-1} T^{-(2d-1)}$$

where $\alpha_i \in \mathbb{F}_q$ and $\alpha_{2d-1} \in \mathbb{F}_q^\times$. The conductor of such a twist is T^{2d}.

If the j-invariant of an elliptic curve E over K is not constant, the K-isogeny class of E contains infinitely many K-isomorphism classes since we can apply the Frobenius isogeny (i.e., squaring the coefficients of the equation) again and again.

Since $Y^2+XY=X^3+a_2X^2+\frac{1}{j(E)}$ is isomorphic to $Y^2+XY=X^3+a_2^2X^2+\frac{1}{j(E)}$, we see that a curve is "Frobenius-minimal" if and only if $j(E)$ is not a square in K. In Sections 3 to 5 we will describe K-isogeny classes by specifying their Frobenius-minimal curves. The following simple fact is fundamental for our calculations.

PROPOSITION 1.3. *Let $j(E)=\frac{f(T)}{g(T)}$ with relatively prime $f(T)$, $g(T)\in A$ be the j-invariant of the elliptic curve E over K. Then*:

(a) *Only primes of bad reduction can divide $g(T)$. All primes of multiplicative reduction divide $g(T)$.*

(b) *Only primes of additive or supersingular reduction can divide $f(T)$. All primes of supersingular reduction divide $f(T)$.*

(c) *If E has multiplicative reduction at ∞, then deg$(f)>$deg(g).*

Proof. E has a model over A which is minimal at all finite places and $g(T)$ divides its discriminant. If $\mathfrak{p}$ is a place of multiplicative reduction, then over the completion $K_{\mathfrak{p}}$ of K either E or its twist by the unramified quadratic extension of $K_{\mathfrak{p}}$ is a Tate curve, so $j(E)$ has a pole at $\mathfrak{p}$.

Statement (b) follows easily from (a) and the fact that an elliptic curve in characteristic 2 is supersingular if and only if its j-invariant is 0. ▮

To get a handle on the places of supersingular reduction we have to make a detour involving Drinfeld modular curves. In particular we need the (proven!) analogue of the conjecture of Shimura, Taniyama and Weil, namely that the modular elliptic curves over K are exactly those that are Tate curves at ∞.

THEOREM 1.4 [G&R]. *Every elliptic curve over K with conductor $\infty\cdot\mathfrak{n}$ and split multiplicative reduction at ∞ is K-isogenous to a one-dimensional factor of the Jacobian of the Drinfeld modular curve $X_0(\mathfrak{n})$.*

The genus of a curve over a field of characteristic p is an upper bound for the p-rank of its Jacobian. The curve is called ordinary, if this p-rank equals the genus. For elliptic curves this is just the usual definition of being ordinary as opposed to being supersingular.

The Drinfeld modular curves $X_0(\mathfrak{n})$ are ordinary; in [G&R] their Jacobians are described by means of certain multiplicative period lattices. In Section 2 we will use the following theorem to show the ordinarity of the reduction of $X_0(\mathfrak{n})$ at certain primes and hence the ordinarity of certain reductions of some modular elliptic curves.

Theorem 1.5 [Cr], [Ray]. *Let X be a curve over a field of characteristic p, and let G be a finite p-group of automorphisms of X. Then the following two conditions are equivalent*:

(a) *X is ordinary.*

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

2. THE PLACES OF SUPERSINGULAR REDUCTION

It is well known that for a prime $\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{n}$ the Drinfeld modular curve $X_0(\mathfrak{n})$ has good reduction mod $\mathfrak{p}$. We denote this reduction by $\widetilde{X_0(\mathfrak{n})}$.

The inner (i.e., non-cusp) points of $\widetilde{X_0(\mathfrak{n})}$ correspond to isomorphism classes of triples (ϕ, u, ψ) where ϕ and ψ are Drinfeld modules of rank 2 in A-characteristic $\mathfrak{p}$ and u is a cyclic $\mathfrak{n}$-isogeny from ϕ to ψ. The Atkin–Lehner involution $W_\mathfrak{n}$ induces a nontrivial involution $\widetilde{W_\mathfrak{n}}$ on $\widetilde{X_0(\mathfrak{n})}$, which acts on these triples by mapping (ϕ, u, ψ) to (ψ, u^t, ϕ) where $u^t \circ u = \mathfrak{n}$ in $End(\phi)$.

We also need quaternion algebras for our proof but, strangely enough, not the ones which are endomorphism rings of supersingular elliptic curves.

Let $\mathbb{H}_\mathfrak{p}$ be the quaternion algebra over K ramified at ∞ and $\mathfrak{p}$. An embedding of a quadratic order B into a maximal order $\mathcal{O}$ of $\mathbb{H}_\mathfrak{p}$ is called *optimal* if the intersection of the quotient field of B with $\mathcal{O}$ is B and not a bigger order.

Fix a maximal order $\mathcal{O}$ in $\mathbb{H}_\mathfrak{p}$ and a set of representatives I_i, $i = 1, ..., h(\mathbb{H}_\mathfrak{p})$ for the left ideal classes of $\mathcal{O}$. Let $\mathcal{O}_i$ be the right order of the ideal I_i. We denote by $m(B_\mathfrak{f}, \mathcal{O}_i)$ the number of optimal embeddings of the inseparable order $B_\mathfrak{f} = A[\mathfrak{f}\sqrt{T}]$ into $\mathcal{O}_i$ modulo conjugation by $\mathcal{O}_i^\times$.

Lemma 2.1. *If $\mathfrak{p} \nmid \mathfrak{f}$ then*

$$\sum_{i=1}^{h(\mathbb{H}_\mathfrak{p})} m(B_\mathfrak{f}, \mathcal{O}_i) = h(B_\mathfrak{f}),$$

where $h(B_\mathfrak{f})$ is the ideal class number of $B_\mathfrak{f}$.

Proof. Unfortunately, all the results in the literature on optimal embeddings of quadratic orders seem to be stated only for separable orders. It is however not difficult to check that the arguments on pp. 96–101 of [Ei] carry over to our situation. ∎

Lemma 2.2. *Let $\mathfrak{n} = T^3 + aT^2 + bT + c \in A$ be a polynomial of degree 3. There exists a unique $s \in \mathbb{F}_q$ with $s^2 = b$. At all places outside $\infty \cdot \mathfrak{n} \cdot (T - s)$ the Drinfeld modular curve $X_0(\mathfrak{n})$ has good and ordinary reduction.*

Proof. We fix a place $\mathfrak{p}$ not dividing $\infty \cdot \mathfrak{n} \cdot (T-s)$. It is well known that the genus of $\widetilde{X_0(\mathfrak{n})}$ is q or $q-1$ depending on whether $\mathfrak{n}$ is square-free or not.

So we only have to find $q+1$ (respectively q) fixed points of $\widetilde{W}_{\mathfrak{n}}$. Then we will see from the Hurwitz formula that $\widetilde{W}_{\mathfrak{n}} \backslash \widetilde{X_0(\mathfrak{n})}$ has genus 0, that there are no other fixed points, and that the second ramification groups of $\widetilde{W}_{\mathfrak{n}}$ are trivial. Since $\widetilde{W}_{\mathfrak{n}} \backslash \widetilde{X_0(\mathfrak{n})}$, being a rational curve, is trivially ordinary, Theorem 1.5 then will imply that $X_0(\mathfrak{n})$ *mod* $\mathfrak{p}$ is ordinary.

To construct the fixed points we use the embeddings of B_{T-s} into $\mathcal{O}_i$. Writing $\sqrt{\mathfrak{n}} = l(T) + (T-s)\sqrt{T}$ with $l(T) \in A$, one easily sees the following chain of equivalences:

$$(T-s) \mid \mathfrak{n} \Leftrightarrow (T-s) \mid l(T) \Leftrightarrow (T-s)^2 \mid \mathfrak{n} \Leftrightarrow \mathfrak{n} \text{ has a multiple root.}$$

Putting $\lambda = l(T) + (T-s)\sqrt{T}$, each embedding of B_{T-s} into an $\mathcal{O}_i$ corresponds to some $\lambda \in \mathcal{O}_i$ with $\lambda^2 = \mathfrak{n}$. If the embedding is optimal, λ is primitive, i.e., cannot be divided in $\mathcal{O}_i$ by any non-constant $\mathfrak{a} \in A$. If $\mathfrak{n}$ is square-free, the optimal embedding of B_1 gives rise to another primitive λ in some $\mathcal{O}_i$, because $(T-s) \nmid l(T)$. By Lemma 2.1 the number of these primitive λ up to conjugation by $\mathcal{O}_i^\times$ thus is $h(B_{T-s}) + h(B_1) = q+1$ for square-free $\mathfrak{n}$, and $h(B_{T-s}) = q$ otherwise.

According to [Ge2], the isomorphism classes of supersingular Drinfeld modules of rank 2 in A-characteristic $\mathfrak{p}$ are in bijection with the left ideal classes of $\mathcal{O}$, their endomorphism rings being isomorphic to the right orders $\mathcal{O}_i$. Thus every primitive $\lambda \in \mathcal{O}_i$ with $\lambda^2 = \mathfrak{n}$ gives rise to a triple $(\phi_i, \lambda, \phi_i)$ invariant under $\widetilde{W}_{\mathfrak{n}}$. (The primitivity guarantees that $\lambda \in \mathcal{O}_i = End(\phi_i)$ has cyclic kernel.) Of course, conjugates of λ by $\mathcal{O}_i^\times$ give isomorphic triples and hence the same fixed point.

So we have constructed enough fixed points, up to one subtlety. We have to exclude the possibility that together with $\lambda^2 = \mathfrak{n}$ for $\lambda \in \mathcal{O}_i$ we also have $(\varepsilon\lambda)^2 = \mathfrak{n}$ for some $1 \neq \varepsilon \in \mathcal{O}_i^\times$, because both elements would lead to the same fixed point.

Obviously, $(\varepsilon\lambda)^2 = \mathfrak{n} = \lambda^2$ can only occur if ε doesn't commute with λ. One easily verifies that in this situation $\{1, \varepsilon, \lambda, \varepsilon\lambda\}$ is the A-basis of an order in $\mathbb{H}_{\mathfrak{p}}$ and that the discriminant of this order is $\mathfrak{n}^2$. Together with $\mathfrak{p} \nmid \mathfrak{n}$ this contradicts the fact that $\mathbb{H}_{\mathfrak{p}}$ is ramified at $\mathfrak{p}$.

Hence we have found enough fixed points and the proof is complete. ∎

PROPOSITION 2.3. *Let E be an elliptic curve over K with conductor $\infty \cdot \mathfrak{n}$ where $\mathfrak{n} = T^3 + aT^2 + bT + c \in A$ is a polynomial of degree* 3. *There exists a unique $s \in \mathbb{F}_q$ with $s^2 = b$.*

(a) *At all places outside* $\infty \cdot \mathfrak{n} \cdot (T-s)$ *the curve* E *has good and ordinary reduction.*

(b) *At the places dividing* $\infty \cdot \mathfrak{n}$ *and different from* $T-s$ *the reduction of* E *is multiplicative.*

(c) *If* $(T-s) \mid \mathfrak{n}$, *then* E *has additive reduction at* $T-s$. *If* $(T-s) \nmid \mathfrak{n}$, *the reduction of* E *at* $T-s$ *is supersingular.*

Proof. Replacing E by its twist with the quadratic constant extension of K if necessary, we may suppose that E is a Tate curve at ∞. Then (a) follows from combining Theorem 1.4 with Lemma 2.2.

If $\mathfrak{n}$ has a multiple root, this root obviously must be s. This already proves statement (b).

Equally easily one shows that s cannot be a simple root of $\mathfrak{n}$, which settles the first half of (c). Finally, $j(E)$ must have a pole at ∞. By Proposition 1.3 the only possible prime divisor of the numerator of $j(E)$ is $T-s$. This shows the supersingularity of the reduction mod $(T-s)$ in case $(T-s) \nmid \mathfrak{n}$. ▌

The remainder of this section will not be needed in the sequel, but is interesting in its own right.

We want to indicate that the method of proof of Lemma 2.2 can be generalized. Namely, instead of $W_{\mathfrak{n}}$ we may use partial Atkin–Lehner involutions $W_{\mathfrak{m}}$ of $X_0(\mathfrak{n})$. We refer to [Sch1] for an account of their most important properties.

Every $\mathfrak{m} \in A$ can be written as $\mathfrak{m} = \mathfrak{c}^2 + \mathfrak{d}^2 T$ with uniquely determined $\mathfrak{c}, \mathfrak{d} \in A$. We write $\mathfrak{d}(W_{\mathfrak{m}})$ for the $\mathfrak{d}$ defined by $\mathfrak{m}$ in this way. Obviously the polynomial $T-s$ in Lemma 2.2 is a special case of this.

LEMMA 2.4. *Suppose* $\mathfrak{n} \in A$ *is square-free, and let* G *be a subgroup of the Atkin–Lehner involutions of* $X_0(\mathfrak{n})$. *If the prime* $\mathfrak{p} \in A$ *satisfies the following three conditions*:

(a) $\mathfrak{p} \nmid \mathfrak{n}$,

(b) *the curve* $G \backslash X_0(\mathfrak{n})$ *has ordinary reduction mod* $\mathfrak{p}$,

(c) $\mathfrak{p} \nmid \mathfrak{d}(W_{\mathfrak{m}})$ *for all* $W_{\mathfrak{m}} \in G$,

then the reduction of $X_0(\mathfrak{n})$ *mod* $\mathfrak{p}$ *is ordinary.*

Sketch of proof. For square-free $\mathfrak{n}$ we have a complete description of the fixed points of all Atkin–Lehner involutions $W_{\mathfrak{m}}$ on $X_0(\mathfrak{n})$ (compare Lemma 12 in [Sch1] and its proof). The fixed points of $\widetilde{W}_{\mathfrak{m}}$ on the reduction of $X_0(\mathfrak{n})$ mod $\mathfrak{p}$ for $\mathfrak{p} \nmid \mathfrak{n}$ involve supersingular Drinfeld modules ϕ such that $End(\phi)$ contains an optimally embedded $B_{\mathfrak{f}}$ with $\mathfrak{f} \mid \mathfrak{d}(W_{\mathfrak{m}})$. If $\mathfrak{p} \nmid \mathfrak{d}(W_{\mathfrak{m}})$, one can conclude from Lemma 2.1 that $\widetilde{W}_{\mathfrak{m}}$ has as many fixed points on $\widetilde{X_0(\mathfrak{n})}$ as $W_\mathfrak{m}$ has on $X_0(\mathfrak{n})$. Since the second ramification groups of $W_\mathfrak{m}$ are trivial, by the Hurwitz formula the same must hold for $\widetilde{W}_\mathfrak{m}$. Theorem 1.5 completes the proof. ▌

At the price of making the description more technical we could even give a more general version of Lemma 2.4 for arbitrary $\mathfrak{n}$, but one doesn't seem to gain much.

Obviously, we can only make use of this lemma if we have some control over the curve $G\backslash X_0(\mathfrak{n})$. This is the case for example if $G\backslash X_0(\mathfrak{n})$ is rational or if it is elliptic and we know its places of supersingular reduction. There are only finitely many such curves with $deg(\mathfrak{n}) \geqslant 4$. They are listed in [Sch2].

Take for example $q=2$ and $\mathfrak{n}=T(T^4+T^3+1)$, and let G be the full group of Atkin–Lehner involutions of $X_0(\mathfrak{n})$. As described in [Sch2] Propositions 5.6 and 4.5, in this case $G\backslash X_0(\mathfrak{n})$ is an elliptic curve of conductor $\infty \cdot (T^4+T^3+1)$ and isogenous over $\mathbb{F}_2(T)$ to $Y^2+TXY+Y=X^3+X^2$. One easily verifies that T is the only place of supersingular reduction of this elliptic curve. For the non-trivial elements of G we have $\mathfrak{d}(W_T)=1$, $\mathfrak{d}(W_{T^4+T^3+1})=T$, and $\mathfrak{d}(W_\mathfrak{n})=(T+1)^2$. Hence for $q=2$ the curve $X_0(T(T^4+T^3+1))$ has good and ordinary reduction at all places outside $\infty \cdot T(T^4+T^3+1)(T+1)$.

Now if $q=2$ and $\mathfrak{n} \in A$, the covering $X_0(T^2\mathfrak{n}) \to X_0(T\mathfrak{n})$ is galois of degree 2. Moreover it is unramified outside the cusps. Since for every place $\mathfrak{p}$ not dividing $\infty \cdot T\mathfrak{n}$ the reduction map mod $\mathfrak{p}$ is injective on the set of cusps, we can use Theorem 1.5 to show inductively that $X_0(T^n\mathfrak{n})$ has ordinary reduction mod $\mathfrak{p}$ provided we know that $X_0(T\mathfrak{n})$ has.

By similar arguments we obtain

Proposition 2.5. *Let E be an elliptic curve over $\mathbb{F}_2(T)$ with conductor $\infty \cdot \mathfrak{n}$. If n and m are positive integers, then we obtain the following table of possible places of supersingular reduction of E* (see Table 1).

TABLE 1

$\mathfrak{n}$	No supersingular reduction outside
T^n	—
$T^n(T^2+T+1)$	$T+1$
$T^n(T^3+T^2+1)$	$T+1$
$T^n(T^3+T+1)$	$T+1$
$T^n(T^4+T^3+1)$	$T+1$
$T^n(T+1)^m$	—
$T^n(T+1)^m\,(T^2+T+1)$	—
$T^n(T+1)^m\,(T^3+T+1)$	T^2+T+1

Together with Proposition 1.3 this yields strong restrictions on the possible j-invariants of such curves.

3. CURVES WITH 4 RATIONAL PLACES OF MULTIPLICATIVE REDUCTION

We begin our classification with the case where the curve has four K-rational places of multiplicative reduction. After applying a Möbius transformation we may suppose that ∞, 0, and 1 are among these places.

LEMMA 3.1. *If there exists an elliptic curve E over K with multiplicative reduction at the four different K-rational places ∞, 0, 1, b and good reduction elsewhere, then b must be a third root of unity; in particular K must contain the field $\mathbb{F}_4$.*

Moreover, if E is Frobenius-minimal and k, l, m, n denote the pole orders of $j(E)$ at ∞, b, 0, 1, repectively, then we must have $k+l+m+n=12$ and $k \equiv l \equiv m \equiv n \equiv \pm 1$ mod 4.

Proof. We divide the somewhat lengthy proof into three steps.

Step 1. There exists a unique $s \in \mathbb{F}_q$ with $s^2 = b$. Combining Propositions 1.3 and 2.3 we see that the j-invariant of E must be of the form

$$j(E) = \frac{(T-s)^d}{\varepsilon(T-b)^l \, T^m (T-1)^n}$$

with $\varepsilon \in \mathbb{F}_q^\times$, $d, l, m, n \in \mathbb{N}$ and $d > l+m+n$. We consider the normal form

$$Y^2 + XY = X^3 + a_2 X^2 + \frac{1}{j(E)}.$$

Making this equation integral, we see from the discriminant that d must be a multiple of 12, say $d = 12e$, for otherwise E would have bad reduction at $T-s$. Furthermore, since we assume E to be Frobenius-minimal, at least one of the numbers l, m, n must be odd.

Step 2. We examine the "untwisted" form of our curve, i.e., the one with $a_2 = 0$. Its integral model is

$$Y^2 + (T-s)^{2e} XY = X^3 + \varepsilon(T-b)^l \, T^m (T-1)^n.$$

Executing Tate's algorithm ([Ta] or [Si2]) to determine the exponent of $T-s$ in the conductor we need a shift $Y \mapsto Y + r$ with $r \in \mathbb{F}_q$ such that

$$H := r^2 + \varepsilon(T-b)^l \, T^m (T-1)^n$$

is divisible by $T-s$.

As $H \equiv \varepsilon(s^2+s)^{l-1} s^m (s+1)^n (l+m(s+1)+ns)(T-s) \, mod \, (T-s)^2$, we see that $(T-s)^2 \mid H \Leftrightarrow l \equiv m \equiv n \, mod \, 2$, because s is different from 0 and 1 and not all of l, m, n are even.

Let's assume $(T-s)^2 \mid H$ for the moment and write $l = 2\lambda + 1$, $m = 2\mu + 1$, $n = 2\nu + 1$. Then we have

$$H = \varepsilon(s^2+s)^{2\lambda} s^{2\mu}(1+s)^{2\nu} (1+s+s^2+\lambda+\mu(1+s)^2+\nu s^2)(T-s)^2$$
$$+ \varepsilon(s^2+s)^{2\lambda} s^{2\mu}(1+s)^{2\nu} (T-s)^3 + \textit{higher terms in } (T-s).$$

Hence $(T-s)^3 \mid H$ if and only if $1+s+s^2=0$ and $\lambda \equiv \mu \equiv \nu \, mod \, 2$.

Now one easily verifies that the conductor of the "untwisted" curve is

$$\infty \cdot T(T-1)(T-b)(T-s)^{12e-4} \qquad \text{if} \quad (T-s)^2 \mid H, \qquad \text{and}$$
$$\infty \cdot T(T-1)(T-b)(T-s)^{12e} \qquad \text{if} \quad (T-s)^2 \nmid H.$$

Step 3. Now we are looking for a suitable a_2 to get rid of the bad reduction at $T-s$. Let's first suppose $(T-s)^2 \nmid H$. By Theorem 1.2 the conductor of the twist a_2 must be $(T-s)^{6e}$ for otherwise we would have bad reduction at $T-s$ or additive reduction elsewhere. Thus $a_2 = \alpha_{6e-1}(T-s)^{-(6e-1)} + \cdots + \alpha_1(T-s)^{-1}$. The integral model is now

$$Y^2 + (T-s)^{3e} XY = X^3 + (\alpha_{6e-1}(T-s) + \cdots + \alpha_1(T-s)^{6e-1}) X^2$$
$$+ \varepsilon(T-s)^{6e} (T-b)^l T^m (T-1)^n.$$

Tate's algorithm reveals immediately that this curve has bad reduction at $T-s$.

Similarly, Tate's algorithm shows that $e>1$ always leads to bad reduction at $(T-s)$. Hence e must be 1 and therefore $k+l+m+n = 12e = 12$.

Finally, applying Tate's algorithm under the conditions $(T-s)^2 \mid H$ and $e=1$, we see that E can only have good reduction at $(T-s)$ if $(T-s)^3 \mid H$. As discussed in Step 2, this implies that s, and hence b, is a third root of unity and it also implies the congruence condition for k, l, m, n. ∎

THEOREM 3.2. *Elliptic curves over K with multiplicative reduction at four K-rational places and good reduction elsewhere exist if and only if $\mathbb{F}_4 \subseteq K$. There exists an $\mathbb{F}_q$-automorphism of K that maps the* 4 *rational places to $\infty, 1, s, s^2$ where s is a third root of unity.*

Over every field $K = \mathbb{F}_q(T)$ with $\mathbb{F}_4 \subseteq \mathbb{F}_q$ there are eight K-isogeny classes of elliptic curves with conductor $\infty \cdot (T-1)(T-s)(T-s^2)$. The Frobenius-minimal curves of four of these isogeny classes are listed in Table 2, *where curves in the same box belong to the same class. The other four classes are obtained by twisting with the quadratic constant field extension of K.*

TABLE 2

No.	Equation	Δ
(3333)	$Y^2+TXY+Y=X^3+T^3+1$	$(T^3+1)^3$
(9111)	$Y^2+TXY+Y=X^3$	T^3+1
(1911)	$Y^2+TXY+Y=X^3+T^2(T^3+1)$	$(T+1)^9\,(T^2+T+1)$
(1191)	$Y^2+s^2TXY+Y=X^3+sT^2(T^3+1)$	$s(T+1)(T+s)^9\,(T+s^2)$
(1119)	$Y^2+sTXY+Y=X^3+s^2T^2(T^3+1)$	$s^2(T+1)(T+s)(T+s^2)^9$
(5511)	$Y^2+TXY+Y=X^3+X^2+T$	$(T+1)^5\,(T^2+T+1)$
(1155)	$Y^2+TXY+Y=X^3+X^2+T^5+T^2+T$	$(T+1)(T^2+T+1)^5$
(5115)	$Y^2+sTXY+Y=X^3+X^2+sT$	$s(T+1)(T+s)(T+s^2)^5$
(1551)	$Y^2+sTXY+Y=X^3+X^2+s^2T^5+s^2T^2+sT$	$s^2(T+1)^5\,(T+s)^5\,(T+s^2)$
(5151)	$Y^2+s^2TXY+Y=X^3+X^2+s^2T$	$s^2(T+1)(T+s)^5\,(T+s^2)$
(1515)	$Y^2+s^2TXY+Y=X^3+X^2+sT^5+sT^2+s^2T$	$s(T+1)^5\,(T+s)(T+s^2)^5$

The number $(klmn)$ *gives the pole order of the j-invariant* (*in this case* T^{12}/Δ) *at* ∞, 1, s, *and* s^2, *respectively. All these curves have supersingular reduction at the place* 0, *but nowhere else.*

Over $\mathbb{F}_4(T)$ *we have the types of multiplicative reduction listed in Table* 3.

Proof. We can apply a Möbius transformation such that the multiplicative reduction of our curve E is located at ∞, 0, 1, and b with a suitable $b\in\mathbb{F}_q$. By the previous lemma this implies $\mathbb{F}_4\subseteq K$ and $b=s^2$. Now we translate $T\mapsto T+s$; then the conductor is $\infty\cdot(T-1)(T-s)(T-s^2)$.

Moreover, Lemma 3.1 shows that E (if Frobenius minimal) has a model

$$Y^2+XY=X^3+\alpha X^2+\frac{\varepsilon(T-1)^l\,(T-s)^m\,(T-s^2)^n}{T^{12}}$$

with $\varepsilon\in\mathbb{F}_q^\times$, $\alpha\in K$, $l+m+n<12$ and $l\equiv m\equiv n\equiv\pm 1\ mod\,4$.

The curve with $\alpha=0$ has conductor $\infty\cdot T^8(T-1)(T-s)(T-s^2)$. If we want to get rid of the bad reduction at T without creating additive reduction somewhere else, by Theorem 1.2 the conductor of the twist α must be T^4, i.e. $\alpha=\alpha_3T^{-3}+\alpha_1T^{-1}$ with $\alpha_3\in\mathbb{F}_q^\times$ and $\alpha_1\in\mathbb{F}_q$.

TABLE 3

Isogeny class	δ_∞	δ_1	δ_s	δ_{s^2}
(3333), (9111), (1911), (1191), (1119)	1	1	1	1
(5511), (1155)	1	1	-1	-1
(5115), (1551)	1	-1	-1	1
(5151), (1515)	1	-1	1	-1

Now the Tate algorithm shows that E has good reduction at T only for $\alpha_3 = 1$, $\varepsilon = s^{n-m}$ and α_1 a value depending on l, m, and n. Carrying out all the calculations one obtains the curves listed above.

The proof concerning the isogeny classes is postponed to Proposition 3.5. ∎

Remarks 3.3.

(a) The curve 1b' in table (9.3.) of [Ge1] is isomorphic over $\mathbb{F}_2(T)$ to the $\mathbb{F}_4(T)$-twist of our curve (3333).

(b) The equations of Theorem 3.2 give exactly the elliptic surfaces listed in [La1]. Note however that the equations for the surfaces (5511) and (3333) given on page 436 of [La1] contain some misprints.

Lemma 3.4. *Let E_i $(i = 1, 2)$ be elliptic curves over a finite field $\mathbb{F}_q$ with characteristic polynomials of the Frobenius $X^2 - a_i X + q = (X - \omega_i)(X - \bar{\omega}_i)$. If over some finite extension of $\mathbb{F}_q$ both curves have the same number of rational points, then*

$$\frac{\omega_1}{\omega_2} = \frac{a_1 + \sqrt{a_1^2 - 4q}}{a_2 + \sqrt{a_2^2 - 4q}} \qquad \text{or} \qquad \frac{\bar{\omega}_1}{\omega_2} = \frac{a_1 - \sqrt{a_1^2 - 4q}}{a_2 + \sqrt{a_2^2 - 4q}}$$

must be an m-th root of unity with $m \in \{1, 2, 3, 4, 6, 8, 12\}$.

Proof. If E_1 and E_2 have the same number of rational points over $\mathbb{F}_{q^m}$, then we must have $\omega_1^m = \omega_2^m$ or $\bar{\omega}_1^m = \omega_2^m$, so ω_1/ω_2 or $\bar{\omega}_1/\omega_2$ is an mth root of unity. On the other hand, $(a_1 \pm \sqrt{a_1^2 - 4q})/(a_2 + \sqrt{a_2^2 - 4q})$ is contained in the compositum of two quadratic number fields. ∎

Proposition 3.5.

(a) *The* 3-*torsion of the curve* (3333) *is K-rational. We show the* 3-*isogenies of* (3333) *in Table* 4.

TABLE 4

Kernel	Image
$\{\mathbf{0}, (T^2, sT^3 + s^2), (T^2, s^2T^3 + s)\}$	(9111)
$\{\mathbf{0}, (T + 1, 1), (T + 1, T^2 + T)\}$	(1911)
$\{\mathbf{0}, (sT + s^2, 1), (sT + s^2, sT^2 + s^2T)\}$	(1191)
$\{\mathbf{0}, (s^2T + s, 1), (s^2T + s, s^2T^2 + sT)\}$	(1119)

(b) *The point* $(1, 1)$ *is a* 5*-torsion point of the curve* (5511). *It generates the kernel of a K-rational* 5*-isogeny from* (5511) *to* (1155).

(c) *The curves* (3333), (5511), (5115), *and* (5151) *are pairwise nonisogenous over K.*

Proof.

(a) The cyclic 3-torsion groups induce K-isogenies of the curve (3333). The images must again be Tate curves at the places ∞, 1, s, and s^2, the pole order of the j-invariant being 1 or 9. By Theorem 3.2 the only curves with these properties are (9111), (1911) etc. To see which kernel corresponds to which image one looks at the behaviour under the transformation $T \mapsto sT$.

(b) is proved similarly.

(c) An isogeny between any two of these curves would by use of the map $T \mapsto sT$ imply that (5511) and (5151) are isogenous.

But over the field $\mathbb{F}_4[T]/(T^2+T+s)$ the curve (5511) has 20 rational points whereas (5151) has 10. So the characteristic polynomials of the Frobenius on these reductions are $X^2-3X+16$ and $X^2+7X+16$. Now Lemma 3.4 shows that (5511) and (5151) are not isogenous over any K. ∎

4. CURVES WITH NONRATIONAL PLACES OF MULTIPLICATIVE REDUCTION

Now we want to classify all semistable elliptic curves whose conductors have degree 4 but do not split completely into prime divisors of degree 1 over K.

We begin with the case where the conductor splits into two linear and one quadratic prime divisor.

THEOREM 4.1. *Elliptic curves over K with conductor of decomposition type* $(1, 1, 2)$ *exist only if there exisits an* $\mathbb{F}_q$*-automorphism of K that transforms the conductor into* $\infty \cdot (T-1)(T^2+T+1)$. *In particular, K cannot contain the field* $\mathbb{F}_4$.

Over every field $K = \mathbb{F}_q(T)$ *with* $\mathbb{F}_4 \not\subseteq \mathbb{F}_q$ *there exist four isogeny-classes of elliptic curves with conductor* $\infty \cdot (T-1)(T^2+T+1)$ (*see Table* 5).

Proof. Suppose E has conductor of type $(1, 1, 2)$. There exists a Möbius transformation which maps one rational place of multiplicative reduction to ∞. Then the conductor is $\infty \cdot \mathfrak{n}$, where by a translation we can achieve $\mathfrak{n} = T^3 + bT + c$. Over the quadratic constant field extension, $\mathfrak{n}$ splits into

TABLE 5

No.	Equation	δ_∞	δ_1	δ_{T^2+T+1}
1	(3333), (9111), (1911)	1	-1	1
2	$K(\mathbb{F}_4)$ – twists of no. 1	-1	1	1
3	(5511), (1155)	1	1	-1
4	$K(\mathbb{F}_4)$ – twists of no. 3	-1	-1	-1

linear factors. By the results of Section 3 this implies $b=0$. As $\mathfrak{n}$ has a root in $\mathbb{F}_q$, we may transform to $\mathfrak{n}=T^3-1=(T+1)(T^2+T+1)$.

Since T^2+T+1 has to be irreducible, K cannot contain the field $\mathbb{F}_4$. Over the quadratic constant field extension $K(\mathbb{F}_4)$, however, $\mathfrak{n}$ splits into linear factors and the reduction of E at ∞ is split multiplicative. Hence (up to Frobenius isogeny) $E/K(\mathbb{F}_4)$ must be one of the curves in the table of Theorem 3.2 and $j(E)$ must have the same pole order at s and s^2.

Remains to show that the $K(\mathbb{F}_4)$-isogenies from (3333) to (9111) and (1911) and from (5511) to (1155) are already defined over K. But this is clear from the Galois action on the 3-torsion points (resp. 5-torsion points) in Proposition 3.5. ▮

THEOREM 4.2. *Elliptic curves E over K with conductor of type* (1, 3) *exist if and only if K contains $\mathbb{F}_4$. Over every such K there are two $PGL_2(\mathbb{F}_q)$-orbits of such conductors, namely the orbits of $\infty\cdot(T^3+c)$ and $\infty\cdot(T^3+c^2)$ where c is a fixed element of $\mathbb{F}_q$ that is not a third power.*

The curves with conductor $\infty\cdot(T^3+c)$ form two isogeny classes. The first class consists (*up to Frobenius isogeny*) *of the curves listed in Table* 6; *the other class consists of their unramified quadratic twists.*

Proof. Let E be an elliptic curve over K with conductor of type (1, 3). After Möbius transformation we may assume $cond(E)=\infty\cdot(T^3+bT+c)$. Over the cubic constant field extension the polynomial (T^3+bT+c) splits into linear factors. By Theorem 3.2 this implies $b=0$. Now A contains irreducible polynomials of the form T^3+c if and only if $\mathbb{F}_4\subseteq K$.

From Theorem 3.2 we also see that over the cubic constant field extension (where we can transform T^3+c into T^3-1) the curve E must be

TABLE 6

No.	Equation	Δ	δ_∞	δ_{T^3+c}
(3333)′	$Y^2+TXY+cY=X^3+c(T^3+c)$	$c(T^3+c)^3$	1	1
(9111)′	$Y^2+TXY+cY=X^3$	$c^3(T^3+c)$	1	1

isomorphic to one of the curves listed above. By a standard Galois cohomology argument this isomorphism is already defined over K. (Note that the curves are not defined over a finite field and hence have endomorphism ring $\mathbb{Z}$ and automorphism group $\{\pm 1\}$.)

As in Proposition 3.5 the 3-torsion point $(0,0)$ generates the kernel of a rational 3-isogeny from $(9111)'$ to $(3333)'$. ▮

Lemma 4.3. *Let E be a semistable elliptic curve over K with conductor of degree* 4. *Then E has exactly one* (*rational*) *place of supersingular reduction. If this place is ∞, then the conductor of E is of the form T^4+cT+d.*

Proof. Over a big enough constant field extension L of K, the curve E has four rational places t_1, t_2, t_3, t_4 of multiplicative reduction. By the previous results E has over L exactly one place of supersingular reduction. This place is L-rational and since it is the only one, it must even be K-rational.

Now suppose this place is ∞. There exists a Möbius transformation M of L that maps t_1, t_2, t_3 to ∞, 1, s, respectively where s is a third root of unity. Theorem 3.2 then implies $M(t_4)=s^2$ and $M(\infty)=0$. Thus $z\mapsto\frac{1}{M(z)}$ is an affine transformation of L. Hence $cond(E)$ is an affine transformation of $T(T-1)(T-s)(T-s^2)=T^4+T$. Consequently $cond(E)$ is of the form T^4+cT+d. ▮

Theorem 4.4. *Elliptic curves over K with conductor of type* $(2,2)$ *exist if and only if K contains the field $\mathbb{F}_4$.*

Every such field has an $\mathbb{F}_q$-automorphism that places the supersingular reduction at ∞ and transforms the conductor into $(T^2+T+v)(T^2+T+v+1)$, where v is a fixed element of $\mathbb{F}_q-\wp(\mathbb{F}_q)$. There are 4 *isogeny classes of such curves, represented by the equations in Table* 7 *and their twists by the quadratic constant field extension of K.*

The curve $(1155)''$ *obtained from* $(5511)''$ *by* $v\mapsto v+1$ *is isogenous to* $(5511)''$ *or its unramified quadratic twist.*

Proof. If we place the supersingular reduction at ∞, then by Lemma 4.3 the conductor is of the form $(T^2+aT+e)(T^2+aT+e+a^2)$. This is easily transformed to $(T^2+T+v)(T^2+T+v+1)$. As $v\notin\wp(\mathbb{F}_q)$ and $v+1\notin\wp(\mathbb{F}_q)$, we have $1\in\wp(\mathbb{F}_q)$, which is equivalent to $\mathbb{F}_4\subseteq\mathbb{F}_q$.

TABLE 7

No.	Equation
$(3333)''$	$Y^2+XY=X^3+(T^3+(v^2+v)\,T^2)\,X^2+(T^2+T+v)^3\,(T^2+T+v+1)^3$
$(5511)''$	$Y^2+XY=X^3+(T^3+(v^2+v+1)\,T^2)\,X^2+(T^2+T+v)^5\,(T^2+T+v+1)$

Using the transformation $T \mapsto \frac{1}{T+\lambda}$ where $\lambda^2+\lambda=v$, the divisors (T^2+T+v) and $(T^2+T+v+1)$ change to $\infty \cdot (T-1)$ and (T^2+T+1), respectively. For example, from the curve $(3333)''$ we obtain the λ^3-twist of (3333) and from $(5511)''$ we obtain the $(\lambda^3+\lambda^2)$-twist of (5511).

Every elliptic curve over K with conductor $(T^2+T+v)(T^2+T+v+1)$ must be isogenous to one of these two curves over the quadratic constant field extension of $K(\lambda)$ and hence already over $K(\lambda)$. Thus we see that there exist precisely the four isogeny classes described in the theorem. ∎

LEMMA 4.5. *$\mathbb{F}_q[T]$ contains irreducible polynomials of the form T^4+cT+d if and only if $\mathbb{F}_q$ doesn't contain $\mathbb{F}_4$.*

Proof. Suppose T^4+cT+d is irreducible. We can assume that $\mathbb{F}_q$ contains a 3rd root of c. (If not we go over to the cubic extension of $\mathbb{F}_q$; the polynomial remains irreducible.) So we can transform to T^4+T+d (with a new d).

Easy calculation shows that T^4+T+d can be written as a product of two (not necessarily irreducible) quadratic polynomials if and only if this decomposition is $T^4+T+d=(T^2+aT+b)(T^2+aT+c)$ with $d=bc$, $b+c=a^2$, and $a^3=1$.

If $\mathbb{F}_4 \subseteq \mathbb{F}_q$ and $s \in \mathbb{F}_q$ is a primitive 3-rd root of unity, at least one of the elements d, sd, or $s^2d=d+sd$ must lie in $\wp(\mathbb{F}_q)$. So we can write $d=b^2+a^2b$ with $a^3=1$ and consequently T^4+T+d is not irreducible.

If $\mathbb{F}_4 \not\subseteq \mathbb{F}_q$, the criterion for T^4+T+d to split into two quadratic polynomials is that d be of the form b^2+b. There exists a d in $\mathbb{F}_q$ which is not of this form. A fortiori d is not of the form $x^4+x=(x^2+x)^2+(x^2+x)$. Hence T^4+T+d has no linear factor either. So T^4+T+d is irreducible. ∎

THEOREM 4.6. *Elliptic curves over K with conductor a prime divisor of degree 4 exist if and only if K doesn't contain the field $\mathbb{F}_4$. Every such field K has an $\mathbb{F}_q$-automorphism that places the supersingular reduction at ∞ and transforms the conductor to T^4+T+d, where d is a fixed element in $\mathbb{F}_q - \wp(\mathbb{F}_q)$.*

There are 2 isogeny classes of such curves, represented by Table 8.

TABLE 8

No.	Equation
$(3333)''$	$Y^2+XY=X^3+(T^3+dT^2)\,X^2+(T^4+T+d)^3$
$K(\mathbb{F}_4)$-twist of $(3333)''$	$Y^2+XY=X^3+(T^3+dT^2+1)\,X^2+(T^4+T+d)^3$

Proof. If E is such a curve, we see from Lemma 4.3 and 4.5 that $\mathbb{F}_4 \not\subseteq \mathbb{F}_q$. So we can transform the conductor to T^4+T+d. Over the quadratic constant field extension, E must be isomorphic to the curve $(3333)''$ of Theorem 4.4. (Note that the $K(\mathbb{F}_{16})$-twist of $(3333)''$ is not defined over K.) ▮

5. CURVES WITH MULIPLICATIVE AND ADDITIVE REDUCTION

If the conductor is of type $(1, 1^3)$ we can transform it into $\infty \cdot T^3$. More generally, elliptic curves with conductor $\infty \cdot T^n$ have been classified in [Ge3] and [Ge4]. As a special case we have

THEOREM 5.1. *Over $K=\mathbb{F}_q(T)$ there are $2(q-1)$ isogeny classes of elliptic curves with conductor $\infty \cdot T^3$. The $q-1$ different curves*

$$Y^2+TXY=X^3+\varepsilon T^5, \qquad \varepsilon \in \mathbb{F}_q^\times$$

are the Frobenius-minimal curves of the $q-1$ different isogeny classes with split multiplicative reduction at ∞. Their twists by the quadratic constant field extension give the other $q-1$ classes.

Proof. [Ge4], Theorem (6.3) and Corollary (6.4). ▮

Next we are interested in curves with conductors of type $(1, 1, 1^2)$. After Möbius transformation we may assume that the conductor is $\infty \cdot T^2(T+1)$. Combining the Propositions 1.3 and 2.3, we see that the j-invariant of such a curve must be $\frac{T^k}{\varepsilon(T+1)^l}$ with $\varepsilon \in \mathbb{F}_q^\times$ and $k>l>0$. The curve is Frobenius minimal if k or l is odd.

LEMMA 5.2. *Let $k>l>0$, not both even, and let $\varepsilon \in \mathbb{F}_q^\times$. Then the elliptic curve*

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

has conductor $\infty \cdot T^n(T+1)$ with

$$n=\begin{cases} k+2 & \textit{if} \quad 2 \nmid k, \\ k & \textit{if} \quad 2 \mid k \quad \textit{and} \quad k \neq 2, \\ 3 & \textit{if} \quad k=2. \end{cases}$$

Proof. Tate's algorithm ([Ta]). ▮

LEMMA 5.3. *Let E be an elliptic curve as in Lemma 5.2 with $4 \mid k$ and $k > 4$. Then the twisted curve*

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

has conductor

$$cond(E_\alpha) = \begin{cases} \infty \cdot T^{k-1}(T+1) & \text{if } \delta^2 = \varepsilon, \\ \infty \cdot T^k(T+1) & \text{if } \delta^2 \neq \varepsilon. \end{cases}$$

Proof. We shortly describe the case $k = 12e$; the other two cases are treated in the same way.

We start with the integral model

$$Y^2 + T^{3e}XY = X^3 + \delta T X^2 + \varepsilon T^{6e}(T+1)^l$$

with $\Delta = T^{24e}(T+1)^l$. Executing Tate's algorithm ([Ta]) in order to determine the exponent f of T in the conductor, we end up in the branch where the cubic polynomial $W^3 + a_{2,1} W^2 + a_{4,2} W + a_{6,3}$ ($\equiv W^3 + \delta W^2$) has one single and one double root modulo T. Thus $f = 24e - 4 - v$.

Running through this branch we have to make the transformations

$$\begin{aligned} Y &\mapsto Y + \sigma T^{3e} && \text{with} \quad \sigma^2 = \varepsilon \quad \text{and} \\ X &\mapsto X + \tau T^{3e} && \text{with} \quad \delta\tau^2 = \varepsilon. \end{aligned}$$

The equation is now

$$Y^2 + T^{3e}XY + \tau T^{6e} Y = X^3 + (\delta T + \tau T^{3e})\, X^2 + (\sigma + \tau^2)\, T^{6e} X + \varepsilon T^{6e+2} h(T)$$

with some $h(T) \in A$. The congruences

$$\begin{aligned} a_3 &\equiv \tau T^{6e} \; mod \; T^{6e+1}, \\ a_4 &\equiv (\sigma + \tau^2)\, T^{6e} \; mod \; T^{6e+1} \end{aligned}$$

remain valid during the subsequent transformations.

If $\sigma \neq \tau^2$ (which is easily seen to be equivalent to $\delta^2 \neq \varepsilon$), the polynomial $a_{2,1} X^2 + a_{4,6e} X + a_{6,12e-1}$ has distinct roots mod T. So in this case the algorithm ends with $v = 12e - 4$ and hence $f = 12e = k$.

If $\sigma = \tau^2$ (i.e. if $\delta^2 = \varepsilon$) the algorithm stops at the next step with $v = 12e - 3$ and $f = k - 1$, because then $Y^2 + a_{3,6e} Y - a_{6,12e}$ has distinct roots mod T. ▮

The Tate algorithm also shows that the curve

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

with $l\in\{1,3\}$ and $\varepsilon,\delta\in\mathbb{F}_q^\times$ has conductor $\infty\cdot T^n(T+1)$ where

$$n=\begin{cases}2 & \textit{if}\quad \delta^2=\varepsilon=1,\\ 3 & \textit{if}\quad \delta^2=\varepsilon\neq 1,\\ 4 & \textit{if}\quad \delta^2\neq\varepsilon.\end{cases}$$

Combining the previous results with Theorem 1.2, we know the conductors of all the twists of the curves in Lemma 5.2. In particular we obtain

THEOREM 5.4. *There are two isogeny classes of elliptic curves over K with conductor $\infty\cdot T^2(T+1)$. The class with split multiplicative reduction at ∞ contains two Frobenius-minimal curves, namely*

$$(31)\qquad Y^2+TXY=X^3+TX^2+T^2(T+1),$$

$$(13)\qquad Y^2+TXY=X^3+TX^2+T^2(T+1)^3.$$

The other class is represented by their unramified quadratic twists.

The points $\mathbf{0}$, (T,T), (T,T^2+T) form the kernel of a K-rational 3*-isogeny from* (31) *to* (13). (*Compare the proof of Proposition* 3.5.)

COROLLARY 5.5. *There are no elliptic curves over K with conductor of type* $(1^2,2)$.

Proof. Over the quadratic constant field extension such a curve would have a conductor of type $(1^2,1,1)$ and its j-invariant would have the same pole order at both places of multiplicative reduction. By Theorem 5.4 this is impossible. ▌

Remark 5.6. Replacing T by εT in Theorem 5.1 one obtains the surface VI from page 435 of [La2]. Moreover, applying the Frobenius once, twice, or three times and making the equation minimal gives the surfaces V, IV, III, respectively.

Equation (31) of Theorem 5.4 is isomorphic to the surface IX whereas its image under Frobenius is a non-minimal model of surface VIII. The curve (13) is the $K(\mathbb{F}_4)$-twist of the image of (31) under the transformation $T\mapsto\frac{T}{T+1}$.

6. CURVES WITH PURELY ADDITIVE REDUCTION

Finally we treat the remaining 3 types of conductors. The corresponding curves are essentially different from those in the preceding three sections as they will turn out to be (not necessarily quadratic) twists of constant elliptic curves. Thus the results of this section do not depend on Section 2.

THEOREM 6.1. *Elliptic curves over K with conductor of type* $(1^2, 1^2)$ *have j-invariant* 0.

More precisely, the curves with conductor $\infty^2 \cdot T^2$ are of the form

$$Y^2 + \varepsilon T^2 Y = X^3 + \lambda T^4 \qquad \textit{or}$$

$$Y^2 + \varepsilon T Y = X^3 + \lambda T^2$$

with $\varepsilon \in \mathbb{F}_q^{\times}$ and $\lambda \in \mathbb{F}_q$.

Proof. Let E be an elliptic curve over K with conductor $\infty^2 \cdot T^2$.

If E is not a twisted constant curve, $j(E)$ has a pole at ∞ or T; lets say at ∞. Consider the model

$$Y^2 + XY = X^3 + a_2 X^2 + \frac{1}{j(E)}.$$

Write $a_2 = \alpha + \widetilde{a_2}$ with $\alpha \in \mathbb{F}_q[T]$ and $\widetilde{a_2} \in \frac{1}{T}\mathbb{F}_q[[\frac{1}{T}]]$. The twisted curve

$$E_\alpha : Y^2 + XY = X^3 + \widetilde{a_2} X^2 + \frac{1}{j(E)}$$

is a Tate curve at ∞ and the quadratic twist α is unramified outside ∞. Thus E_α has conductor $\infty \cdot T^2$, which is impossible.

We could also argue that E is a quadratic twist of E_α and hence by Theorem 1.2 the exponent of ∞ in $cond(E)$ cannot be 2. For the same reason we cannot have $j(E) \in \mathbb{F}_q^{\times}$, because then E would be a quadratic twist of an elliptic curve with conductor 1.

So $j(E) = 0$ and we can find a model

$$Y^2 + a_3 Y = X^3 + a_4 X + a_6$$

as in Proposition 1.1. Thus $a_3 = \varepsilon T^e$ with $\varepsilon \in \mathbb{F}_q^{\times}$.

The Tate algorithm shows that $e \in \{1, 2\}$ is a necessary condition for T to have exponent 2 in $cond(E)$. Similarly $ord_{1/T}(T^{e-3d})$ must be 1 or 2. Hence $d = 1$ and consequently $deg(a_4) \leqslant 4$ and $deg(a_6) \leqslant 6$.

Let's say $e=2$; the case $e=1$ will then show up by mapping T to $\frac{1}{T}$. Applying the Tate algorithm for the place T we see that E has a model

$$Y^2+\varepsilon T^2 Y=X^3+(\beta T^3+\gamma T^4)\,X+\lambda T^4+\mu T^5+\nu T^6.$$

Applying the Tate algorithm for the place ∞ to this equation, we see that E even has a model

$$Y^2+\frac{\varepsilon}{T}\,Y=X^3+\frac{\lambda}{T^2},$$

which gives us the first equation of Theorem 6.1. ▮

Corollary 6.2. *There are no elliptic curves over K with conductor of type* (2^2).

Proof. Over the constant field extension $\mathbb{F}_{q^2}(T)$ such a curve would have a conductor $(T-u)^2(T-v)^2$ and the exponents of $(T-u)$ and $(T-v)$ in the discriminant would be equal. By Theorem 6.1 this is not possible. ▮

It was proved in [Ge3] that elliptic curves with conductor of type (1^n) are twisted constant. Proceeding as in the proof of Theorem 6.1 we obtain the following more explicit result for $n=4$.

Theorem 6.3. *There are two types of elliptic curves over K with conductor ∞^4:*

(a) *curves with nonzero j-invariant, given by equations*

$$Y^2+XY=X^3+\delta T X^2+\frac{1}{j}$$

with $j, \delta\in\mathbb{F}_q^{\times}$ and their unramified quadratic twists (all together $2(q-1)^2$ isomorphism classes over K),

(b) *curves with j-invariant* 0. *These are of the form*

$$Y^2+\varepsilon Y=X^3+\lambda X+\mu T+\nu$$

with $\varepsilon, \mu\in\mathbb{F}_q^{\times}$ and $\lambda, \nu\in\mathbb{F}_q$.

Remark 6.4. Over the algebraic closure of $\mathbb{F}_2$ the first equation in Theorem 6.1 is isomorphic to the surface VII on page 435 of [La2].

Mapping T to $\frac{1}{T}$ (i.e. changing the conductor to T^4) we see that the equations in Theorem 6.3 give the surface II and among the one parameter family of surfaces I those with j-invariant in $\mathbb{F}_q^{\times}$.

ACKNOWLEDGMENTS

This paper was written while I was a post-doc in Montreal; I thank Concordia University, McGill University, and CICMA for their support. I am also grateful to E.-U. Gekeler for helpful discussions and to H. Ito for pointing out an unjustified claim in the first version of this paper.

REFERENCES

[Cr] R. Crew, Etale p-covers in characteristic p, *Compositio Math.* **52** (1984), 31–45.

[Ei] M. Eichler, The basis problem for modular forms and the traces of the Hecke operators, *in* "Modular Functions of One Variable I," Lecture Notes in Mathematics, Vol. 320, pp. 75–151, Springer-Verlag, Berlin/Heidelberg/New York, 1973.

[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, On finite Drinfeld modules, *J. Algebra* **141** (1991), 187–203.

[Ge3] E.-U. Gekeler, Highly ramified pencils of elliptic curves in characteristic two, *Duke Math. J.* **89** (1997), 95–107.

[Ge4] E.-U. Gekeler, 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.), pp. 49–64, Springer-Verlag, Berlin/Heidelberg/New York, 1998.

[G&R] E.-U. Gekeler and 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. Annalen* **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.

[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.), pp. 330–343, World Scientific, Singapore, 1997.

[Sch2] A. Schweizer, Involutory elliptic curves over $\mathbb{F}_q(T)$, *J. Théor. Nombres Bordeaux* **10** (1998), 107–123.

[Sh] T. Shioda, Some remarks on elliptic curves over function fields, *Astérisque* **209** (1992), 99-114.

[Si1] J. H. Silverman, "The Arithmetic of Elliptic Curves," Graduate Texts in Mathematics, Vol. 106, Springer-Verlag, Berlin/Heidelberg/New York, 1986.

[Si2] J. H. Silverman, "Advanced Topics in the Arithmetic of Elliptic Curves," Graduate Texts in Mathematics, Vol. 151, Springer-Verlag, Berlin/Heidelberg/New York, 1994.

[Ta] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, *in* "Modular Functions of One Variable IV," Lecture Notes in Mathematics, Vol. 476, pp. 33–52, Springer-Verlag, Berlin/Heidelberg/New York, 1975.