ASIAN J. MATH.
Vol. 5, No. 4, pp. 705–720, December 2001

BIELLIPTIC DRINFELD MODULAR CURVES*

ANDREAS SCHWEIZER†

Abstract. We determine all Drinfeld modular curves $X_0(\mathfrak{n})$ that are bielliptic, i.e. double covers of elliptic curves. This allows us to find all $X_0(\mathfrak{n})$ that have infinitely many quadratic points over $\mathbb{F}_q(T)$. We also improve one of the results of Poonen concerning uniform boundedness for Drinfeld modules of rank 2.

Mathematics Subject Classification (2000): 11G09, 14H45, *secondary:* 14G05

0. Introduction. Let $\mathfrak{n} \in \mathbb{F}_q[T]$. Then the Drinfeld modular curve $X_0(\mathfrak{n})$ has infinitely many rational points over $\mathbb{F}_q(T)$ if and only if it is a rational curve, which is the case if and only if $deg(\mathfrak{n}) \leq 2$. This results from a criterion in [Sa], since the curves $X_0(\mathfrak{n})$ with positive genus are non-isotrivial and the elliptic ones have rank 0.

The question which of the curves $X_0(\mathfrak{n})$ have infinitely many quadratic points over $\mathbb{F}_q(T)$, or more generally, over a finite extension of $\mathbb{F}_q(T)$, is related in a more complicated way to the problem which $X_0(\mathfrak{n})$ are hyperelliptic or bielliptic. The hyperelliptic ones have been determined in [Sch3] and now we treat the bielliptic case.

In the classical situation (i.e. over $\mathbb{C}$ or $\mathbb{Q}$) all bielliptic modular curves $X_0(n)$ have been determined in [Ba]. In order to reduce the possibly bielliptic modular curves to a finite number one uses a strategy originally due to A. Ogg, namely counting points on a suitable reduction. This works equally well in the classical and in the Drinfeld setting. However, when dealing with the remaining cases, life is harder for us, since, unlike the classical situation, not much is known about the full automorphism group of $X_0(\mathfrak{n})$. Therefore we have to use several different strategies and ad hoc arguments.

The first main result (Theorem 4.6) is that up to affine tranformations of $\mathfrak{n}$ there are exactly 12 bielliptic curves $X_0(\mathfrak{n})$ (of which 6 are at the same time hyperelliptic). All bielliptic involutions we find are modular automorphisms (and often even Atkin-Lehner involutions). However, we do not claim that these 12 curves have no other bielliptic involutions, although this seems unlikely.

Section 5 contains the other main results: Theorem 5.1 relates the two properties, to have infinitely many quadratic points and being bielliptic. Theorem 5.3 lists all $X_0(\mathfrak{n})$ with infinitely many quadratic points over $\mathbb{F}_q(T)$. As an application we improve a result from [Po] on the uniform boundedness of the $\mathfrak{p}$-primary torsion of $\mathbb{F}_q[T]$-Drinfeld modules of rank 2 over a fixed finite extension L of $\mathbb{F}_q(T)$; namely, in Theorem 5.4 we make the bound uniform over all quadratic extensions of L. See also Remark 5.5, where further possible generalizations are indicated.

1. Basic Facts. As always, $\mathbb{F}_q$ is the finite field with q elements. Throughout this paper K stands for the rational function field $\mathbb{F}_q(T)$ and A for the polynomial ring $\mathbb{F}_q[T]$, where sometimes q is specified in the context. The monic irreducible elements of A are called primes and denoted by the letter $\mathfrak{p}$. We refer to the corresponding places of K as finite places and use the symbol ∞ for the place with uniformizer $\frac{1}{T}$.

For every non-zero $\mathfrak{n} \in A$ we have the Drinfeld modular curve $X_0(\mathfrak{n})$. Here we are interested in these curves as algebraic curves over K. We refer to [Sch3] for a

*Received December 21, 2000; accepted for publication March 2, 2001.

†Korea Institute for Advanced Study (KIAS), 207-43 Cheongryangri-dong, Dongdaemun-gu, Seoul 130-012, Korea (schweiz@kias.re.kr).

short account of the (well-known) facts that are important for us, including Gekeler's closed formula for the genus. Or see [G&R] for a really thorough treatment of Drinfeld modular curves in general.

If X is a curve defined over a field k, then $Aut(X)$ means $Aut_{\overline{k}}(X)$, i.e. the group of automorphisms defined over the algebraic closure $\overline{k}$ of k.

Definition 1.1. *Let k be a field and X/k a curve. We say that X is* **bielliptic** *over k if the genus of X over k is at least 2 and X is a double cover over k of an elliptic curve E.*

Insisting that the genus is at least 2 has the advantage that even in characteristic 2 the covering $X \to E$ is galois, that is, there exists an involution v of X, defined over k, such that $v\backslash X = E$. We say that v is a **bielliptic involution** *of X.*

We mainly apply this to the curves $X_0(\mathfrak{n})$. By [Sch3], Proposition 5 these are conservative, i.e., we don't have to worry about such strange phenomena as change of the genus upon inseparable extension of the ground field. So $X_0(\mathfrak{n})$ is bielliptic over the algebraic closure of K if and only if it is bielliptic over some finite extension of K. In this case we simply say that $X_0(\mathfrak{n})$ is bielliptic.

Moreover, the curves $X_0(\mathfrak{n})$, and hence also their quotients, always have a K-rational point. Thus an involution w of $X_0(\mathfrak{n})$ is bielliptic if the genus of $w\backslash X_0(\mathfrak{n})$ is 1.

If the characteristic of K is 2, the ramification of the covering $X_0(\mathfrak{n}) \to w\backslash X_0(\mathfrak{n})$ is of course wild. But by [Sch3], Proposition 7 (which I owe to E.-U. Gekeler) the second ramification groups are trivial. Loosely spoken: In characteristic 2 the fixed points of an involution on $X_0(\mathfrak{n})$ count double. Thus in characteristic 2 an involution w of $X_0(\mathfrak{n})$ is bielliptic if and only if it has exactly $g(X_0(\mathfrak{n}))-1$ fixed points.

In general, the only involutions of $X_0(\mathfrak{n})$ we know are the Atkin-Lehner involutions $W_{\mathfrak{m}}$. We refrain from presenting the somewhat involved formulas for their fixed points, proved in [Sch3] and repeated in [Sch4]. Actually, the bielliptic Atkin-Lehner involutions can be easily read off from the main results in [Sch4].

If $q > 2$ the Atkin-Lehner involutions exhaust already all so-called modular automorphisms of $X_0(\mathfrak{n})$, that is the automorphisms induced by automorphisms of the Drinfeld upper half-plane.

For $q = 2$ there might be more; for example if $T^2|\mathfrak{n}$, then $\Gamma_0(\mathfrak{n})$ is normal in $\Gamma_0(\frac{\mathfrak{n}}{T})$ and the matrix $\left(\begin{smallmatrix} 1 & 0 \\ \frac{\mathfrak{n}}{T} & 1 \end{smallmatrix}\right)$ induces on $X_0(\mathfrak{n})$ a modular involution which we called U_1 in [Sch2]. Clearly, $U_1\backslash X_0(\mathfrak{n})$ is nothing else than $X_0(\frac{\mathfrak{n}}{T})$. Note however that U_1 does not commute with all Atkin-Lehner involutions of $X_0(\mathfrak{n})$. See [Sch2] for a complete description of all modular automorphisms of $X_0(\mathfrak{n})$.

Although it is unlikely that a Drinfeld modular curve $X_0(\mathfrak{n})$ of genus at least 2 has any non-modular automorphisms, this doesn't seem to be proved for one single case. This is the reason for the circumstantial argumentation in section 4.

Examples show that a curve can have more than one bielliptic involution. But the next result makes clear that this can only happen if the genus is small.

Proposition 1.2. *Let X be a curve of genus $g(X) \geq 6$ over an algebraically closed field k.*

a) If X is bielliptic, then the bielliptic involution is unique and lies in the center of the automorphism group of X.

b) Let w be an involution of X which, if $char(k) \neq 2$, has more than 8 fixed points (resp. more than 4 fixed points if $char(k) = 2$). Then either w is the bielliptic involution or X is not bielliptic.

Proof. a) For later use we present the presumably well-known proof. Let u and v be two bielliptic involutions of X. They generate a dihedral group G with $2n$ elements where n is the order of uv in $Aut(X)$. Every element of G outside the cyclic subgroup $\langle uv \rangle$ is conjugate to u or v and hence bielliptic. The contribution of the ramification of a bielliptic involution w to the Hurwitz formula for $X \to w\backslash X$ is $g-1$. Thus the Hurwitz formula for $X \to G\backslash X$ yields $g-1 \geq 2n(0-1)+n(g-1)$, that is $n \leq \frac{g-1}{g-3} < 2$, which means $u = v$.

If σ is any automorphism of X, then $\sigma v \sigma^{-1}$ is again bielliptic, hence equal to v; so v commutes with σ.

b) Suppose X has a bielliptic involution $v \neq w$. Since w commutes with v, it induces an involution $\widetilde{w}$ on the elliptic curve $v\backslash X$. But $\widetilde{w}$ has more than 4 fixed points (resp. more than 2 if the characteristic is 2). This contradicts the Hurwitz formula. □

One of the best strategies if one wants to prove that a certain Drinfeld modular curve $X_0(\mathfrak{n})$ is not bielliptic is to work with a reduction. Namely, one uses the fact that for every place $\mathfrak{p}$ of K with $\mathfrak{p} \not| \infty \cdot \mathfrak{n}$ the curve $X_0(\mathfrak{n})$ has good reduction modulo $\mathfrak{p}$ and the reduced curve has the same moduli interpretation for Drinfeld modules over extensions of $A/\mathfrak{p}$.

Also, if $X_0(\mathfrak{n})$ is bielliptic, then the elliptic curve $v\backslash X_0(\mathfrak{n})$ must somehow show up in the Jacobian $J_0(\mathfrak{n})$ of $X_0(\mathfrak{n})$. We refer to [G&R] for more information on $J_0(\mathfrak{n})$ and on strong Weil curves.

Lemma 1.3. *If $X_0(\mathfrak{n})$ is bielliptic and $g(X_0(\mathfrak{n})) \geq 6$, then the bielliptic involution is defined over a finite, purely inseparable extension L of K.*

For every place $\mathfrak{p}$ of K with $\mathfrak{p} \not| \infty \cdot \mathfrak{n}$ the reduction $\widetilde{X_0(\mathfrak{n})}$ of $X_0(\mathfrak{n})$ mod $\mathfrak{p}$ is also a bielliptic curve. More precisely, if $\wp$ is the place of L lying above $\mathfrak{p}$, then the bielliptic involution v reduces to a bielliptic involution $\widetilde{v}$, defined over $A/\mathfrak{p}$, and $\widetilde{v}\backslash\widetilde{X_0(\mathfrak{n})}$ is nothing else than the reduction mod $\wp$ of the elliptic curve $v\backslash X_0(\mathfrak{n})$.

Proof. Since v is unique, it is stable under every $\sigma \in Aut(\overline{K}/K)$ and hence defined over a purely inseparable extension of K.

Taking a K-rational canonical map i from $X_0(\mathfrak{n})$ into its Jacobian $J_0(\mathfrak{n})$ we can find a map $f : J_0(\mathfrak{n}) \to v\backslash X_0(\mathfrak{n})$ such that $f \circ i$ is the map from $X_0(\mathfrak{n})$ to $v\backslash X_0(\mathfrak{n})$. Then the lemma follows because i and f behave well under the reduction. □

2. The Hyperelliptic Cases. If $deg(\mathfrak{n}) \leq 2$, then $X_0(\mathfrak{n})$ is rational and thus certainly not bielliptic. In this section we settle the case $deg(\mathfrak{n}) = 3$.

Lemma 2.1. *Let X be a hyperelliptic curve over an algebraically closed field k. If X is also bielliptic, then $g(X) \leq 3$.*

Proof. The hyperelliptic involution u commutes with every automorphism, in particular with the bielliptic involution v. Applying the Hurwitz formula to the Galois cover $X \to \langle u, v\rangle\backslash X$ yields $g-1 \geq (g+1)+(g-1)-4$. □

Corollary 2.2. *If $X_0(\mathfrak{n})$ is bielliptic and $deg(\mathfrak{n}) = 3$, then necessarily $q \leq 4$.*

Proof. If $deg(\mathfrak{n}) = 3$, then $X_0(\mathfrak{n})$ is hyperelliptic (or elliptic) and its genus is q or $q-1$, depending on whether $\mathfrak{n}$ is square-free or not. □

Lemma 2.3. *The curves $X_0(T^3)$ are not bielliptic.*

Proof. If $q = 2$, then $X_0(T^3)$ is elliptic and hence excluded by definition. So we need to examine only $q = 3$ and $q = 4$.

If $q = 4$, then according to [Ge3, Corollary 6.4] the Jacobian $J_0(T^3)$ of $X_0(T^3)$ is, up to isogeny, the product of the three elliptic curves

$$Y^2 + XY = X^3 + \frac{\varepsilon}{T}, \quad \varepsilon \in \mathbb{F}_4^\times.$$

These curves are non-isogenous even over the algebraic closure of K. To verify this we first observe that, given two of these curves, we can find an $\alpha \in \mathbb{F}_4^\times$ such that the characteristic polynomials of the Frobenius over $\mathbb{F}_4$ on their reductions mod $T - \alpha$ are $X^2 + 3X + 4$ and $X^2 - X + 4$, respectively. If those reductions become isogenous over some $\mathbb{F}_{4^n}$, then the n-th powers of the roots of these polynomials must be equal, i.e.,

$$\frac{-3 + \sqrt{-7}}{1 + \sqrt{-15}} \quad \text{or} \quad \frac{-3 - \sqrt{-7}}{1 + \sqrt{-15}} \in \mathbb{Q}(\sqrt{-7}, \sqrt{-15})$$

must be an n-th root of unity. But one easily checks that this is not the case.

Now suppose $X_0(T^3)$ has a bielliptic involution v, defined over some finite extension L of K. Then $v\backslash X_0(T^3)$ must lie in one of the three isogeny factors of $J_0(T^3)$ over L with corresponding strong Weil curve E over K. (See the end of Remark 4.7 for a contrast). This implies that there is an elliptic curve $\widetilde{E}$ over L, such that over L the strong Weil uniformization $X_0(T^3) \to E$ and the map $X_0(T^3) \to v\backslash X_0(T^3)$ both factor through $\widetilde{E}$. Obviously only $\widetilde{E} = v\backslash X_0(T^3)$ is possible.

Using the data in Table 10.2 of [Ge1] one can calculate (see [Ge2], Theorems 8.9 and 8.10 and Example 9.1) that the degree of the strong Weil uniformization $X_0(T^3) \to E$ is 4 and the pole order of $j(E)$ at ∞ is also 4. In view of the results in [Ge3] we now even know the equation of E, namely:

$$Y^2 + XY = X^3 + \frac{\varepsilon}{T^4}.$$

From this and the 2-isogeny from E to $\widetilde{E}$ we see that $\widetilde{E}$ is defined over K. But this contradicts the fact that E is a strong Weil curve, and hence $X_0(T^3)$ cannot be bielliptic.

The same proof works for $q = 3$. Here the Jacobian splits into the two elliptic curves $Y^2 = X^3 + X^2 \pm \frac{1}{T}$ ([Ge3], Corollary 6.4), which again are absolutely non-isogenous. The degree of the strong Weil uniformizations is 3. Note that there is a misprint in table 10.2 of [Ge1]; the second vector for $q = 3$, $\mathfrak{n} = T^3$ should be $(0, -1, 2, -1)$. □

PROPOSITION 2.4. *Up to affine transformations $T \mapsto \alpha T + \beta$ the following table lists all hyperelliptic curves $X_0(\mathfrak{n})$ with $g(X_0(\mathfrak{n})) \leq 3$. Moreover, all bielliptic Atkin-Lehner involutions of these curves are given. So if there exist bielliptic involutions other than those in the table, they cannot be modular.*

q	$\mathfrak{n}$	g	*bielliptic*	*some bielliptic involutions*
2	$T(T^2+T+1)$	2	*yes*	W_T, W_{T^2+T+1}
2	T^3+T+1	2	*no*	–
2	$(T^2+T+1)^2$	2	*no*	–
3	T^3	2	*no*	–
3	$T^2(T-1)$	2	*yes*	W_{T^2}, W_{T-1}
3	$T(T-1)(T+1)$	3	*yes*	$W_{T(T-1)}$, $W_{T(T+1)}$, $W_{(T-1)(T+1)}$
3	$T(T^2+1)$	3	*yes*	W_T
3	$T(T^2+T-1)$	3	*yes*	W_{T^2+T-1}
3	T^3-T+1	3	*no*	–
3	T^3+T^2-1	3	*no*	–
4	T^3	3	*no*	–
4	$T^2(T-1)$	3	*yes*	W_{T^2}

Proof. The cases with a bielliptic Atkin-Lehner involution were already determined in Proposition 3.1 of [Sch4].

According to Table 10.2 in [Gel], for the three irreducible $\mathfrak{n}$ listed above the Jacobian $J_0(\mathfrak{n})$ of $X_0(\mathfrak{n})$ is simple over K. But by [Ta, Appendix] for irreducible $\mathfrak{n}$ the decomposition up to isogeny of $J_0(\mathfrak{n})$ into simple abelian varieties over K is already the absolute decomposition (i.e. over $\overline{K}$). Hence these three curves cannot be bielliptic.

The curves $X_0(T^3)$ have been treated in the previous lemma.

Finally, if $q=2$ and $\mathfrak{n}=(T^2+T+1)^2$, then $W_\mathfrak{n}$ has 3 fixed points on $X_0(\mathfrak{n})$ and hence it is the hyperelliptic involution. These fixed points are cusps and they are F-rational points of $X_0(\mathfrak{n})$ where F is a certain cubic Galois extension of K. (See [Sch3] for all this). The group $Aut(X_0(\mathfrak{n}))/W_\mathfrak{n}$ is a subgroup of S_3, given by the permutation representation of these automorphisms on the three fixed points of $W_\mathfrak{n}$.

If $Aut(X_0(\mathfrak{n}))$ contains an involution $v \neq W_\mathfrak{n}$, then v, fixing one of the fixed points of $W_\mathfrak{n}$, is bielliptic. Applying $\sigma \in Aut(\overline{F}/F)$ to v we obtain an involution with the same fixed point; so it can only be v or $vW_\mathfrak{n}$. This shows that the elliptic curve $v\backslash X_0(\mathfrak{n})$ is defined over a finite, purely inseparable extension of a quadratic extension of F. In particular, the existence of v would imply that the Jacobian of $X_0(\mathfrak{n})$ *mod* T splits over $\mathbb{F}_{2^6}$ into two elliptic curves.

Using the quotient graph of the Bruhat-Tits tree by the congruence group $\Gamma_0(\mathfrak{n})$ (compare the examples at the end of [G&R] or [Ge2]), one can calculate that the eigenvalues of the Hecke operator $\mathcal{H}_T$ on $J_0(\mathfrak{n})$ are $\frac{1+\sqrt{5}}{2}$ and $\frac{1-\sqrt{5}}{2}$. So the L-polynomial of the curve $X_0(\mathfrak{n})$ *mod* T over $\mathbb{F}_2$ is

$$(1-\frac{1+\sqrt{5}}{2}X+2X^2)(1-\frac{1-\sqrt{5}}{2}X+2X^2).$$

From this one easily calculates the L-polynomial of the same curve over $\mathbb{F}_{2^6}$, namely

$$1-10X+73X^2-640X^3+4096X^4.$$

This polynomial is irreducible (check modulo 3). Ergo $J_0(\mathfrak{n})$ *mod* T doesn't split over $\mathbb{F}_{2^6}$ and hence v doesn't exist. □

3. Bounding q and $deg(\mathfrak{n})$. In this section we restrict the possible q and $\mathfrak{n}$ with bielliptic $X_0(\mathfrak{n})$ to a finite set by using "Ogg's trick", which consists in combining the following two facts.

On the one hand, if $\mathfrak{p} \in A$ is a prime with $\mathfrak{p} \not| \mathfrak{n}$, one can use the moduli interpretation to show that the reduction of $X_0(\mathfrak{n})$ modulo $\mathfrak{p}$ has many points which are rational over the quadratic extension of $A/\mathfrak{p}$. On the other hand, if $X_0(\mathfrak{n})$ is bielliptic and $g(X_0(\mathfrak{n})) \geq 6$, then $X_0(\mathfrak{n})$ *mod* $\mathfrak{p}$ as a double cover of an elliptic curve over $A/\mathfrak{p}$ (see Lemma 1.3) has at most $2(q^{deg(\mathfrak{p})}+1)^2$ rational points over $\mathbb{F}_{q^{2deg(\mathfrak{p})}}$.

So first we have to make sure in how far we can apply Lemma 1.3.

LEMMA 3.1. *Let $deg(\mathfrak{n}) > 3$ and $g(X_0(\mathfrak{n})) < 6$. Then necessarily $q = 2$ and $deg(\mathfrak{n}) = 4$.*

Proof. If $\mathfrak{n}$ is irreducible or of degree 4 we can apply the explicit formulas 2.19 and 2.21 in [G&N]. If $\mathfrak{m}$ is a proper divisor of $\mathfrak{n}$, then the Hurwitz formula for the covering $X_0(\mathfrak{n}) \to X_0(\mathfrak{m})$ yields $4 \geq g(X_0(\mathfrak{n})) - 1 \geq q(g(X_0(\mathfrak{m})) - 1)$. After some annoying case distinctions we arrive at the claimed result. □

LEMMA 3.2. *Let $deg(\mathfrak{n}) = d > 3$ and suppose that $X_0(\mathfrak{n})$ is bielliptic. Then necessarily $q = 2$ and $d \leq 5$ or $q = 3$ and $d = 4$.*

Proof.

Step 1. First suppose that there is an $\alpha \in \mathbb{F}_q$ with $(T-\alpha) \not| \mathfrak{n}$. Let ϕ be the Drinfeld module over $A/(T-\alpha)$ given by $\phi_T = \tau^2 + \alpha$. Then ϕ has $\varepsilon(\mathfrak{n})$ cyclic $\mathfrak{n}$-isogenies, where

$$\varepsilon(\mathfrak{n}) = q^{deg(\mathfrak{n})} \prod_{\mathfrak{p}|\mathfrak{n}} (1 + q^{-deg(\mathfrak{p})}).$$

Each of these isogenies is stable under $\phi_{T-\alpha} = \tau^2$, which is the Frobenius of $\mathbb{F}_{q^2}$. This means that the isogeny is $\mathbb{F}_{q^2}$-rational. Still $Aut(\phi) = \mathbb{F}_{q^2}^\times$ acts on these isogenies with orbits of length $q+1$ or 1. Thus we obtain at least $\frac{\varepsilon(\mathfrak{n})}{q+1}$ $\mathbb{F}_{q^2}$-rational points on $X_0(\mathfrak{n})$ *mod* $(T-\alpha)$. (Compare the proof of Lemma 18 in [Sch3] for all this.) Also, $X_0(\mathfrak{n})$ has at least 2^s rational cusps where s is the number of different prime divisors of $\mathfrak{n}$. As explained above, the reduction of $X_0(\mathfrak{n})$ modulo $(T-\alpha)$ has at most $2(q+1)^2$ rational points over the quadratic extension $\mathbb{F}_{q^2}$ of $A/(T-\alpha)$. All in all we have

$$2^s + \frac{\varepsilon(\mathfrak{n})}{q+1} \leq 2(q+1)^2.$$

We use this to estimate $q^d < \varepsilon(\mathfrak{n}) < 2(q+1)^3 \leq 2(\frac{3}{2}q)^3 < 7q^3$. Consequently $d \leq 5$, and for $q \geq 3$ even $d \leq 4$. For $q \geq 4$ we can improve the above estimate to $q^d < 2(q+1)^3 \leq 2(\frac{5}{4}q)^3 < 4q^3$ and then $d \leq 3$.

Step 2. Next suppose that $(T^q - T)|\mathfrak{n}$, but there is a place $\mathfrak{p}$ of degree 2 with $\mathfrak{p} \not| \mathfrak{n}$. Using the supersingular Drinfeld module over $A/\mathfrak{p}$ we obtain as above $2^s + \varepsilon(\mathfrak{n}) \leq 2(q^2+1)^2$. (Compare the proof of Lemma 18 in [Sch3].) We conclude

$$q^d < \varepsilon(\mathfrak{n}) \leq 2q^2(q^2+2) \leq 2q^2\frac{3}{2}q^2 = 3q^4.$$

So we see that $d \leq 5$, and actually $d = 5$ is only possible for $q = 2$. Moreover, $d = 4$ implies $q \leq 4$ (because of $(T^q - T)|\mathfrak{n}$), and $q = 4$ leads to the contradiction $2^4 + 5^4 \leq 2 \cdot 17^2$.

Step 3. Now suppose that $(T^{q^2} - T)|\mathfrak{n}$, but there is a place $\mathfrak{p}$ of degree 3 with $\mathfrak{p} \not| \mathfrak{n}$. According to Proposition 16 of [Sch1], for every prime $\mathfrak{p}$ of odd degree $e \geq 3$ there are at least $q + 1$ non-isomorphic supersingular Drinfeld modules over $A/\mathfrak{p}$. If ϕ is such a Drinfeld module, then $\phi_\mathfrak{p} = \alpha\tau^{2e}$ and one easily verifies $\alpha \in \mathbb{F}_q^\times$. Hence, as in step 1, the $\varepsilon(\mathfrak{n})$ cyclic $\mathfrak{n}$-isogenies of ϕ are rational over the quadratic extension of $A/\mathfrak{p}$. Counting rational points on $X_0(\mathfrak{n})$ *mod* $\mathfrak{p}$ over this extension yields

$$2^s + (q + \frac{1}{q+1})\varepsilon(\mathfrak{n}) \leq 2(q^e + 1)^2.$$

Since under our assumptions $e = 3$ and $\varepsilon(\mathfrak{n}) \geq q^{q^2}$, we easily obtain $q^{q^2+1} < q^9$, that is $q^2 + 1 < 9$, which implies $q = 2$. Doing the calculation for $q = 2$ more precisely, we see that only $\mathfrak{n} = T(T+1)(T^2+T+1)$ is possible.

Step 4. Now we show that this potentially infinite line of argument actually terminates.

Suppose $(T^{q^2} - T)|\mathfrak{n}$ and $(T^{q^3} - T)|\mathfrak{n}$. Let r be the biggest odd number such that $\mathfrak{n}$ is divisible by all primes of odd degree not greater than r. Then there exists a prime $\mathfrak{p}$ of degree $r + 2$ with $\mathfrak{p} \not| \mathfrak{n}$. Taking the $q + 1$ supersingular Drinfeld modules over $A/\mathfrak{p}$ mentioned in step 3, we obtain $q^{q^r+1} < q^{2r+7}$ or $q^r < 2r + 6$. This is only possible for $r = 3$ and $q = 2$. Redoing the calculation more precisely with these values yields a contradiction.

So only the steps 1 to 3 occur for bielliptic $X_0(\mathfrak{n})$. □

PROPOSITION 3.3. *Up to affine transformations there is only one bielliptic curve $X_0(\mathfrak{n})$ with deg$(\mathfrak{n}) \geq 5$, namely:*

q	$\mathfrak{n}$	g	*bielliptic*	*bielliptic involution*
2	$T^5 + T^3 + 1$	10	*yes*	$W_{T^5+T^3+1}$

Proof. If $\mathfrak{n}$ is square-free, then $W_\mathfrak{n}$ has at least 5 fixed points. So by Proposition 1.2.b) the curve $X_0(\mathfrak{n})$ is bielliptic if and only if $X_+(\mathfrak{n})$ is elliptic. According to Proposition 4.5 in [Sch4] the only such case, up to translation, is $\mathfrak{n} = T^5 + T^3 + 1$.

The case $\mathfrak{n} = T^2(T+1)(T^2+T+1)$ was excluded in step 3 of the proof of the previous lemma. The other cases with a multiple factor can be ruled out by doing the calculations in the steps 1 and 2 of that proof with the precise value of $\varepsilon(\mathfrak{n})$. (For $\mathfrak{n} = T^5$ one also needs that $X_0(T^5)$ has 4 rational cusps). □

In order to deal with the remaining cases $q \in \{2, 3\}$, *deg*$(\mathfrak{n}) = 4$ we have to refine the method a little bit. We postpone this to the next section.

En passant we note that the results on $X_0(\mathfrak{n})$ can also be used to restrict the values for which the Drinfeld modular curves $X_1^*(\mathfrak{n})$, $X_1(\mathfrak{n})$ or $X(\mathfrak{n})$ might be bielliptic.

LEMMA 3.4.*Let deg$(\mathfrak{n}) \geq 4$ and suppose that $X_1^*(\mathfrak{n})$ (or $X_1(\mathfrak{n})$ or $X(\mathfrak{n})$) is bielliptic. Then $X_0(\mathfrak{n})$ must be bielliptic or hyperelliptic.*

Proof. Let X be one of $X_1^*(\mathfrak{n})$, $X_1(\mathfrak{n})$, $X(\mathfrak{n})$. There exists a group G of (modular) automorphisms of X such that $G\backslash X = X_0(\mathfrak{n})$.

Now suppose that $deg(\mathfrak{n}) \geq 4$ and that X has a bielliptic involution v. Then v is not contained in G, since $g(X_0(\mathfrak{n})) \geq 2$ for $deg(\mathfrak{n}) \geq 4$. Using our Lemma 3.1 and the explicit formula for the genus of $X_1^*(\mathfrak{n})$ (Corollary 5.3 in [G&N]) one sees that $g(X) \geq 6$. So v commutes with G and thus induces an involution on $X_0(\mathfrak{n})$ with elliptic or rational quotient. □

4. The Remaining Cases. In this section we complete our discussion by showing that there are no bielliptic $X_0(\mathfrak{n})$ with $q = 3$, $deg(\mathfrak{n}) = 4$ and determining the ones with $q = 2$, $deg(\mathfrak{n}) = 4$.

If $q = 3$ and $deg(\mathfrak{n}) = 4$, then the reduction method from Lemma 3.2 in many cases falls short of proving that $X_0(\mathfrak{n})$ is not bielliptic. The main crux is, of course, that $(q+1)^2$ is the general upper bound for the number of rational points on an elliptic curve over $\mathbb{F}_{q^2}$. If we knew for example that the curve is ordinary, we could already lower this bound by 1. Therefore, in this section we will repeatedly apply the following version of the key lemma 2.4 in [Sch5].

LEMMA 4.1. *Let k be a perfect field of characteristic* 3 *and let E be an elliptic curve over $k(T)$ with $j(E) \notin k$. Suppose that $j(E)$ is not a* 3*-rd power in $k(T)$. Put*

$$G(T) = \prod \mathfrak{p}_i^{r_i}$$

where the product is over all finite places $\mathfrak{p}_i$ of bad reduction of E and

$$0 \leq r_i \leq 2 \quad with \quad r_i \equiv -ord_{\mathfrak{p}_i}(j(E)) \ mod\ 3.$$

If $\mathfrak{p}$ is a finite place of supersingular reduction of E, then $ord_{\mathfrak{p}}(j(E)) = 6e$ for some $e > 0$ with

$$\mathfrak{p}^{2e-1} | G'(T).$$

The condition that $j(E)$ is not a third power guarantees that not all r_i are 0. It doesn't really restrict the applicability of the lemma, since in every Frobenius isogeny class there is one such curve.

Recall from Lemma 1.3 that if v is the unique bielliptic involution of $X_0(\mathfrak{n})$, then v is defined over a finite, purely inseparable extension L of K. Applying a suitable power of the Frobenius to the elliptic curve $v\backslash X_0(\mathfrak{n})$ we obtain an elliptic curve E over K. It is well known that E, being an isogeny factor of $J_0(\mathfrak{n})$ over K, has split multiplicative reduction at ∞ and conductor $\infty \cdot \mathfrak{m}$ for some $\mathfrak{m} \in A$ with $\mathfrak{m}|\mathfrak{n}$ and $deg(\mathfrak{m}) \geq 3$. If $\mathfrak{p}$ is a place of K with $\mathfrak{p} \not| \infty \cdot \mathfrak{m}$ and $\wp$ is the place of L lying above $\mathfrak{p}$, then $v\backslash X_0(\mathfrak{n})$ *mod* $\wp$ and E *mod* $\mathfrak{p}$ have the same number of rational points over any finite extension of $A/\mathfrak{p}$.

LEMMA 4.2. *If $q = 3$ and $\mathfrak{n}$ is irreducible of degree* 4, *then $X_0(\mathfrak{n})$ is not bielliptic.*

Proof. After an affine transformation we may assume that $\mathfrak{n}$ is one of the polynomials $T^4 - T^2 - 1$, $T^4 + T^2 + T + 1$, $T^4 - T - 1$, $T^4 + T^2 - 1$.

If $\mathfrak{n} = T^4 - T^2 - 1$, then $W_{\mathfrak{n}}$ has 12 fixed points on $X_0(\mathfrak{n})$. As $g(X_0(\mathfrak{n})) = 9$, we see from Proposition 1.2.b) that $X_0(T^4 - T^2 - 1)$ is not bielliptic. Unfortunately this method doesn't work in the three other cases.

To prove that $X_0(\mathfrak{n})$ is not bielliptic in the next two cases we claim that for these $\mathfrak{n}$ there are no elliptic curves E over $\mathbb{F}_3(T)$ with conductor $\infty \cdot \mathfrak{n}$: We use Lemma 4.1

to find the possible supersingular places of E, that is, the possible zeroes of $j(E)$ that are places of good reduction. There are only two possible choices for $G(T)$, namely $\mathfrak{n}$ and $\mathfrak{n}^2$.

If $\mathfrak{n} = T^4 + T^2 + T + 1$, we have $G'(T) = T^3 - T + 1$ or $G'(T) = -(T^3 - T + 1)\mathfrak{n}$. Thus only $j(E) = \frac{\pm(T^3-T+1)^6}{(T^4+T^2+T+1)^l}$ with $l \in \{1, 2, 3\}$ is possible. But

$$Y^2 = X^3 + X^2 - \frac{\pm(T^4 + T^2 + T + 1)^l}{(T^3 - T + 1)^6}$$

has additive reduction at $T^3 - T + 1$, and every twist of this curve will also have additive reduction at some place. (See [Ge3] or [Sch5] on how twisting effects the reduction.)

If $\mathfrak{n} = T^4 - T - 1$, we have $G'(T) = (T-1)^3$ or $-(T-1)^3\mathfrak{n}$, hence $j(E) = \frac{\pm(T-1)^{6e}}{(T^4-T-1)^l}$ with $e \in \{1, 2\}$ and $4l < 6e$. But, just as above, $e = 1$ is not possible. Using the Tate algorithm we see that the curve

$$Y^2 = X^3 + X^2 - \frac{\pm(T^4 - T - 1)^l}{(T - 1)^{12}}$$

with $l \in \{1, 2\}$ also has bad reduction at $T - 1$. Therefore no E with conductor $\infty \cdot (T^4 - T - 1)$ exists.

Finally, if $\mathfrak{n} = T^4 + T^2 - 1$, we have $G'(T) = T(T-1)(T+1)$ or $-T(T-1)(T+1)\mathfrak{n}$. If for example $j(E) = \frac{\pm T^6(T-1)^6}{(T^4+T^2-1)^l}$, then, in order to avoid additive reduction, the equation can only be

$$Y^2 = X^3 + T(T - 1)X^2 - \frac{\pm(T^4 + T^2 - 1)^l}{T^3(T - 1)^3}.$$

Applying the Tate algorithm to check the reduction at T and $T - 1$ (or $T + 1$) and make the model minimal over $\mathbb{F}_3[T]$, we end up with the following three curves

$$\begin{aligned}
Y^2 &= X^3 + (T^2 - T)X^2 + (T + 1)X + 1, & j &= \tfrac{T^6(T-1)^6}{T^4+T^2-1},\\
Y^2 &= X^3 + (T^2 + T)X^2 - (T - 1)X + 1, & j &= \tfrac{T^6(T+1)^6}{T^4+T^2-1},\\
Y^2 &= X^3 + (T^2 - 1)X^2 - X, & j &= \tfrac{(T-1)^6(T+1)^6}{T^4+T^2-1}.
\end{aligned}$$

Now if v is the bielliptic involution of $X_0(\mathfrak{n})$, then $v\backslash X_0(\mathfrak{n})$ cannot be isogenous to one of the first two curves, because then, replacing T by $-T$ we would obtain a second bielliptic structure on $X_0(\mathfrak{n})$, in contradiction to Proposition 1.2.

The reduction mod T of the third curve has 12 rational points over $\mathbb{F}_9$. So if $X_0(T^4 + T^2 - 1)$ is bielliptic, its reduction modulo T cannot have more than 24 $\mathbb{F}_9$-rational points. The usual argument from step 1 of Lemma 3.2 exhibits 24 such points. Luckily, we can provide two more. Let ψ be the Drinfeld module over A/T given by $\psi_T = \tau^2 + \tau$. Then

$$\begin{aligned}
\psi_{T^4+T^2-1} &= \tau^8 + \tau^7 + \tau^5 - \tau^4 - \tau^3 + \tau^2 - 1\\
&= (\tau^4 - \tau - 1) \circ (\tau^4 + \tau^3 - \tau + 1)\\
&= (\tau^4 + \tau^3 - \tau + 1) \circ (\tau^4 - \tau - 1).
\end{aligned}$$

The zeroes of $X^{81} - X^3 - X$ resp. $X^{81} + X^{27} - X^3 + X$ are two $\mathbb{F}_3$-rational $(T^4 + T^2 - 1)$-isogenies of ψ. Since $j(\psi) \neq 0$ this gives two new $\mathbb{F}_9$-rational points on $X_0(T^4 + T^2 - 1)$, which therefore cannot be bielliptic. □

LEMMA 4.3. *If $q = 3$, the curves $X_0(\mathfrak{n})$ with $deg(\mathfrak{n}) = 4$ are not bielliptic.*

Proof. We mostly use the reduction method and its refinements. We order the cases according to the composition type of $\mathfrak{n}$.

Type (4), i.e., $\mathfrak{n}$ is irreducible: see the previous lemma.

Type $(1,3)$: After translation $\mathfrak{n} = T\mathfrak{p}$ where $\mathfrak{p} \in \mathbb{F}_3[T]$ is irreducible of degree 3. Replacing T by $-T$ if necessary we can assume that $\mathfrak{p}$ is one of the polynomials

$$T^3 - T + 1, \quad T^3 - T^2 + 1, \quad T^3 - T^2 + T + 1, \quad T^3 + T^2 - T + 1.$$

Correspondingly, the number of fixed points of the Atkin-Lehner involution $W_\mathfrak{p}$ on $X_0(T\mathfrak{p})$ is 14, 10, 10, or 6. So Proposition 1.2.b) together with $g(X_0(T\mathfrak{p})) = 12$ implies that the first three curves are not bielliptic.

To show that $X_0(T(T^3 + T^2 - T + 1))$ is also not bielliptic we apply the reduction technique. Let E be an elliptic curve over $\mathbb{F}_3(T)$ with conductor $\infty \cdot T(T^3 + T^2 - T + 1)$ or $\infty \cdot (T^3 + T^2 - T + 1)$. Checking the 8 (resp. 2) possibilities for $G(T)$ in Lemma 4.1 we see that E has ordinary reduction at one of the places $T - 1$ or $T + 1$. Hence this reduction cannot have more than 15 points over $\mathbb{F}_9$. But the reduction of $X_0(T(T^3 + T^2 - T + 1))$ has at least 32 $\mathbb{F}_9$-rational points.

Type (2^2): After translation $\mathfrak{n} = (T^2 + 1)^2$. We apply the method from [Sch5] to show that there is no elliptic curve E over $\mathbb{F}_3(T)$ with conductor $\infty \cdot (T^2 + 1)^2$. Then $X_0((T^2 + 1)^2)$ cannot be bielliptic. Suppose E exists. We can assume that $j(E)$ is not a 3-rd power in $\mathbb{F}_3(T)$. By [Sch5, Lemma 2.2.d)] then $j(E)$ has a pole at $T^2 + 1$. Thus by Lemma 4.1 we must have $j(E) = \pm\frac{T^6}{(T^2+1)^k}$. But this leads to additive reduction at a place different from $T^2 + 1$.

Type $(2,2)$: After translation $\mathfrak{n} = (T^2 + T - 1)(T^2 - T - 1)$. Again by Lemma 4.1 we find a linear place, such that E has ordinary reduction and hence at most 15 rational points over $\mathbb{F}_9$. But we also have to be careful with the points on the reduction of $X_0(\mathfrak{n})$. The Drinfeld module $\phi_T = \tau^2$ has $\varepsilon(T^2 + T - 1) = 10$ different $(T^2 + T - 1)$-isogenies. If such an isogeny is stable under one $\alpha \in \mathbb{F}_9^\times - \mathbb{F}_3^\times$, then it is stable under all $\alpha \in \mathbb{F}_9^\times$. Hence there are at least 2 of these isogenies that are stable under the action of $Aut(\phi)$. Analogously for the $(T^2 - T - 1)$-isogenies. Thus we see that $Aut(\phi)$ fixes at least 4 of the 100 $\mathfrak{n}$-isogenies of ϕ. This gives a minimum of 28 orbits. Together with the 4 cusps we have at least 32 $\mathbb{F}_9$-rational points on the reduction of $X_0(T^2 + T - 1)(T^2 - T - 1)$, which therefore cannot be bielliptic.

Types $(1^2, 2)$, $(1,1,2)$, $(1^3, 1)$ and $(1^2, 1^2)$ can be handled straightforward reducing modulo a linear place that doesn't divide $\mathfrak{n}$.

Type (1^4): Without loss of generality $\mathfrak{n} = T^4$. The reduction mod $T - 1$ is ordinary by [Ge3] or Lemma 4.1. But we also need that $X_0(T^4)$ has 4 rational cusps.

Type $(1^2, 1, 1)$: There is a quadratic place of ordinary reduction. The numbers are just good enough to show that $X_0(T^2(T - 1)(T + 1))$ is not bielliptic. □

LEMMA 4.4. *If $q = 2$, the curve $X_0(T^2(T^2 + T + 1))$ is not bielliptic.*

Proof. Argueing as in the proof of Proposition 1.2.a) we see that for bielliptic curves of genus 5 all bielliptic involutions commute with each other, and moreover, that the product of two or three different bielliptic involutions has no fixed points and is hence not bielliptic.

Suppose the genus 5 curve $X_0(T^2(T^2 + T + 1))$ has a bielliptic involution v. Let G be the group generated by all its bielliptic involutions. Then the elements of $G/\langle v\rangle$ are automorphisms of the genus 1 curve $v\backslash X_0(T^2(T^2 + T + 1))$. Moreover, they must permute the 4 ramification points of v. Fix one of these ramification points and call it P. Then the stabilizer H of P in $G/\langle v\rangle$ is a 2-elementary abelian subgroup of the automorphism group of an elliptic curve. Hence the cardinality of H divides 2 and thus $|G/\langle v\rangle|$ divides 8. So the cardinality of G divides 16 and therefore by the previous paragraph $X_0(T^2(T^2+T+1))$ has at most 5 bielliptic involutions.

The modular involution U_1 of $X_0(T^2(T^2+T+1))$ acts by conjugation on these bielliptic involutions. If their number is odd, then there is one, let's call it again v, that commutes which U_1. Counting fixed points one sees that v induces the hyperelliptic involution on $U_1\backslash X_0(T^2(T^2+T+1)) = X_0(T(T^2+T+1))$. So

$$\langle v, U_1\rangle\backslash X_0(T^2(T^2+T+1)) = X_+(T(T^2+T+1)).$$

Thus $\Gamma_0(T^2(T^2+T+1))$ would be normal in $\left\langle \Gamma_0(T(T^2+T+1)), \left(\begin{smallmatrix} 0 & 1 \\ T(T^2+T+1) & 0 \end{smallmatrix}\right)\right\rangle$. But this is easily disproved.

Consequently the number of bielliptic involutions is even, and we want to show it is zero. If not, it is incongruent to 0 modulo 3. Hence there exists a bielliptic involution, once again called v, that commutes with the modular automorphism $U_1W_{T^2}$, which has order 3. In [Sch2] it was worked out that $\langle U_1W_{T^2}\rangle\backslash X_0(T^2(T^2+T+1))$ is an elliptic curve; so $U_1W_{T^2}$ also has 4 fixed points. From this one easily sees that $U_1W_{T^2}$ and v have exactly the same fixed points. Thus the different of the degree 6 galois cover

$$X_0(T^2(T^2+T+1)) \to \langle vU_1W_{T^2}\rangle\backslash X_0(T^2(T^2+T+1))$$

has degree 12. Compared to $g(X_0(T^2(T^2+T+1))) = 5$ this yields the final contradiction. □

PROPOSITION 4.5. *Up to translation $T \mapsto T+1$, the table below contains all curves $X_0(\mathfrak{n})$ for $q=2$ with deg$(\mathfrak{n}) = 4$.*

$\mathfrak{n}$	g	*bielliptic*	*some bielliptic involutions*
T^4+T+1	4	*no*	–
T^4+T^3+1	4	*yes*	$W_{T^4+T^3+1}$
$T(T^3+T+1)$	6	*no*	–
$T(T^3+T^2+1)$	6	*yes*	$W_{T^3+T^2+1}$
$(T^2+T+1)^2$	2	*no*	–
$T^2(T^2+T+1)$	5	*no*	–
$T(T+1)(T^2+T+1)$	8	*no*	–
T^4	3	*yes*	W_{T^4}, U_1, U_2, $(W_{T^4}U_1)^2$, ...
$T^3(T+1)$	5	*yes*	U_1, $W_{T^3}U_1W_{T^3}$, ...
$T^2(T+1)^2$	4	*yes*	W_{T^2}, $W_{(T+1)^2}$, U_1, V_1, ...

The bielliptic involutions of $X_0(T^4+T^3+1)$ and $X_0(T(T^3+T^2+1))$ are unique.

Proof. The modular automorphisms in the table are easily checked to be bielliptic involutions. Compare [Sch4, Proposition 4.5] for the Atkin-Lehner involutions and [Sch2, Proposition 1] for strong Weil curves.

Now to the curves declared not bielliptic.

Suppose that $X_0(T^4+T+1)$ is bielliptic. Then its Jacobian contains an elliptic curve E. By [Ta, Appendix] we may suppose that E is defined over K. Then the conductor of E can only be $\infty\cdot(T^4+T+1)$. But by the characteristic 2 analogue of Lemma 4.1 (compare Lemma 2.4 in [Sch5] and the last page of that paper) there are no elliptic curves over $\mathbb{F}_2(T)$ with this conductor. Alternatively one can show, using for example the method described in Section 3 of [Sch1], that $J_0(T^4+T+1)$ splits over K into two simple 2-dimensional abelian varieties. Anyhow, $X_0(T^4+T+1)$ is not bielliptic.

A similar argument shows that the bielliptic involution of $X_0(T^4+T^3+1)$ is unique.

The Atkin-Lehner involutions W_T and $W_{T(T^3+T+1)}$ of $X_0(T(T^3+T+1))$ both have one fixed point, and since they commute it must be the same fixed point. Let's call it P. Now suppose $X_0(T(T^3+T+1))$ is bielliptic. Since its genus is 6, the bielliptic involution v commutes with W_T and $W_{T(T^3+T+1)}$ and hence also fixes P. As $W_TW_{T(T^3+T+1)} = W_{T^3+T+1}$ has 3 fixed points and thus is also different from v, the Atkin-Lehner involutions induce three different involutions on the elliptic curve $v\backslash X_0(T(T^3+T+1))$ (with origin P). But an elliptic curve has only one involution. So $X_0(T(T^3+T+1))$ is not bielliptic.

The cases $\mathfrak{n}=(T^2+T+1)^2$ and $\mathfrak{n}=T^2(T^2+T+1)$ were already treated in Proposition 2.4 resp. Lemma 4.4.

For $\mathfrak{n}=T(T+1)(T^2+T+1)$ we can apply Proposition 1.2.b); the involution $W_{(T+1)(T^2+T+1)}$ has 5 fixed points. □

We summarize the results of the last three sections.

THEOREM 4.6.

a) *Up to affine transformations, the bielliptic $X_0(\mathfrak{n})$ which are also hyperelliptic are the ones marked bielliptic in the table of Proposition 2.4.*

b) *Bielliptic curves $X_0(\mathfrak{n})$ which are not hyperelliptic exist only for $q=2$. Up to a translation $T\mapsto T+1$, these curves are given by $\mathfrak{n}=T^5+T^3+1$ (see Proposition 3.3) and the ones marked bielliptic in the table of Proposition 4.5.*

REMARK 4.7. A posteriori we see that there always exists at least one bielliptic involution which is modular and defined over K. With the exception of $q=2$, $\mathfrak{n}=T^3(T+1)$ (and of course $\mathfrak{n}=T(T+1)^3$ too) we can even find a bielliptic Atkin-Lehner involution.

However, we point out that for $q=2$ the curve $X_0(T^4)$ also has the bielliptic modular involution U_2, which is only defined over the quadratic extension $K(\alpha)$ where $\alpha^2+\alpha=\frac{1}{T}$ (see [Sch2]).

Actually, the group of modular automorphisms of $X_0(T^4)$ is isomorphic to the symmetric group S_4 (see [Sch2]) and every modular involution is conjugate to W_{T^4} or U_1 and hence bielliptic.

The Jacobian $J_0(T^4)$ of $X_0(T^4)$ splits up to isogeny into 3 elliptic curves, namely two copies of $X_0(T^3)$ and the new part $(W_{T^4}U_1)^2\backslash X_0(T^4)$. Over $K(\alpha)$ these two elliptic curves become isogenous ([Sch2]). This makes it possible that $U_2\backslash X_0(T^4)$ lies somehow diagonally in the old and new parts of $J_0(T^4)$. Compare [Ge2], Example 9.5 for the graph-theoretic interpretation.

5. Quadratic Points on $X_0(\mathfrak{n})$.

Let L be a global function field, i.e. a finite extension of $\mathbb{F}_q(T)$, and let C be a curve over L. A point P on C is called quadratic over L, if P is an L'-rational point on C for some quadratic extension L' of L.

For example, if C is hyperelliptic, then C has infinitely many quadratic points over L. Namely, over almost every L-rational point of the corresponding $\mathbb{P}^1$ there are two points on C, and these are rational over a suitable quadratic extension of L. Similarly, if C has an involution v, defined over L, such that $v\backslash C$ is an elliptic curve with positive rank over L.

As for number fields, proving some sort of converse requires a very deep result on abelian varieties. Also, there is a non-isotriviality condition, generalizing the non-isotriviality condition in [Sa, Théorème 5].

THEOREM 5.1. *Let L be a finite extension of $\mathbb{F}_q(T)$. Let C be a conservative, non-hyperelliptic curve over L with $g(C) \geq 3$, such that the Jacobian $Jac(C)/\overline{L}$ has no non-zero homomorphic images defined over $\overline{\mathbb{F}_q}$. Also suppose that C has at least one L-rational point P_0.*

If C has infinitely many quadratic points over L, then $Jac(C)/L$ contains an elliptic curve E which has positive rank over L. Moreover, there is a map of degree 2 from C to E; in particular, C is bielliptic.

Proof. Let $C^{(2)}$ be the symmetric product of C, that is $C \times C$ divided by the group that interchanges the two components. Mapping a quadratic point P on C to the class of $(P, \overline{P})$ in $C^{(2)}$, where $\overline{P}$ is the Galois conjugate of P, shows that if C has infinitely many quadratic points over L then $C^{(2)}$ has infinitely many L-rational points. Here we have neglected the (by [Sa, Théorème 5] finitely many) quadratic points that are inseparable over L.

The map $P \mapsto$ class of $(P - P_0)$ from C to $Jac(C)$ induces a K-rational map from $C^{(2)}$ to $Jac(C)$. Since C is not hyperelliptic, this map is injective and $C^{(2)}$ embeds into $Jac(C)$ as the locus W_2 of effective line bundles of degree 2 over C.

It is well known that under our condition on $Jac(C)$ the group Γ of L-rational points of $Jac(C)$ is finitely generated. The reasoning above shows that if C has infinitely many quadratic points over L then $W_2 \cap \Gamma$ is infinite.

Over the maximal algebraic constant field extension $\overline{\mathbb{F}_q}L$ of L we can apply Hrushovski's theorem, or rather a special case of it, namely [Hr, Corollary 1.2] with $A = Jac(C)$ and $X = W_2$. Since W_2 is 2-dimensional but not an abelian variety, this tells us that there exists at least one (translate of an) elliptic curve E in W_2 such that $E \cap \Gamma$ is infinite.

A priori E is defined over some finite constant field extension N of L. But if $\sigma \in Gal(N/L)$, then $\sigma(E)$ and E intersect in the infinitely many (L-rational) points of $E \cap \Gamma$. Thus $\sigma(E) = E$ and E is defined over L.

The conditions on $Jac(C)$ imply that E is not isotrivial. Having infinitely many L-rational points it therefore must have positive rank over L.

From now on we follow the proof in [A&H], because the strategy from [H&S] would need a lot of extra considerations in positive characteristic. Apparently there are some problems with the paper [A&H] (see the discussion in [D&F]), but they don't concern Lemma 1 and 2, which is essentially all we need.

To establish accordance with the notation in [A&H] we write A for E and define $A_2 = \{\alpha_1 + \alpha_2 \mid \alpha_i \in A\}$. For $\alpha \in A_2$ let L_α be the associated line bundle and $r(\alpha) = h^0(L_\alpha) - 1$. Then as in [A&H, Lemma 1] we have $r(\alpha) \geq 1$ for every $\alpha \in A_2$. On the other hand $r(\alpha) \leq 1$ for the general $\alpha \in A_2$ by Clifford's theorem. Now as in [A&H, Lemma 2] one obtains the existence of a map of degree 2 from C to A $(= E)$. □

The Jacobian $J_0(\mathfrak{n})$ of a Drinfeld modular curve $X_0(\mathfrak{n})$ has totally split multiplicative reduction at ∞. Hence $J_0(\mathfrak{n})$ has no non-zero homomorphic images defined over $\overline{\mathbb{F}_q}$. So the theorem applies in particular to Drinfeld modular curves.

It is almost the converse of the easy observations made above, except that it is not clear whether the degree 2 map from C to E is defined over L. But in the applications we have in mind we can circumvent this.

LEMMA 5.2. *There are exactly* 4 *bielliptic curves* $X_0(\mathfrak{n})$ *such that* $J_0(\mathfrak{n})/K$ *contains an elliptic curve* E *which has positive rank over* K. *These curves are, up to translation* $T \mapsto T+1$, *the ones with*

$$q=2, \quad \mathfrak{n}=T^5+T^3+1,$$
$$q=2, \quad \mathfrak{n}=T^4+T^3+1.$$

Moreover, the bielliptic involution must be the full Atkin-Lehner involution $W_\mathfrak{n}$. *The corresponding elliptic curves*

$$X_+(T^5+T^3+1): \quad Y^2+TXY+Y=X^3+TX^2,$$
$$X_+(T^4+T^3+1): \quad Y^2+TXY+Y=X^3+X^2,$$

both have rank 1 *over* K.

Proof. As an isogeny factor of $J_0(\mathfrak{n})/K$ the elliptic curve E has conductor $\infty \cdot \mathfrak{m}$ with $\mathfrak{m}|\mathfrak{n}$. According to A. Weil, the L-function $L_{E/K}(s)$ is a polynomial in q^{-s} of degree $deg(\mathfrak{m})-3$ (see [Shi], Theorem 4). By a result of Tate (compare [Shi], Theorem 7) the analytic rank of E over K (i.e. the zero order of $L_{E/K}(s)$ at $s=1$) is an upper bound for the (Mordell-Weil) rank of E over K.

So if this rank is positive, we must have $deg(\mathfrak{m}) \geq 4$. On the other hand, in Section 3 we have shown $deg(\mathfrak{n}) \leq 4$ (except for the case treated in Proposition 3.3). Hence $deg(\mathfrak{m}) = deg(\mathfrak{n}) = 4$ and E is contained in the new part $J_0^{new}(\mathfrak{n})$ of $J_0(\mathfrak{n})$. Moreover, the sign in the functional equation of $L_{E/K}(s)$ must be negative. Thus E is contained in $J_+^{new}(\mathfrak{n})$, the fixed part of $J_0^{new}(\mathfrak{n})$ under the full Atkin-Lehner involution $W_\mathfrak{n}$.

Using [Sch4, Lemma 1.2] it is not difficult to calculate the dimensions of $J_+^{new}(\mathfrak{n})$ for the bielliptic curves listed in Proposition 4.5. They are 0 except for $\mathfrak{n}=T^4+T^3+1$ (and $\mathfrak{n}=T^5+T^3+1$).

One easily checks that the elliptic curves $X_+(T^5+T^3+1)$ and $X_+(T^4+T^3+1)$ both have analytic rank 1 and no rational torsion points over $\mathbb{F}_2(T)$. Hence $(0,0)$ is a point of infinite order and the arithmetic rank is 1. □

THEOREM 5.3. *The Drinfeld modular curve* $X_0(\mathfrak{n})$ *has infinitely many quadratic points over* $\mathbb{F}_q(T)$ *in and only in the following cases*

- $deg(\mathfrak{n}) \leq 3$,
- $q=2$, $\mathfrak{n}=(T^2+T+1)^2$,
- $q=2$, $\mathfrak{n}=T^4+T^3+1$,
- $q=2$, $\mathfrak{n}=T^4+T^3+T^2+T+1$,
- $q=2$, $\mathfrak{n}=T^5+T^3+1$,
- $q=2$, $\mathfrak{n}=T^5+T^4+T^3+T^2+1$.

Proof. The first two cases give the $X_0(\mathfrak{n})$ which are rational, elliptic, or hyperelliptic. So the statement follows by combining Theorem 5.1. and Lemma 5.2. □

We conclude with another nice application of Theorem 5.1.

THEOREM 5.4. *Fix an irreducible* $\mathfrak{p} \in \mathbb{F}_q[T]$ *and a finite extension* L *of* $\mathbb{F}_q(T)$. *Then there is a uniform bound (depending only on* q, $\mathfrak{p}$ *and* L*) on the size of the* $\mathfrak{p}$*-primary part of the* L'*-rational torsion of* ϕ, *where* L' *ranges over all quadratic* *extensions of L, and ϕ ranges over all $\mathbb{F}_q[T]$-Drinfeld modules of rank 2 defined over L'.*

Proof. If n is big enough, the curve $X_0(\mathfrak{p}^n)$ has genus at least 3 and is neither hyperelliptic nor bielliptic. Hence by Theorem 5.1 it has only finitely many quadratic points over L. So there are only finitely many $\tilde{\jmath} \in \overline{K}$ that are j-invariants of Drinfeld modules ϕ over some L' with an L'-rational $\mathfrak{p}^n$-torsion point.

By [Po] Theorem 4, for each of these $\tilde{\jmath}$ there are only finitely many ϕ over L' with non-trivial torsion. Still, $\tilde{\jmath}$ may lie in L. Then there can be infinitely many such ϕ, finitely many over each of the infinitely many L'. In this case we apply Theorem 3 of [Po] with $d = 2$ and see that the torsion of these ϕ is uniformly bounded over all L'. □

REMARK 5.5. To prove Theorem 5.4 one obviously doesn't need the long-winded calculations from Section 4; indeed, Step 1 from the proof of Lemma 3.2 suffices.

Theorem 5.4 is somewhat stronger than Theorem 6 in [Po]. Actually, the applicability of Hrushovski's theorem to Drinfeld modular curves allows to strengthen Poonen's result even more by making it uniform in the degree $d = [L : K]$ of the extension. More precisely, by relating points of degree d on $X_0(\mathfrak{n})$ to maps of degree at most $2d$ from $X_0(\mathfrak{n})$ to $\mathbb{P}^1$ and then applying Ogg's trick, the bound on the $\mathfrak{p}$-primary torsion in Theorem 6 of [Po] can be chosen to depend only on q, $\mathfrak{p}$ and d. We intend to work out the details and some related results in a subsequent paper.

ACKNOWLEDGEMENTS

This paper was written in the year of the Dragon, which I spent at Academia Sinica in Taipei. I thank Prof. Jing Yu and Academia Sinica for the support and I am grateful to all the people there for making my stay in Taiwan such a pleasant experience.

REFERENCES

[A&H] D. ABRAMOVICH AND J. HARRIS, *Abelian varieties and curves in $W_d(C)$*, Compositio Math., 78 (1991), pp. 227–238.

[Ba] F. BARS, *Bielliptic modular curves*, J. Number Theory, 76 (1999), pp. 154–165.

[D&F] O. DEBARRE AND R. FAHLAOUI, *Abelian varieties in $W^r_d(C)$ and points of bounded degree on algebraic curves*, Compositio Math., 88 (1993), pp. 235–249.

[Ge1] E.-U. GEKELER, *Automorphe Formen über $\mathbb{F}_q(T)$ mit kleinem Führer*, Abh. Math. Sem. Univ. Hamburg, 55 (1985), pp. 111–146.

[Ge2] E.-U. GEKELER, *Jacquet-Langlands theory over K and relations with elliptic curves*, in: Drinfeld Modules, Modular Schemes and Applications, (E.-U. Gekeler, M. van der Put, M. Reversat, J. Van Geel, eds.), World Scientific, Singapore, 1997, pp. 224–257.

[Ge3] 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, G. Hiß, eds.), Springer, Berlin-Heidelberg-New York, 1998, pp. 49–64.

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

[G&R] E.-U. GEKELER AND M. REVERSAT, *Jacobians of Drinfeld Modular Curves*, J. Reine Angew. Math., 476 (1996), pp. 27–93.

[H&S] J. HARRIS AND J. SILVERMAN, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc., 112 (1991), pp. 347–356.

[Hru] E. HRUSHOVSKI, *The Mordell-Lang conjecture for function fields*, J. Amer. Math. Soc., 9 (1996), pp. 667–690.

[Po] B. POONEN, *Torsion in rank 1 Drinfeld modules and the uniform boundedness conjecture*, Math. Annalen, 308 (1997), pp. 571–586.

[Sa] P. SAMUEL, *Compléments à un article de Hans Grauert sur la conjecture de Mordell*, Publ. Math. I.H.E.S., 29 (1966), pp. 55–62.

[Sch1] A. SCHWEIZER, *On the Drinfeld Modular Polynomial* $\Phi_T(X, Y)$, J. Number Theory, 52 (1995), pp. 53–68.

[Sch2] A. SCHWEIZER, *Modular automorphisms of the Drinfeld modular curves* $X_0(\mathfrak{n})$, Collect. Math., 48 (1997), pp. 209–216.

[Sch3] A. SCHWEIZER, *Hyperelliptic Drinfeld Modular Curves*, in: Drinfeld Modules, Modular Schemes and Applications, (E.-U. Gekeler, M. van der Put, M. Reversat, J. Van Geel, eds.), World Scientific, Singapore, 1997, pp. 330–343.

[Sch4] A. SCHWEIZER, *Involutory elliptic curves over* $\mathbb{F}_q(T)$, J. Théor. Nombres Bordeaux, 10 (1998), pp. 107–123.

[Sch5] A. SCHWEIZER, *Extremal elliptic surfaces in characteristic* 2 *and* 3, Manuscripta Math., 102 (2000), pp. 505–521.

[Shi] T. SHIODA, *Some remarks on elliptic curves over function fields*, Astérisque, 209 (1992), pp. 99–114.

[Ta] A. TAMAGAWA, *The Eisenstein quotient of the Jacobian variety of a Drinfeld modular curve*, Publ. Res. Inst. Math. Sci., 31 (1995), pp. 203–246.