Journal de Théorie des Nombres
de Bordeaux **10** (1998), 107–123

Involutory elliptic curves over $\mathbb{F}_q(T)$

par Andreas SCHWEIZER

Résumé. Pour $\mathfrak{n} \in \mathbb{F}_q[T]$, G désigne un sous-groupe d'involutions d'Atkin-Lehner de la courbe modulaire $X_0(\mathfrak{n})$ de Drinfeld. On détermine tous les $\mathfrak{n}$ et G tels que la courbe $G \backslash X_0(\mathfrak{n})$ est rationnelle ou elliptique.

Abstract. For $\mathfrak{n} \in \mathbb{F}_q[T]$ let G be a subgroup of the Atkin-Lehner involutions of the Drinfeld modular curve $X_0(\mathfrak{n})$. We determine all $\mathfrak{n}$ and G for which the quotient curve $G \backslash X_0(\mathfrak{n})$ is rational or elliptic.

0. Introduction

In [M&SD] Mazur and Swinnerton-Dyer called a modular elliptic curve involutory if its Weil uniformization is given by a subgroup of the Atkin-Lehner involutions. They listed several examples. Later Kenku [Ke] showed that there exist only finitely many.

Using a slightly more general definition for elliptic curves over $\mathbb{F}_q(T)$ we ask: For which $\mathfrak{n} \in \mathbb{F}_q[T]$ and which subgroups G of the Atkin-Lehner involutions of the Drinfeld modular curve $X_0(\mathfrak{n})$ is the quotient curve $G \backslash X_0(\mathfrak{n})$ elliptic?

In this paper we will show that there are only finitely many (for all q together) and list them.

Two strategies are used to restrict the possible $\mathfrak{n}$. The first method, due to Ogg, consists in counting rational points on a suitable reduction. The second one transfers the problem from $\mathfrak{n}$ to divisors $\mathfrak{l}$ of $\mathfrak{n}$ by exploiting the knowledge how automorphic forms for $\Gamma_0(\mathfrak{l})$ lift to automorphic forms for $\Gamma_0(\mathfrak{n})$. Combined, these two strategies yield surprisingly good bounds for $\deg(\mathfrak{n})$. In the remaining cases the genus of $G \backslash X_0(\mathfrak{n})$ can be calculated or estimated using the explicit formulas of Section 2.

The results are gathered in Propositions 3.1, 3.2, 5.6, and 5.7 for elliptic quotient and in Propositions 3.3 and 5.5 for rational quotient.

Manuscrit reçu le 21 juillet 1997.

1. Basic facts

Let $\mathbb{F}_q$ be a finite field with q elements, $A := \mathbb{F}_q[T]$ the polynomial ring, $K := \mathbb{F}_q(T)$ the rational function field, $K_\infty := \mathbb{F}_q((T^{-1}))$ its completion at ∞ $(= \frac{1}{T})$, and C the completion of an algebraic closure of K_∞. The letters $\mathfrak{n}, \mathfrak{m}, \mathfrak{l}, \ldots$ will denote monic elements of A and $\mathfrak{p}$ will be a prime (i.e., a monic irreducible element) of A. Throughout this paper we will assume $\mathfrak{n} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ with different primes $\mathfrak{p}_i \in A$, and d will denote the degree of $\mathfrak{n}$.

The group $GL_2(K_\infty)$ acts on $\mathbb{P}^1(C)$, on $\mathbb{P}^1(K_\infty)$, and on the Drinfeld upper halfplane $\Omega = C - K_\infty$ by fractional linear transformations. So does the Hecke congruence subgroup

$$\Gamma_0(\mathfrak{n}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A) \ : \ \mathfrak{n}|c \right\}.$$

The quotient space $\Gamma_0(\mathfrak{n})\backslash\Omega$ can be compactified by adding the finite set of cusps $\Gamma_0(\mathfrak{n})\backslash\mathbb{P}^1(K)$. The resulting rigid analytic space is called the Drinfeld modular curve $X_0(\mathfrak{n})$.

As an algebraic curve $X_0(\mathfrak{n})$ is defined already over K and has good reduction at all finite primes $\mathfrak{p}$ with $\mathfrak{p} \not| \mathfrak{n}$. Its genus is ([Ge1 p.79] or [G&N]):

$$g(X_0(\mathfrak{n})) = 1 + \frac{\varepsilon(\mathfrak{n}) - (q+1)\kappa(\mathfrak{n}) - 2^{s-1}(q(q-1)r(\mathfrak{n}) + (q+1)(q-2))}{q^2-1}$$

where

$$\begin{aligned}
\varepsilon(\mathfrak{n}) &= \prod_{i=1}^{s} q^{(e_i-1)\deg(\mathfrak{p}_i)}(q^{\deg(\mathfrak{p}_i)} + 1), \\
\kappa(\mathfrak{n}) &= \prod_{i=1}^{s} (q^{\lfloor \frac{e_i}{2} \rfloor \deg(\mathfrak{p}_i)} + q^{\lfloor \frac{e_i-1}{2} \rfloor \deg(\mathfrak{p}_i)}), \\
r(\mathfrak{n}) &= \begin{cases} 1 & \text{if } 2|\deg(\mathfrak{p}_i) \text{ for all } \mathfrak{p}_i|\mathfrak{n}, \\ 0 & \text{otherwise.} \end{cases}
\end{aligned}$$

For every $\mathfrak{m}|\mathfrak{n}$ with $(\mathfrak{m}, \frac{\mathfrak{n}}{\mathfrak{m}}) = 1$ there exists the (partial) Atkin-Lehner involution $W_\mathfrak{m}^{(\mathfrak{n})}$ on $X_0(\mathfrak{n})$, sometimes simply denoted by $W_\mathfrak{m}$ if the $\mathfrak{n}$ is clear. It is given on $\Gamma_0(\mathfrak{n})\backslash\Omega$ (resp. $\Gamma_0(\mathfrak{n})\backslash\mathbb{P}^1(K)$) by multiplication from the left with any matrix $\begin{pmatrix} \mathfrak{m}a & b \\ \mathfrak{n}c & \mathfrak{m}d \end{pmatrix}$ with $a, b, c, d \in A$ and determinant $\gamma\mathfrak{m}$ for some $\gamma \in \mathbb{F}_q^\times$. From this it is obvious that $W_{\mathfrak{m}_1}W_{\mathfrak{m}_2} = W_{\mathfrak{m}_3}$ with $\mathfrak{m}_3 = \frac{\mathfrak{m}_1\mathfrak{m}_2}{(\mathfrak{m}_1,\mathfrak{m}_2)^2}$. Consequently the Atkin-Lehner involutions of $X_0(\mathfrak{n})$ form a 2-elementary-abelian group $\mathcal{W}(\mathfrak{n})$ of order 2^s.

In particular, $W_\mathfrak{n}^{(\mathfrak{n})}$, represented for example by $\begin{pmatrix} 0 & -1 \\ \mathfrak{n} & 0 \end{pmatrix}$, is called the full Atkin-Lehner involution and we define $X_+(\mathfrak{n}) := W_\mathfrak{n}\backslash X_0(\mathfrak{n})$.

Theorem 1.1 ([Sch3]). *Let $\mathfrak{n} \in \mathbb{F}_q[T]$ be of degree d. Then*

a) *$X_0(\mathfrak{n})$ is rational if and only if $d \leq 2$.*
b) *$X_0(\mathfrak{n})$ is elliptic if and only if $q = 2$, $d = 3$, and $\mathfrak{n}$ has a multiple root.*
c) *$X_0(\mathfrak{n})$ is hyperelliptic if and only if $d = 3$ (except the elliptic cases listed under b) or if $q = 2$ and $\mathfrak{n} = (T^2 + T + 1)^2$.*

In all these cases the curve $X_+(\mathfrak{n})$ is rational. In particular, for hyperelliptic $X_0(\mathfrak{n})$ the hyperelliptic involution is always the full Atkin-Lehner involution.

Throughout the paper we will freely use the fact that we can change coordinates by an affine transformation $T \mapsto \gamma T + \beta$ with $\beta \in \mathbb{F}_q$ and $\gamma \in \mathbb{F}_q^\times$. This reduces drastically the amount of explicit calculation we will have to do.

Let $\mathcal{T}$ be the Bruhat-Tits tree of $PGL_2(K_\infty)$. Its oriented edges are the cosets $GL_2(K_\infty)/(K_\infty^\times \cdot \mathcal{J})$ where $\mathcal{J}$ is the so-called Iwahori subgroup. For precise definitions and the connection between Ω and $\mathcal{T}$ see [G&R]. We only need some functorial properties.

The group $GL_2(K_\infty)$ acts from the right on the functions on the oriented edges of $\mathcal{T}$ by acting from the left on the argument. If φ is such a function and $M \in GL_2(K_\infty)$ we write $\varphi \circ M$ for the function which on the oriented edge e takes the value $\varphi(Me)$.

By $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ we denote the (finite-dimensional) $\mathbb{R}$-vector space of $\mathbb{R}$-valued, alternating, harmonic, $\Gamma_0(\mathfrak{n})$-invariant functions on the edges of $\mathcal{T}$, having finite support modulo $\Gamma_0(\mathfrak{n})$. Then the Atkin-Lehner involutions act from the right on $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$.

The importance of $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ for our purposes lies in the fact that for every subgroup G of $\mathcal{W}(\mathfrak{n})$ the genus of the curve $G\backslash X_0(\mathfrak{n})$ equals the dimension of the subspace of G-invariant elements of $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$.

If $\mathfrak{l}|\mathfrak{n}$ and $\mathfrak{a}|\frac{\mathfrak{n}}{\mathfrak{l}}$ then $\varphi \mapsto i_{\mathfrak{a},\mathfrak{l}}(\varphi) := \varphi \circ \begin{pmatrix} \mathfrak{a} & 0 \\ 0 & 1 \end{pmatrix}$ is an injective linear mapping from $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{l})}$ into $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$. Defining the space of newforms $\underline{H}_!^{\text{new}}(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ as the orthogonal complement of the space of oldforms $\sum\limits_{\substack{\mathfrak{l}|\mathfrak{n} \\ \mathfrak{l}\neq\mathfrak{n}}} \sum\limits_{\mathfrak{a}|\frac{\mathfrak{n}}{\mathfrak{l}}} i_{\mathfrak{a},\mathfrak{l}}(\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{l})})$ relative to the so-called Petersson scalar product, one obtains ([G&N]):

$$\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})} = \bigoplus_{\mathfrak{l}|\mathfrak{n}} \bigoplus_{\mathfrak{a}|\frac{\mathfrak{n}}{\mathfrak{l}}} i_{\mathfrak{a},\mathfrak{l}}(\underline{H}_!^{\text{new}}(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{l})}).$$

Thus, for every specific $\mathfrak{n}$ the dimension of the space of newforms can be calculated recursively.

In the analogy between $X_0(\mathfrak{n})$ and classical modular curves (over $\mathbb{C}$ or $\mathbb{Q}$) the elements of $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ correspond to cusp forms of weight 2 for a Hecke congruence subgroup. For more information, as for example the (proven!) analogue of the famous conjecture of Shimura, Taniyama, and Weil, see [G&R].

The following results are more or less analogous to Lemmata 25, 26, and 27 in [A&L].

Lemma 1.2. *Let* $\mathfrak{a}|\mathfrak{l}|\mathfrak{m}|\mathfrak{n}$ *with* $(\mathfrak{m}, \frac{\mathfrak{n}}{\mathfrak{m}}) = 1$ *and* $\deg(\mathfrak{l}) \geq 1$.

If $\varphi \in \underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\frac{\mathfrak{n}}{\mathfrak{l}})}$ *with* $\varphi \circ W_{\frac{\mathfrak{m}}{\mathfrak{l}}}^{(\frac{\mathfrak{n}}{\mathfrak{l}})} = \mu\varphi$ *(necessarily* $\mu \in \{\pm 1\}$*), then*

$$i_{\mathfrak{a},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi) \circ W_{\mathfrak{m}}^{(\mathfrak{n})} = \mu \cdot i_{\frac{\mathfrak{l}}{\mathfrak{a}},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi).$$

Especially: If $\mathfrak{a}^2 = \mathfrak{l}$*, then* $i_{\mathfrak{a},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi) \in \underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ *is an eigenform for* $W_{\mathfrak{m}}^{(\mathfrak{n})}$ *with eigenvalue* μ*. If* $\mathfrak{a}^2 \neq \mathfrak{l}$ *and* $\lambda \in \{\pm 1\}$*, then* $i_{\mathfrak{a},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi) + \lambda \cdot i_{\frac{\mathfrak{l}}{\mathfrak{a}},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi)$ *is a non-trivial eigenform for* $W_{\mathfrak{m}}^{(\mathfrak{n})}$ *with eigenvalue* $\lambda\mu$*.*

Proof. If $\begin{pmatrix} \mathfrak{m}x & y \\ \mathfrak{n}z & \mathfrak{m}t \end{pmatrix} \in Mat_2(\mathbb{F}_q[T])$ represents $W_{\mathfrak{m}}^{(\mathfrak{n})}$, then

$$\begin{aligned} i_{\mathfrak{a},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi) \circ W_{\mathfrak{m}}^{(\mathfrak{n})} &= \varphi \circ \begin{pmatrix} \mathfrak{a} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mathfrak{m}x & y \\ \mathfrak{n}z & \mathfrak{m}t \end{pmatrix} = \varphi \circ \begin{pmatrix} \mathfrak{a}\mathfrak{m}x & \mathfrak{a}y \\ \mathfrak{n}z & \mathfrak{m}t \end{pmatrix} \\ = \quad & \varphi \circ \begin{pmatrix} \mathfrak{m}x & y \\ \frac{\mathfrak{n}}{\mathfrak{a}}z & \frac{\mathfrak{m}}{\mathfrak{a}}t \end{pmatrix} = \varphi \circ \begin{pmatrix} \mathfrak{a}\frac{\mathfrak{m}}{\mathfrak{l}}x & y \\ \frac{\mathfrak{n}}{\mathfrak{l}}z & \frac{\mathfrak{m}}{\mathfrak{a}}t \end{pmatrix} \begin{pmatrix} \frac{\mathfrak{l}}{\mathfrak{a}} & 0 \\ 0 & 1 \end{pmatrix} \\ = \quad & (\varphi \circ W_{\frac{\mathfrak{m}}{\mathfrak{l}}}^{(\frac{\mathfrak{n}}{\mathfrak{l}})}) \circ \begin{pmatrix} \frac{\mathfrak{l}}{\mathfrak{a}} & 0 \\ 0 & 1 \end{pmatrix} = \mu\varphi \circ \begin{pmatrix} \frac{\mathfrak{l}}{\mathfrak{a}} & 0 \\ 0 & 1 \end{pmatrix} = \mu \cdot i_{\frac{\mathfrak{l}}{\mathfrak{a}},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi). \end{aligned}$$

$\square$

One important consequence of Lemma 1.2 is:

If S is a $\mathcal{W}(\frac{\mathfrak{n}}{\mathfrak{l}})$-stable subspace of $\underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\frac{\mathfrak{n}}{\mathfrak{l}})}$, then $\bigoplus_{\mathfrak{a}|\mathfrak{l}} i_{\mathfrak{a},\frac{\mathfrak{n}}{\mathfrak{l}}}(S)$ is stable under $\mathcal{W}(\mathfrak{n})$.

For $\mathfrak{l} = \mathfrak{p}$ a prime this results from the fact that $\mathcal{W}(\mathfrak{n})$ can be generated by involutions $W_{\mathfrak{m}}$ with $\mathfrak{p}|\mathfrak{m}$. The general case then is proved by iteration.

Especially we see that the space of oldforms in $\underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ is stable under $\mathcal{W}(\mathfrak{n})$. Since the Atkin-Lehner involutions are self-adjoint with respect to the Petersson scalar product, the space of newforms, too, must be stable under $\mathcal{W}(\mathfrak{n})$. Taking $S = \underline{\mathrm{H}}_!^{\mathrm{new}}(\mathcal{T}, \mathbb{R})^{\Gamma_0(\frac{\mathfrak{n}}{\mathfrak{l}})}$, we obtain

Proposition 1.3. *The subspaces*

$$\bigoplus_{\mathfrak{a}|\frac{\mathfrak{n}}{\mathfrak{l}}} i_{\mathfrak{a},\mathfrak{l}}(\underline{\mathrm{H}}_!^{\mathrm{new}}(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{l})})$$

of $\underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ *are stable under* $\mathcal{W}(\mathfrak{n})$*.*

If $g(G\backslash X_0(\mathfrak{n})) = 1$ for some subgroup G of $\mathcal{W}(\mathfrak{n})$, then $E = G\backslash X_0(\mathfrak{n})$ is an elliptic curve defined over K because $X_0(\mathfrak{n})$ and the Atkin-Lehner involutions are already defined over K and $X_0(\mathfrak{n})$ always has K-rational points. Generalizing the definition of [M&SD] slightly we call E an **involutory elliptic curve**.

E, being a quotient of $X_0(\mathfrak{n})$, has split multiplicative reduction at ∞. Moreover, the space of G-invariant elements of $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ is one-dimensional. By Proposition 1.3 its basis vector φ is contained in one of the subspaces $\bigoplus\limits_{\mathfrak{a}|\frac{\mathfrak{n}}{\mathfrak{l}}} i_{\mathfrak{a},\mathfrak{l}}(\underline{\mathrm{H}}_!^{\mathrm{new}}(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{l})})$. As the splitting of $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ into new and old parts of different level and under the action of the Hecke algebra and the Atkin-Lehner involutions reflects the corresponding decomposition of the Jacobian of $X_0(\mathfrak{n})$, the conductor of E is $\infty\cdot\mathfrak{l}$.

Obviously, an involutory elliptic curve $E = G\backslash X_0(\mathfrak{n})$ is a strong Weil curve if and only if $cond(E) = \infty\cdot\mathfrak{n}$ (i.e. the corresponding φ is a newform) and $g(U\backslash X_0(\mathfrak{n})) > 1$ for all proper subgroups U of G.

For more information on how data of (not necessarily involutory) strong Weil curves are encoded in the corresponding newforms see [Ge3].

Now we decompose $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{l})}$ into its simultaneous eigenspaces under the action of $\mathcal{W}(\mathfrak{l})$. If V is such an eigenspace, then by Lemma 1.2 for every possible choice of $\mathfrak{a}$ and λ the lifting $(i_{\mathfrak{a},\mathfrak{l}} + \lambda i_{\frac{\mathfrak{n}}{\mathfrak{a}\mathfrak{l}},\mathfrak{l}})(V)$ is contained in a simultaneous $\mathcal{W}(\mathfrak{n})$-eigenspace of $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$.

From this we see that the $\varphi \in \underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ belonging to an involutory elliptic curve $E = G\backslash X_0(\mathfrak{n})$ is contained in a subspace $(i_{\mathfrak{a},\mathfrak{l}}+\lambda i_{\frac{\mathfrak{n}}{\mathfrak{a}\mathfrak{l}},\mathfrak{l}})(V)$ where $V \subseteq \underline{\mathrm{H}}_!^{\mathrm{new}}(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{l})}$ is a one-dimensional simultaneous $\mathcal{W}(\mathfrak{l})$-eigenspace of $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{l})}$.

Let $\widetilde{G}$ be the group of all Atkin-Lehner involutions $W_{\mathfrak{m}}^{(\mathfrak{l})}$ which have eigenvalue $+1$ on V. Then E is isogenous over K to the involutory elliptic curve $\widetilde{E} = \widetilde{G}\backslash X_0(\mathfrak{l})$. Since the strong Weil curve in the isogeny class of $\widetilde{E}$ is necessarily involutory, we have proved

Proposition 1.4. *Every involutory elliptic curve $G\backslash X_0(\mathfrak{n})$ is isogenous over K to an involutory strong Weil curve of conductor $\infty\cdot\mathfrak{l}$ for some $\mathfrak{l}|\mathfrak{n}$.*

2. Calculating the genus of $G\backslash X_0(\mathfrak{n})$

We obtain almost the same formula as in the classical setting ([Kl]).

Proposition 2.1. *For any subgroup G of $\mathcal{W}(\mathfrak{n})$ we have*

$$g(G\backslash X_0(\mathfrak{n})) = 1 + \frac{1}{|G|}\left(g(X_0(\mathfrak{n})) - 1 - \frac{1+\delta}{2}\sum_{id\neq W_{\mathfrak{m}}\in G} \#(W_{\mathfrak{m}})\right),$$

where $\#(W_{\mathfrak{m}})$ denotes the number of fixed points of $W_{\mathfrak{m}}$ on $X_0(\mathfrak{n})$, and δ is 1 if q is even and 0 if q is odd.

Proof. This is essentially the Hurwitz formula. If q is odd, all ramification of the covering $X_0(\mathfrak{n}) \to G\backslash X_0(\mathfrak{n})$ is tame. If q is even, all ramification is wild but by a theorem of Gekeler, based on results of R. Crew and M. Raynaud, the second ramification groups are trivial (compare [Sch3], Proposition 7). $\square$

There are two types of fixed points of $W_{\mathfrak{m}}$ on $X_0(\mathfrak{n})$, those which are cusps and those which are interior points (i.e. in $\Gamma_0(\mathfrak{n})\backslash\Omega$). We denote their respective numbers by $\#_c(W_{\mathfrak{m}})$ and $\#_i(W_{\mathfrak{m}})$.

Proposition 2.2. *Let $W_{\mathfrak{m}}$ be a non-trivial Atkin-Lehner involution of $X_0(\mathfrak{n})$. For $y \in A$ define the number-theoretic function*

$$\varphi(y) := q^{\deg(y)} \prod_{\mathfrak{p}|y} (1 - q^{-\deg(\mathfrak{p})}).$$

a) *If q is odd we have*

$$\#_c(W_{\mathfrak{m}}) = \begin{cases} \frac{\varphi(y_1)}{q-1} \cdot 2^r & \text{if } \mathfrak{m} = y_1^2, \\ 0 & \text{otherwise.} \end{cases}$$

Here r denotes the number of different prime divisors of $\frac{\mathfrak{n}}{\mathfrak{m}}$.

b) *If q is even we have*

$$\#_c(W_{\mathfrak{m}}) = \begin{cases} \frac{\varphi(y_1)}{q-1} \sum\limits_{y_2 | \frac{\mathfrak{n}}{\mathfrak{m}}} \varphi(\gcd(y_2, \frac{\mathfrak{n}}{\mathfrak{m} y_2})) & \text{if } \mathfrak{m} = y_1^2, \\ 0 & \text{otherwise.} \end{cases}$$

The polynomials y_1 and y_2 are understood to be monic.

Proof. Combine Propositions 1 and 9 of [Sch3]. $\square$

Proposition 2.3 ([Sch3]). *If q is odd, the number of interior (i.e., non-cusp) fixed points of $W_{\mathfrak{m}}$ on $X_0(\mathfrak{n})$ is*

$$\#_i(W_{\mathfrak{m}}^{(\mathfrak{n})}) = \begin{cases} h(\sqrt{\alpha\mathfrak{m}}) \prod\limits_{\mathfrak{p}|\frac{\mathfrak{n}}{\mathfrak{m}}} (1 + (\frac{\alpha\mathfrak{m}}{\mathfrak{p}})) & \text{if } 2|\deg(\mathfrak{m}), \\ h(\sqrt{\mathfrak{m}}) \prod\limits_{\mathfrak{p}|\frac{\mathfrak{n}}{\mathfrak{m}}} (1 + (\frac{\mathfrak{m}}{\mathfrak{p}})) + h(\sqrt{\alpha\mathfrak{m}}) \prod\limits_{\mathfrak{p}|\frac{\mathfrak{n}}{\mathfrak{m}}} (1 + (\frac{\alpha\mathfrak{m}}{\mathfrak{p}})) & \text{if } 2 \not| \deg(\mathfrak{m}). \end{cases}$$

Here $\alpha \in \mathbb{F}_q^\times$ is a fixed non-square, $(\frac{f}{\mathfrak{p}})$ is the Legendre symbol, and $h(\sqrt{f})$ denotes the ideal class number of the (not necessarily maximal) order $\mathbb{F}_q[T, \sqrt{f}]$.

Lemma 2.4 ([Sch3]). *Suppose that q is even and $\mathfrak{n} = \mathfrak{l}\mathfrak{m}$ with $(\mathfrak{l}, \mathfrak{m}) = 1$ and $\deg(\mathfrak{m}) \geq 1$. Write $\mathfrak{m} = \mathfrak{m}_2^2\mathfrak{m}_1$ with $\mathfrak{m}_1, \mathfrak{m}_2 \in \mathbb{F}_q[T]$, where $\mathfrak{m}_1$ is square-free. There exist uniquely determined $\mathfrak{s}, \mathfrak{t} \in \mathbb{F}_q[T]$, not necessarily monic, with $\mathfrak{m}_1 = \mathfrak{s}^2 + T\mathfrak{t}^2$. Let*

$$\mathfrak{t}_1 = \prod_{\mathfrak{p} \nmid \mathfrak{m}_2} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathfrak{t})} \text{ and } \mathfrak{t}_2 = \prod_{\mathfrak{p} | \mathfrak{m}_2} \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\mathfrak{t})}.$$

a) *The number of interior fixed points of $W_\mathfrak{m}$ on $X_0(\mathfrak{m})$ is*

$$\#_i(W_\mathfrak{m}^{(\mathfrak{m})}) = \begin{cases} 0 & \text{if } \mathfrak{m} \text{ is a square,} \\ q^{\deg(\mathfrak{m}_2\mathfrak{t}_2)} \cdot \sum_{\mathfrak{f}|\mathfrak{t}_1} q^{\deg(\mathfrak{f})} & \text{otherwise.} \end{cases}$$

b) *More generally, we have $\#_i(W_\mathfrak{m}^{(\mathfrak{n})}) \leq \varepsilon(\mathfrak{l})\#_i(W_\mathfrak{m}^{(\mathfrak{m})})$.*
In particular, $\#_i(W_\mathfrak{m}^{(\mathfrak{n})}) = 0$ if $\mathfrak{m}$ is a square.

c) *If there exists a $\mathfrak{p}$ with $\mathrm{ord}_\mathfrak{p}(\mathfrak{l}) > 2\mathrm{ord}_\mathfrak{p}(\mathfrak{t}_1) + 1$, then $\#_i(W_\mathfrak{m}^{(\mathfrak{n})}) = 0$.*

d) *If $\mathfrak{l}$ is square-free and $\mathfrak{m}$ is not a square, then*

$$\#_i(W_\mathfrak{m}^{(\mathfrak{n})}) = q^{\deg(\mathfrak{m}_2\mathfrak{t}_2)} \cdot \sum_{\mathfrak{f}|\mathfrak{t}_1} q^{\deg(\mathfrak{f})}\varepsilon(\gcd(\mathfrak{l}, \frac{\mathfrak{t}_1}{\mathfrak{f}})).$$

Example 2.5. Let $q = 2$ and $\mathfrak{n} = T(T^3 + T^2 + 1)$. Then $g(X_0(\mathfrak{n})) = 6$ and $W_{T^3+T^2+1}^{(\mathfrak{n})}$ has 5 fixed points and hence $g(W_{T^3+T^2+1}\backslash X_0(\mathfrak{n})) = 1$.

We claim that the $W_{T^3+T^2+1}$-invariant form in $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ is a newform. This can be seen as follows:

Since $W_{T^3+T^2+1}$ acts as -1 on $\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(T^3+T^2+1)}$ (and W_1 as $+1$), it follows from Lemma 1.2 that $W_\mathfrak{n}^{(\mathfrak{n})}$ and $W_T^{(\mathfrak{n})}$ have opposite signs on

$$(i_{1,T^3+T^2+1} + \lambda i_{T,T^3+T^2+1})(\underline{H}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(T^3+T^2+1)}).$$

So $W_{T^3+T^2+1}^{(\mathfrak{n})}$ acts as -1 on the oldforms. We conclude that the involutory elliptic curve

$$W_{T^3+T^2+1}\backslash X_0(T(T^3 + T^2 + 1))$$

has conductor $\infty \cdot T(T^3 + T^2 + 1)$. It is even a strong Weil curve, for $X_0(T(T^3 + T^2 + 1))$ is not elliptic.

Furthermore one easily calculates that

$$\mathcal{W}(T(T^3 + T^2 + 1))\backslash X_0(T(T^3 + T^2 + 1))$$

has genus 0.

Example 2.6. Now let $q = 2$ and $\mathfrak{n} = T^2(T^3+T^2+1)$; then $g(X_0(\mathfrak{n})) = 13$. Moreover, W_{T^2} has 2 fixed points (which are cusps) and $W_\mathfrak{n}$ has 4 but Lemma 2.4 gives only a crude upper bound for the number of fixed points of $W_{T^3+T^2+1}$. Proposition 2.1 tells us that $W_{T^3+T^2+1}$ has 2, 6 or 10 fixed points and that the genus of $\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})$ is 2, 1 or 0, correspondingly.

Using Lemma 1.2 and the fact that $\underline{\mathrm{H}}_!^{\mathrm{new}}(\mathcal{T},\mathbb{R})^{\Gamma_0(T(T^3+T^2+1))}$ is 2-dimensional, we see that $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ contains a 6-dimensional subspace of W_{T^2}-invariant oldforms. As $g(W_{T^2}\backslash X_0(\mathfrak{n})) = 6$ we conclude that every W_{T^2}-invariant element (and a fortiori every $\mathcal{W}(\mathfrak{n})$-invariant element) of $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ must be an oldform.

Now suppose that $i_{\mathfrak{a},\mathfrak{l}}(\varphi) + \lambda i_{\frac{\mathfrak{n}}{\mathfrak{a}\mathfrak{l}},\mathfrak{l}}(\varphi)$ is a $\mathcal{W}(\mathfrak{n})$-invariant oldform. Then $\mathfrak{l}$ cannot be T^3+T^2+1 (same reason as in Example 2.5), so

$$\varphi \in \underline{\mathrm{H}}_!^{\mathrm{new}}(\mathcal{T},\mathbb{R})^{\Gamma_0(T(T^3+T^2+1))}.$$

Moreover, φ must be $W_{T^3+T^2+1}$-invariant, for otherwise the lifting would have opposite eigenvalues under W_{T^2} and $W_{\mathfrak{n}}$. Finally, the fact that the $W_{T^3+T^2+1}$-invariant form in $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(T(T^3+T^2+1))}$ has eigenvalue -1 under W_T (compare Example 2.5) forces $\lambda = -1$.

Summarizing: the subspace of $\mathcal{W}(\mathfrak{n})$-invariant forms in $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ is one-dimensional with basis $i_{1,T(T^3+T^2+1)}(\varphi) - i_{T,T(T^3+T^2+1)}(\varphi)$ where φ is the $W_{T^3+T^2+1}$-invariant form in $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(T(T^3+T^2+1))})$ discussed in the previous example.

So

$$\mathcal{W}(T^2(T^3+T^2+1))\backslash X_0(T^2(T^3+T^2+1))$$

is an elliptic curve with conductor $\infty\cdot T(T^3+T^2+1)$ and isogenous over $\mathbb{F}_2(T)$ to the strong Weil curve $W_{T^3+T^2+1}\backslash X_0(T(T^3+T^2+1))$.

Now that we know the number of fixed points of $W_{T^3+T^2+1}^{(T^2(T^3+T^2+1))}$, we easily check that none of the curves $W_{\mathfrak{m}}\backslash X_0(T^2(T^3+T^2+1))$ is elliptic.

3. The case $\deg(\mathfrak{n}) \leq 3$

According to Theorem 1.1, $\deg(\mathfrak{n}) = 3$ is the smallest possible case for which an elliptic $G\backslash X_0(\mathfrak{n})$ might exist.

If $\deg(\mathfrak{n}) = 3$, then the genus of $X_0(\mathfrak{n})$ is q if $\mathfrak{n}$ is square-free, and $q-1$ if not. We will also freely use the fact that then the full Atkin-Lehner involution $W_{\mathfrak{n}}$ acts as -1 on $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ (compare Theorem 1.1 or [Ge2]). Moreover, since there are no oldforms, every elliptic quotient of $X_0(\mathfrak{n})$ has conductor $\infty\cdot\mathfrak{n}$.

Proposition 3.1. *Let* $\deg(\mathfrak{n}) \leq 3$. *Up to affine transformations* $T \mapsto \gamma T + \beta$ $(\gamma,\beta \in \mathbb{F}_q,\ \gamma \neq 0)$, *the curve* $W_{\mathfrak{m}}\backslash X_0(\mathfrak{n})$ *is elliptic exactly in the following cases:*

q	$\mathfrak{n}$	$\mathfrak{m}$
2	T^3	1
2	$T^2(T+1)$	1
2	$T^2(T+1)$	$T+1$
2	$T(T^2+T+1)$	T
2	$T(T^2+T+1)$	T^2+T+1
3	$T^2(T-1)$	T^2
3	$T^2(T-1)$	$T-1$
3	$T(T-1)(T+1)$	$T(T-1)$
3	$T(T-1)(T+1)$	$T(T+1)$
3	$T(T-1)(T+1)$	$(T-1)(T+1)$
3	$T(T^2+1)$	T
3	$T(T^2+T-1)$	T^2+T-1
4	$T^2(T-1)$	T^2

For $q=2$ the curve $W_{T+1}\backslash X_0(T^2(T+1))$ is 2-isogenous to the elliptic curve $X_0(T^2(T+1))$. All other curves are strong Weil curves, and in fact these are all of the strong Weil curves for the given q and $\mathfrak{n}$.

The equations of the strong Weil curves for $q=2$ are

$$\begin{aligned} X_0(T^3) &: \quad Y^2+TXY = X^3+T^2, \\ X_0(T^2(T+1)) &: \quad Y^2+TXY+TY = X^3, \\ W_T\backslash X_0(T(T^2+T+1)) &: \quad Y^2+(T+1)XY+Y = X^3+T(T^2+T+1), \\ W_{T^2+T+1}\backslash X_0(T(T^2+T+1)) &: \quad Y^2+(T+1)XY+Y = X^3+X^2+T+1. \end{aligned}$$

Proof. If $\deg(\mathfrak{m})=1$, then $g_{\mathfrak{m}} := g(W_{\mathfrak{m}}\backslash X_0(\mathfrak{n})) = \frac{1}{2}(q+1-f)$, where $f\in\{0,1,2\}$ depends on q, $\mathfrak{n}$, and $\mathfrak{m}$ (see [Ge2], 8.5 and 8.8). This can also be derived from the formulas in Section 2. Since $g(W_{\frac{\mathfrak{n}}{\mathfrak{m}}}\backslash X_0(\mathfrak{n})) = g - g_{\mathfrak{m}}$, there remains to determine all $\mathfrak{m}$ of degree one with $g_{\mathfrak{m}}=1$ or $g_{\mathfrak{m}}=g-1$. For odd q this implies $1=\frac{1}{2}(q+1-f)\geq\frac{1}{2}(q-1)$ or $1=g-\frac{1}{2}(q+1-f)\geq q-1-\frac{1}{2}(q+1)$, whence $q\leq 3$ or $q\leq 5$, respectively. Similarly for even q. The remaining possible values for q and $\mathfrak{n}$ are then checked by direct calculation.

The remark on strong Weil curves follows from the table in [Ge2, p.142] and the equations for $q=2$ are given in [Ge3] and [G&R]. □

Proposition 3.2. *Up to affine transformations $T\mapsto\gamma T+\beta$ with $\gamma,\beta\in\mathbb{F}_q$, $\gamma\neq 0$, the 12 curves listed below are the only elliptic curves of the form $G\backslash X_0(\mathfrak{n})$ with $\deg(\mathfrak{n})\leq 3$ and $G\subseteq\mathcal{W}(\mathfrak{n})$ with $|G|\geq 4$.*

q	$\mathfrak{n}$	G
3	$T(T-1)(T+1)$	$\langle W_T, W_{T-1}\rangle$
3	$T(T-1)(T+1)$	$\langle W_T, W_{T+1}\rangle$
3	$T(T-1)(T+1)$	$\langle W_{T-1}, W_{T+1}\rangle$
4	$T(T-1)(T-\vartheta)$	$\langle W_T, W_{T-1}\rangle$
4	$T(T-1)(T-\vartheta)$	$\langle W_T, W_{T-\vartheta}\rangle$
4	$T(T-1)(T-\vartheta)$	$\langle W_{T-1}, W_{T-\vartheta}\rangle$
4	$T(T-1)(T-\vartheta)$	$\langle W_{T(T-1)}, W_{T(T-\vartheta)}\rangle$
5	$T(T-1)(T-2)$	$\langle W_T, W_{T-1}\rangle$
5	$T(T-1)(T-2)$	$\langle W_T, W_{T-2}\rangle$
5	$T(T-1)(T-2)$	$\langle W_{T(T-1)}, W_{T(T-2)}\rangle$
7	$T(T-1)(T-2)$	$\langle W_T, W_{T-2}\rangle$
7	$T(T-1)(T-3)$	$\langle W_{T(T-1)}, W_{T(T-3)}\rangle$

Here, of course, $\mathbb{F}_4 = \mathbb{F}_2(\vartheta)$. The curves for $q = 3$ are 2-isogenous to the elliptic curves given in Proposition 3.1. All others are strong Weil curves.

Proof. If $G\backslash X_0(\mathfrak{n})$ is elliptic and $|G| = 4$, then $\mathfrak{n}$ must be a product of 3 different linear factors, because G cannot contain $W_{\mathfrak{n}}$.

Fix a simultaneous eigenbasis $B = \{b_1, \dots, b_g\}$ of $\underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$ for all $W_{\mathfrak{m}}$ in $\mathcal{W}(\mathfrak{n})$. Set $G = \langle W_{\mathfrak{m}_1}, W_{\mathfrak{m}_2}\rangle$ and

$$\begin{aligned} B_{++} &:= \{b_i \in B \ : \ W_{\mathfrak{m}_1}(b_i) = b_i,\ W_{\mathfrak{m}_2}(b_i) = b_i\} \\ B_{+-} &:= \{b_i \in B \ : \ W_{\mathfrak{m}_1}(b_i) = b_i,\ W_{\mathfrak{m}_2}(b_i) = -b_i\} \end{aligned}$$

and similarly B_{-+} and B_{--}.

For odd q we know from the proof of Proposition 3.1 that $|B_{++}|+|B_{+-}| \geq \frac{q-1}{2}$, $|B_{++}|+|B_{-+}| \geq \frac{q-1}{2}$, and $|B_{+-}|+|B_{-+}| \leq \frac{q+1}{2}$ (because $B_{+-}\dot\cup B_{-+}$ is a basis for the elements having eigenvalue -1 under $W_{\mathfrak{m}_1}W_{\mathfrak{m}_2}$). If $|B_{++}| = 1$ this leads to $q-3 \leq |B_{+-}| + |B_{-+}| \leq \frac{q+1}{2}$, and hence $q \leq 7$. For even q a similar argument yields $q \leq 4$. □

Proposition 3.3. *For* $\deg(\mathfrak{n}) \leq 3$ *the curve* $G\backslash X_0(\mathfrak{n})$ *is rational in and only in the following cases:*

a) $\deg(\mathfrak{n}) \leq 2$, *$q$ arbitrary, G any subgroup of $\mathcal{W}(\mathfrak{n})$.*
b) $\deg(\mathfrak{n}) = 3$, *q arbitrary, G a subgroup of $\mathcal{W}(\mathfrak{n})$ containing the full Atkin-Lehner involution $W_{\mathfrak{n}}$.*
c) *For $q = 2$ in addition to cases a) and b),*
   $\mathfrak{n} = T^2(T+1)$, $G = \langle W_{T^2}\rangle$,
   $\mathfrak{n} = T(T+1)^2$, $G = \langle W_{(T+1)^2}\rangle$.

d) *For $q = 3$ in addition to cases a) and b),*
$\mathfrak{n} = T(T+1)(T-1), \qquad G = \langle W_{T(T+1)}, W_{T(T-1)} \rangle.$

Proof. From Theorem 1.1 it is clear that the curves $G\backslash X_0(\mathfrak{n})$ in case a) and b) are rational.

If $\deg(\mathfrak{n}) = 3$ and G doesn't contain $W_{\mathfrak{n}}$, by the same theorem, $X_0(\mathfrak{n})$ must be elliptic or $|G| = 4$, since the hyperelliptic involution is unique. Then by the same argument as in the preceding proofs we obtain $q \leq 3$. $\square$

4. Dividing by a single involution

Proposition 4.1. *The only rational curve of the form $W_{\mathfrak{m}} \backslash X_0(\mathfrak{n})$ with $\deg(\mathfrak{n}) \geq 4$ is the one with $q = 2$ and $\mathfrak{n} = \mathfrak{m} = (T^2 + T + 1)^2$.*

Proof. This follows immediately from Theorem 1.1. $\square$

Lemma 4.2. *Let G be a subgroup of $\mathcal{W}(\mathfrak{n})$.*

a) *If there exists a $\beta \in \mathbb{F}_q$ with $(T - \beta) \not| \mathfrak{n}$, then*

$$2^s + \frac{\varepsilon(\mathfrak{n})}{q+1} \leq |G| \cdot (q^2 + 1 + 2qg(G\backslash X_0(\mathfrak{n}))).$$

b) *If there exists a prime $\mathfrak{p} \in A$ of degree 2 with $\mathfrak{p} \not| \mathfrak{n}$, then*

$$2^s + \varepsilon(\mathfrak{n}) \leq |G| \cdot (q^4 + 1 + 2q^2 g(G\backslash X_0(\mathfrak{n}))).$$

Proof. a) The curve $X_0(\mathfrak{n})$ has good reduction mod $(T-\beta)$ and the Atkin-Lehner involutions induce non-trivial automorphisms of the reduced curve. Thus $X_0(\mathfrak{n})$ *mod* $(T - \beta)$ is a covering of degree $|G|$ of a curve of genus $g(G\backslash X_0(\mathfrak{n}))$. Therefore the right side of the inequality is an upper bound for the number of rational points of $X_0(\mathfrak{n})$ *mod* $(T - \beta)$ over the quadratic extension of $A/(T - \beta)$. On the other hand, we know from the proof of Lemma 18 in [Sch3] that $2^s + \frac{\varepsilon(\mathfrak{n})}{q+1}$ is a lower bound for the number of these rational points, namely: there are at least 2^s rational cusps and $\frac{\varepsilon(\mathfrak{n})}{q+1}$ interior points coming from a special supersingular Drinfeld module.

b) is proved similarly. $\square$

Lemma 4.3.

a) *If $W_{\mathfrak{m}} \backslash X_0(\mathfrak{n})$ is elliptic and $\mathfrak{l}|\mathfrak{m}$ with $\deg(\mathfrak{l}) \geq 1$, then $g(X_0(\frac{\mathfrak{n}}{\mathfrak{l}})) \leq 1$.*

b) *If $W_{\mathfrak{m}}\backslash X_0(\mathfrak{n})$ is elliptic and $\mathfrak{m}|\mathfrak{l}|\mathfrak{n}$ with $\deg(\mathfrak{l}) < \deg(\mathfrak{n})$, then $W_{\mathfrak{m}}\backslash X_0(\mathfrak{l})$ is rational.*

Proof. a) Suppose $\varphi_1, \varphi_2 \in \underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\frac{\mathfrak{n}}{\mathfrak{l}})}$ are linearly independent.

If they are $W_{\frac{\mathfrak{m}}{\mathfrak{l}}}$-invariant, then by taking $\mathfrak{a} = 1$ in Lemma 1.2 we obtain two linearly independent $W_{\mathfrak{m}}$-invariant elements of $\underline{\mathrm{H}}_!(\mathcal{T}, \mathbb{R})^{\Gamma_0(\mathfrak{n})}$. A similar construction works if φ_1 and φ_2 have eigenvalue -1 under $W_{\frac{\mathfrak{m}}{\mathfrak{l}}}$.

So far we have proved $g(X_0(\frac{\mathfrak{n}}{\mathfrak{l}})) \leq 2$. By Theorem 1.1 this implies $\deg(\frac{\mathfrak{n}}{\mathfrak{l}}) \leq 3$ or $q = 2$, $\frac{\mathfrak{n}}{\mathfrak{l}} = (T^2+T+1)^2$. Hence φ_1 and φ_2 are necessarily newforms. Therefore the 4 forms $i_{1,\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi_1)$, $i_{\frac{\mathfrak{n}}{\mathfrak{l}},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi_1)$, $i_{1,\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi_2)$, $i_{\frac{\mathfrak{n}}{\mathfrak{l}},\frac{\mathfrak{n}}{\mathfrak{l}}}(\varphi_2)$ are also linearly independent and we obtain a 2-dimensional $W_{\mathfrak{m}}$-invariant subspace of $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$.

b) Assume that $\varphi \in \underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{l})}$ is invariant under $W_{\mathfrak{m}}^{(\mathfrak{l})}$. Then $W_{\mathfrak{n}}^{(\mathfrak{n})}$ and $W_{\frac{\mathfrak{n}}{\mathfrak{m}}}^{(\mathfrak{n})}$ act on $\mathbb{R}\, i_{1,\mathfrak{l}}(\varphi) \oplus \mathbb{R}\, i_{\frac{\mathfrak{n}}{\mathfrak{l}},\mathfrak{l}}(\varphi) \subseteq \underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$ either both as $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ or both as $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. So $W_{\mathfrak{m}}^{(\mathfrak{n})}$ acts as identity on this 2-dimensional space. $\square$

Corollary 4.4. *If* $\mathfrak{n} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ *and* $W_{\mathfrak{m}} \backslash X_0(\mathfrak{n})$ *is elliptic, then* $s \leq 3$ *and* $\sum e_i \leq 4$.

Proof. We may assume $\mathfrak{p}_1 | \mathfrak{m}$. Then $g(X_0(\frac{\mathfrak{n}}{\mathfrak{p}_1})) \leq 1$ by part a) of the preceding lemma, and Theorem 1.1 implies $s-1 \leq 2$ and $(\sum e_i) - 1 \leq 3$. $\square$

Now assume that $W_{\mathfrak{m}} \backslash X_0(\mathfrak{n})$ is elliptic and $\deg(\mathfrak{n}) \geq 4$.

If $q \geq 4$, then by Corollary 4.4 there exists a $\beta \in \mathbb{F}_q$ with $(T-\beta) \nmid \mathfrak{n}$. Thus Lemma 4.2 yields $q^4 \leq q^d < \varepsilon(\mathfrak{n}) \leq (q+1)(2(q+1)^2-2) = 2q(q+1)(q+2) \leq \frac{15}{4} q^3$, a contradiction.

If $q = 3$, then $\mathfrak{n} = T^2(T-1)(T+1)$ (according to Corollary 4.4 up to translation the only possibility with $(T^3-T) | \mathfrak{n}$) is excluded by Lemma 4.3 a). Hence $(T^3 - T) \nmid \mathfrak{n}$, and Lemma 4.2 implies $\varepsilon(\mathfrak{n}) \leq 120$ (and consequently $d \leq 4$). The few cases holding this condition are excluded by direct calculation.

So we are left with $q = 2$. Applying 4.2, 4.3, and 4.4 imposes the restriction that $d = 4$ or $\mathfrak{n}$ is irreducible of degree 5.

Using the explicit formulas from Section 2 we obtain

Proposition 4.5. *Elliptic curves of the form* $W_{\mathfrak{m}} \backslash X_0(\mathfrak{n})$ *with* $\deg(\mathfrak{n}) \geq 4$ *exist only for* $q = 2$. *There are* 10 *such curves given by the following values and their translates under* $T \mapsto T+1$*:*

$$\begin{array}{lll} E_1: & \mathfrak{n} = T^5 + T^3 + 1, & \mathfrak{m} = \mathfrak{n}, \\ E_2: & \mathfrak{n} = T^4 + T^3 + 1, & \mathfrak{m} = \mathfrak{n}, \\ E_3: & \mathfrak{n} = T(T^3 + T^2 + 1), & \mathfrak{m} = T^3 + T^2 + 1, \\ E_4: & \mathfrak{n} = T^4, & \mathfrak{m} = \mathfrak{n}, \\ E_5: & \mathfrak{n} = T^2(T+1)^2, & \mathfrak{m} = T^2. \end{array}$$

The first three curves are strong Weil curves. Their equations over $\mathbb{F}_2(T)$ *are:*

E_1: $Y^2 + TXY + Y = X^3 + TX^2$,
E_2: $Y^2 + TXY + Y = X^3 + X^2$,
E_3: $Y^2 + (T+1)XY + TY = X^3$.

The curves E_4 *and* E_5 *are isogenous over* $\mathbb{F}_2(T)$ *to* $X_0(T^3)$ *respectively* $X_0(T(T+1)^2)$.

To find the equations of the strong Weil curves one proceeds as in Section 4 of [Ge3]. This involves the calculation of some Hecke operators on the quotient graph $\Gamma_0(\mathfrak{n})\backslash\mathcal{T}$, which is carried out in Chapter 4 of [Sch1]. The results are also listed in [Sch2].

5. Dividing by all involutions

Lemma 5.1. a) *If* $\mathfrak{l}|\mathfrak{n}$ *then* $g(\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})) \geq g(\mathcal{W}(\mathfrak{l})\backslash X_0(\mathfrak{l}))$.
b) *If* $\mathfrak{l}|\mathfrak{n}$ *and* $g(\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})) = g(\mathcal{W}(\mathfrak{l})\backslash X_0(\mathfrak{l})) = 1$, *then* $\frac{\mathfrak{n}}{\mathfrak{l}}$ *must be square-free.*

Proof. a) In fact $(i_{1,\mathfrak{l}} + i_{\frac{\mathfrak{n}}{\mathfrak{l}},\mathfrak{l}})(\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{l})\mathcal{W}(\mathfrak{l})})$ is a $\mathcal{W}(\mathfrak{n})$-invariant subspace of $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$.
b) If $\varphi \in \underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{l})}$ is invariant under $\mathcal{W}(\mathfrak{l})$ and $\mathfrak{a}^2|\frac{\mathfrak{n}}{\mathfrak{l}}$, then $i_{1,\mathfrak{l}}(\varphi)+i_{\frac{\mathfrak{n}}{\mathfrak{l}},\mathfrak{l}}(\varphi)$ and $i_{\mathfrak{a},\mathfrak{l}}(\varphi) + i_{\frac{\mathfrak{n}}{\mathfrak{a}\mathfrak{l}},\mathfrak{l}}(\varphi)$ are two linearly independent $\mathcal{W}(\mathfrak{n})$-invariant forms in $\underline{\mathrm{H}}_!(\mathcal{T},\mathbb{R})^{\Gamma_0(\mathfrak{n})}$.

□

Corollary 5.2. *Suppose* $g(\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})) \leq 1$ *for* $\mathfrak{n} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$.

a) *If* $q > 2$ *then* $\deg(\mathfrak{p}_i^{e_i}) \leq 3$ *for all* i.
b) *If* $q = 2$ *then* $\deg(\mathfrak{p}_i^{e_i}) \leq 5$ *for all* i.

Proof. Lemma 5.1 combined with Propositions 4.1 and 4.5. □

Proposition 5.3. *For* $q > 7$ *there don't exist any involutory elliptic curves over* $\mathbb{F}_q(T)$.

Proof. Suppose $g(\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})) \leq 1$. As $\varepsilon(\mathfrak{n}) \geq (q+1)^s$ and $\varepsilon(\mathfrak{n}) > q^d$, the inequality of Lemma 4.2. a) can be weakened to

$$\left(\frac{q+1}{2}\right)^s \leq q(q+1)(q+2) \tag{$*$}$$

and

$$q^d < 2^s q(q+1)(q+2), \tag{$**$}$$

provided there exists a $\beta \in \mathbb{F}_q$ with $(T-\beta)\not|\,\mathfrak{n}$.

First we show that for $q \geq 16$ there exist no involutory curves. If $(T^q - T)\not|\,\mathfrak{n}$, inequality $(*)$ shows $s \leq 3$. If $(T^q - T)|\mathfrak{n}$, applying Lemma 5.1 a) and then inequality $(*)$ we obtain $s - 1 \leq 3$. As $q \geq 16$, again $(T^q - T)\not|\,\mathfrak{n}$

and consequently $s \leq 3$ must hold for general $\mathfrak{n}$. Furthermore, equation $(**)$ implies $q^d < 8q^{\frac{17}{16}}q^{\frac{18}{16}}q < q^4$, and hence $d \leq 3$. But this was already excluded in Propositions 3.1 and 3.2.

For $q \in \{9, 11, 13\}$ the same argument yields $d = s = 4$. After affine transformation we may assume $\mathfrak{n} = T(T-1)(T-\beta)(T-\gamma)$ where $0, 1, \beta, \gamma$ are different and γ is a square in $\mathbb{F}_q^\times$. Using Proposition 2.1, one sees that $g(\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})) > 1$. (For the number of fixed points of $W_\mathfrak{m}$ with $\deg(\mathfrak{m}) = 3$ it suffices to estimate $h(\sqrt{\mathfrak{m}})$ and $h(\sqrt{\alpha\mathfrak{m}})$ by $q + 1 + 2\sqrt{q}$.)

Likewise, for $q = 8$ the decomposition types $(1,1,1,1)$ and $(2,1,1)$ must be treated by direct computation. $\square$

Lemma 5.4. *Let* $\mathfrak{n} = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ *be such that* $g(\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n}) \leq 1$. *Then (with* $d = \deg(\mathfrak{n})$*) one of the following assertions must hold:*

a) $q = 2$, $d \leq 8$, $s \leq 4$,
b) $q = 3$, $d \leq 5$, $s \leq 4$,
c) $q = 4$, $d \leq 5$, $s \leq 4$,
d) $q = 5$, $d \leq 5$, $s \leq 5$,
e) $q \geq 7$, $d \leq 3$.

Proof. We treat only the case $q = 3$ in detail.

First we assume $(T^3 - T) \not| \mathfrak{n}$. Then $s \leq 5$ by inequality $(*)$ and $d \leq 6$ by inequality $(**)$. But if $d \leq 6$, then s cannot be greater than 4. Moreover, the only possible decomposition type for $\mathfrak{n}$ with $s = 4$, namely $(1,1,2,2)$, is excluded by Lemma 4.2 a). Hence $s \leq 3$ and reentering $(**)$ gives $d \leq 5$.

The above discussion already implies $s \leq 4$ for general $\mathfrak{n}$. Thus, if $(T^3 - T)|\mathfrak{n}$ we can apply Lemma 4.2 b) and obtain $4^3 \cdot 3^{d-3} \leq \varepsilon(\mathfrak{n}) < 1600$, and consequently $d \leq 5$.

The proofs in the other cases are quite similar. For $q = 7$ the cases $3 \leq s \leq d = 4$, which resist Lemma 4.2, have to be excluded by direct computation. $\square$

It is even possible to improve on some of the bounds, but since we want to determine all involutory elliptic curves anyway, it's less work to start from below (i.e. first settle the case $d = 4$) and make use of Lemma 5.1. Carrying out all the calculations one obtains the following three propositions.

Proposition 5.5. *There are exactly* 9 *cases with* $\deg(\mathfrak{n}) \geq 4$ *for which the curve* $\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})$ *is rational, namely (up to translations* $T \mapsto T + \beta$*):*

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

The only rational curve of the form $G\backslash X_0(\mathfrak{n})$ where $\deg(\mathfrak{n}) \geq 4$ and G is a proper subgroup of $\mathcal{W}(\mathfrak{n})$ is the one with $q = 2$, $\mathfrak{n} = T(T+1)(T^2+T+1)$ and $G = \langle W_{T(T^2+T+1)}, W_{(T+1)(T^2+T+1)} \rangle$.

Proposition 5.6. *There are 72 elliptic curves of the form*

$$E = \mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})$$

with $\deg(\mathfrak{n}) \geq 4$, namely (up to affine transformations $T \mapsto \gamma T + \beta$):

q	$\mathfrak{n}$	$cond(E)$	l
2	T^4	$\infty \cdot T^3$	2
2	T^4+T^3+1	$\infty \cdot \mathfrak{n}$	2
2	$T(T^3+T+1)$	$\infty \cdot \mathfrak{n}$	2
2	$T^2(T^2+T+1)$	$\infty \cdot T(T^2+T+1)$	2
2	$T^3(T+1)$	$\infty \cdot T^2(T+1)$	2
2	T^5+T^3+1	$\infty \cdot \mathfrak{n}$	2
2	$(T^2+T+1)(T^3+T+1)$	$\infty \cdot \mathfrak{n}$	2
2	$T(T^4+T^3+1)$	$\infty \cdot (T^4+T^3+1)$	2
2	$T^2(T^3+T^2+1)$	$\infty \cdot T(T^3+T^2+1)$	2
2	$T(T+1)(T^3+T+1)$	$\infty \cdot T(T^3+T+1)$	2
2	$T^2(T+1)(T^2+T+1)$	$\infty \cdot T(T^2+T+1)$	2
3	$T(T^3-T+1)$	$\infty \cdot \mathfrak{n}$	6
3	$T(T^3+T^2+T-1)$	$\infty \cdot \mathfrak{n}$	6
3	$T(T-1)(T^2+1)$	$\infty \cdot \mathfrak{n}$	6
3	$T^2(T-1)(T+1)$	$\infty \cdot T(T-1)(T+1)$	3
4	$T(T+1)(T^2+\vartheta T+1)$	$\infty \cdot \mathfrak{n}$	12
4	$T(T+1)(T^2+\vartheta^2 T+1)$	$\infty \cdot \mathfrak{n}$	12
5	$(T-1)(T+1)(T-2)(T+2)$	$\infty \cdot \mathfrak{n}$	5

As usual $\mathbb{F}_4 = \mathbb{F}_2(\vartheta)$. The number l denotes the length of the orbit of $\mathfrak{n}$ under affine transformations.

Proposition 5.7. *A complete list of all elliptic curves $E = G\backslash X_0(\mathfrak{n})$ where $\deg(\mathfrak{n}) \geq 4$ and G is a proper subgroup of $\mathcal{W}(\mathfrak{n})$ is given below. Each horizontal box consists of one orbit under affine transformations $T \mapsto \gamma T + \beta$.*

For display reasons we use the abbreviations
$\mathfrak{m}_1 = T(T+1)(T+\vartheta)$,
$\mathfrak{m}_2 = T(T+1)(T+\vartheta^2)$,
$\mathfrak{m}_3 = T(T+\vartheta)(T+\vartheta^2)$,

$\mathfrak{m}_4 = (T+1)(T+\vartheta)(T+\vartheta^2)$.

q	$\mathfrak{n}$	G	$\mathrm{cond}(E)$
2	$T(T^3+T^2+1)$	$\langle W_{T^3+T^2+1}\rangle$	$\infty\cdot\mathfrak{n}$
2	$(T+1)(T^3+T+1)$	$\langle W_{T^3+T+1}\rangle$	$\infty\cdot\mathfrak{n}$
2	$T^2(T+1)^2$	$\langle W_{T^2}\rangle$	$\infty\cdot T(T+1)^2$
2	$T^2(T+1)^2$	$\langle W_{(T+1)^2}\rangle$	$\infty\cdot T^2(T+1)$
2	$T(T+1)(T^2+T+1)$	$\langle W_T, W_{\mathfrak{n}}\rangle$	$\infty\cdot T(T^2+T+1)$
2	$T(T+1)(T^2+T+1)$	$\langle W_{T+1}, W_{\mathfrak{n}}\rangle$	$\infty\cdot (T+1)(T^2+T+1)$
2	$T(T+1)(T^2+T+1)$	$\langle W_{T+1}, W_{T^2+T+1}\rangle$	$\infty\cdot T(T^2+T+1)$
2	$T(T+1)(T^2+T+1)$	$\langle W_T, W_{T^2+T+1}\rangle$	$\infty\cdot (T+1)(T^2+T+1)$
3	$(T-1)(T+1)(T^2+1)$	$\langle W_{(T-1)(T^2+1)}, W_{(T+1)(T^2+1)}\rangle$	$\infty\cdot\mathfrak{n}$
3	$T(T-1)(T^2-T-1)$	$\langle W_{T(T^2-T-1)}, W_{(T-1)(T^2-T-1)}\rangle$	$\infty\cdot\mathfrak{n}$
3	$T(T+1)(T^2+T-1)$	$\langle W_{T(T^2+T-1)}, W_{(T+1)(T^2+T-1)}\rangle$	$\infty\cdot\mathfrak{n}$
4	T^4+T	$\langle W_{\mathfrak{m}_1}, W_{\mathfrak{m}_2}, W_{\mathfrak{m}_3}\rangle$	$\infty\cdot\mathfrak{m}_4$
4	T^4+T	$\langle W_{\mathfrak{m}_1}, W_{\mathfrak{m}_2}, W_{\mathfrak{m}_4}\rangle$	$\infty\cdot\mathfrak{m}_3$
4	T^4+T	$\langle W_{\mathfrak{m}_1}, W_{\mathfrak{m}_3}, W_{\mathfrak{m}_4}\rangle$	$\infty\cdot\mathfrak{m}_2$
4	T^4+T	$\langle W_{\mathfrak{m}_2}, W_{\mathfrak{m}_3}, W_{\mathfrak{m}_4}\rangle$	$\infty\cdot\mathfrak{m}_1$

One sees that all the elliptic curves with conductor $\infty\cdot\mathfrak{n}$ listed in Propositions 5.6 and 5.7 are strong Weil curves.

The calculations (compare Example 2.6) also show that for $q=2$ and $\mathfrak{n}=T(T+1)(T^2+T+1)$ the curve $\langle W_T, W_{\mathfrak{n}}\rangle\backslash X_0(\mathfrak{n})$ is isogenous over $\mathbb{F}_2(T)$ to the strong Weil curve $W_T\backslash X_0(T(T^2+T+1))$. The other three involutory curves over $\mathbb{F}_2(T)$ with conductor $\infty\cdot T(T^2+T+1)$ are isogenous to $W_{T^2+T+1}\backslash X_0(T(T^2+T+1))$.

For $q=3$ and $\mathfrak{n}=T^2(T-1)(T+1)$ the curve $\mathcal{W}(\mathfrak{n})\backslash X_0(\mathfrak{n})$ is isogenous to $W_{(T-1)(T+1)}\backslash X_0(T(T-1)(T+1))$. The last curve in the table of Proposition 5.7 is isogenous to $\langle W_{T(T-1)}, W_{T(T-\vartheta)}\rangle\backslash X_0(T(T-1)(T-\vartheta))$.

For all other curves listed it is clear to which strong Weil curve they are isogenous, either by translating T or because there is only one involutory strong Weil curve of the given conductor.

Acknowledgements. The author, being supported by CICMA in form of a post-doc position at Concordia University and McGill University, wishes to express his gratitude to all three institutions.

References

[A&L] A. O. Atkin and J. Lehner, *Hecke Operators on* $\Gamma_0(m)$, Math. Annalen **185** (1970), 134–160.

[Ge1] E.-U. Gekeler, *Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern*, Bonner Mathematische Schriften 119 (1980).

[Ge2] E.-U. Gekeler, *Automorphe Formen über $\mathbb{F}_q(T)$ mit kleinem Führer*, Abh. Math. Sem. Univ. Hamburg **55** (1985), 111–146.

[Ge3] E.-U. Gekeler, *Analytical Construction of Weil Curves over Function Fields*, J. Théor. Nombres Bordeaux **7** (1995), 27–49.

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

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

[Ke] M. Kenku, *A note on involutory Weil curves*, Quat. J. Math. Oxford (Ser. 2) **27** (1976), 401–405.

[Kl] P. G. Kluit, *On the normalizer of $\Gamma_0(N)$. Modular Functions of one Variable V*, Springer LNM 601, Berlin Heidelberg New York 1977, 239–246.

[M&SD] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil Curves*, Invent. Math. **25** (1974), 1–61.

[Sch1] A. Schweizer, *Zur Arithmetik der Drinfeld'schen Modulkurven $X_0(\mathfrak{n})$*, Dissertation, Saarbrücken 1996

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

[Sch3] A. Schweizer, *Hyperelliptic Drinfeld Modular Curves*, in: Drinfeld modules, modular schemes and applications, Proceedings of a workshop at Alden Biesen, September 9-14, 1996, (E.-U. Gekeler, M. van der Put, M. Reversat, J. Van Geel, eds.), World Scientific, Singapore, 1997, pp. 330–343

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

Dept. of Mathematics
McGill University
805 Sherbrooke West
Montreal, Quebec H3A 2K6
Canada