Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint

Invariants of some algebraic curves related to Drinfeld modular curves

Ernst-Ulrich Gekeler

Preprint No. 14
Saarbrücken 2000

Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Invariants of some algebraic curves related to Drinfeld modular curves

Ernst-Ulrich Gekeler

Saarland University
Department of Mathematics
Postfach 15 11 50
D–66041 Saarbrücken
Germany
E-Mail: gekeler@math.uni-sb.de

submitted: August 18, 2000

Preprint No. 14

Saarbrücken 2000

Edited by
FR 6.1 – Mathematik
Im Stadtwald
D–66041 Saarbrücken
Germany

Fax: + 49 681 302 4443
e-mail: preprint@math.uni-sb.de
WWW: http://www.math.uni-sb.de/

Abstract

We collect some facts about Drinfeld modular curves for a polynomial ring $\mathbb{F}_q[T]$ over a finite field $\mathbb{F}_q$. These include formulas for the genera, the numbers of cusps and elliptic points, descriptions of the function fields and fields of definition, and other rationality properties. We then show that any series of Drinfeld modular curves of Hecke type $X_0(N_k)$, where $N_k \in \mathbb{F}_q[T]$ is coprime with T and $\deg(N_k) \longrightarrow \infty$, gives rise to an asymptotically optimal series of curves over $\mathbb{F}_{q^2}$.

0. Introduction. The maximal number $N_q(g)$ of rational points of a curve X of genus g over the finite field $\mathbb{F}_q$ is bounded as

$$N_q(g) \leq q + 1 + g[2q^{1/2}] \quad \text{(see [30])}. \tag{0.1}$$

Here and in the sequel, a "curve" denotes a smooth projective geometrically connected algebraic curve, and "rational" means $\mathbb{F}_q$-rational. Motivated from questions of coding theory, but also for intrinsic mathematical interest, one would like to know the quantity

$$A_q := \limsup_{g \to \infty} N_q(g)/g. \tag{0.2}$$

It is obvious from (0.1) that $A_q \leq [2q^{1/2}]$; however, Drinfeld and Vladut [6] showed that in fact

$$A_q \leq q^{1/2} - 1 \tag{0.3}$$

holds, and it is due to Ihara ([22], see also [31]) that we have equality in (0.3) if q is a perfect square.

In the last years, many papers have been published dealing with related questions, in particular, with the explicit construction of series of curves $X_k/\mathbb{F}_q$ that realize the above bound, a few of which are [31], [23], [32], [9], [7]. Such series $(X_k)_{k\in\mathbb{N}}$ will be called *asymptotically optimal*. Usually, the X_k are some sort of modular curves, and the difficulty lies in calculating or at least estimating their genera. In [9], an asymptotically optimal series is constructed through explicit equations, and the corresponding curves X_k are identified in [7] as (essentially) reductions of very specific Drinfeld modular curves.

Now it turns out that *each* series of Drinfeld modular curves of Hecke type (see (3.1)) over the polynomial ring $A = \mathbb{F}_q[T]$ gives rise to an asymptotically optimal series of curves $X_k/\mathbb{F}_{q^2}$. The precise statement is theorem 10.1, which is our main result. It is at the same time more general (allowing the construction of many different asymptotically optimal series), more precise

(in that it gives exact values instead of estimates), and, arguably, more conceptual compared to some of its predecessor. Its essential ingredients can be found in the author's thesis of 1979 (published 1980 [11] in german language), where the relevant invariants of Drinfeld modular curves have been calculated, and in some other papers (e.g. [13], [14]) of the eighties.

As the above indicates, there is an obvious need to make the mentioned results and calculations around Drinfeld modular curves more widely available, or at least to collect them at one place, which should be accessible to the entire mathematical community.

It is the aim of the present paper to fill that gap. That is, we will give here the necessary precise definitions, a few explanations, and the results about the arithmetic and geometry (rationality questions, descriptions and numbers of cusps and of elliptic points, genera, reduction properties) of various types of Drinfeld modular curves which should enable the reader (even without an extensive background in algebraic geometry) to construct his or her own favorite asymptotically optimal tower of curves. Among these results, apart from (10.1), the following are new or at least appear for the first time in print: (6.2), (6.3), (6.6), (6.7), (6.10), (6.11), (7.2), and (7.3). We will give proofs only in few cases where no satisfactory reference is available (for example, propositions 4.8, 6.2, 9.1); in all other cases, we restrict to giving hints or appropriate references. Since these point to different articles with different aims and notations, some translation has to be made by the reader who wishes to consult the original papers.

We focus on modular curves $X_0(N)$ of Hecke type since it is those which enter into the construction of theorem 10.1. Other Drinfeld modular curves like e.g. the $X_1(N)$ have so far not shown to be equally important. Nevertheless, we present also some results for such curves, which causes only small additional costs, and may turn out useful for other purposes. In order to be as readable as possible also for the non-expert, we avoid the use of Drinfeld modules, except for the proofs of (4.8) and (9.1), which however are inessential for the understanding of (10.1). In that case, we use the definitions and notation of [15] without further reference.

Acknowledgement. I am very grateful to Andreas Schweizer, who pointed out an error in the calculation of numbers of rational cusps (propositions 6.6 and 6.7) in an earlier version of this paper.

1. Notations. The following notation will be used throughout.

(1.1) A = $\mathbb{F}_q[T]$ = polynomial ring over the finite field with q elements, of characteristic p

K = $\mathbb{F}_q(T)$ = field of fractions of A

K_∞ = $\mathbb{F}_q((T^{-1}))$ = completion of K at the infinite place, with natural absolute value "$|\ .\ |$"; $|T| = q$

C_∞ = completed algebraic closure of K_∞, with the canonical extension of "$|\ .\ |$" to C_∞ and its "imaginary part" $|z|_i := \inf|z-x| = \min|z-x|$ $(x \in K_\infty)$

Ω = $C_\infty - K_\infty$ the Drinfeld upper half-plane, with its structure as an analytic space over K_∞ ([5], [8], [24])

(1.2) $\Gamma(1)$ = $\mathrm{GL}(2,A)$ the modular group, which acts on Ω through $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(z) = \frac{az+b}{cz+d}$.

For functions f on Ω, an element $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ of $\Gamma(1)$, and a weight $k \in \mathbb{Z}$, we put

$$f_{[\gamma]_k}(z) := (cz+d)^{-k} f(\gamma z),$$

which defines a right action of $\Gamma(1)$ on functions.

(1.3) Let now N be a non-constant monic element of A. We consider the subgroups $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$ of $\Gamma(1)$ of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ that are congruent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ modulo N, respectively. A *congruence subgroup with conductor* N of $\Gamma(1)$ is a subgroup Γ that contains $\Gamma(N)$, i.e., $\Gamma(N) \subset \Gamma \subset \Gamma(1)$.

(1.4) For N as above, we briefly write A/N for the finite ring A/NA, which contains $\mathbb{F}_q$ as a subring. If $N = P$ happens to be prime, we let $\mathbb{F}_P$ be the finite field A/P. We next put

$$\begin{aligned}
G &= G(N) = \mathrm{GL}(2, A/N), \quad G' = \{g \in G \mid \det g \in \mathbb{F}_q^*\} \\
B &= B(N) = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G\} \qquad B' = B \cap G' \\
I &= \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G \mid d \in \mathbb{F}_q^*\} \qquad J = \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G \mid a \in \mathbb{F}_q^*\} \\
H &= \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G \mid a, d \in \mathbb{F}_q^*\} = I \cap J, \quad U = \{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in G\} \\
Z &= \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \mid a \in \mathbb{F}_q\}, \text{ regarded as a subgroup either of} \\
&\quad \Gamma(1) \text{ or of } G(N).
\end{aligned}$$

(1.5) Let $N = \prod_{1 \le i \le s} P_i^{r_i}$ be the prime factorization of N, i.e., the P_i are different monic irreducible polynomials in A, with degrees $d_i := \deg(P_i)$,

$r_i \geq 1$, $1 \leq i \leq s = s(N)$. We further put $q_i := q^{d_i}$, and define the arithmetic functions

$$\begin{aligned} \varphi(N) &= \prod q_i^{r_i-1}(q_i - 1) \\ \epsilon(N) &= \prod q_i^{r_i-1}(q_i + 1) \\ \kappa(N) &= \prod (q_i^{[r_i/2]} + q_i^{[(r_i-1)/2]}). \end{aligned}$$

Here all the products are over $1 \leq i \leq s$ (thus $\varphi, \epsilon, \kappa$ are multiplicative), and "[.]" denotes "greatest integer". Finally, we put $r(N) = 1$ if all the d_i are even, and $r(N) = 0$ otherwise.

(1.6) Quite generally, if a group G acts from the left on a set X, we let G_x be the stabilizer of $x \in X$ and $G \setminus X$ the set of orbits. The multiplicative group of a ring R is denoted by R^*, the algebraic closure of a field L by L^{alg}. "Points" of a variety X over L are geometric (i.e., L^{alg}-valued) points. If X is a variety over C_∞, we do not distinguish between X, its associated analytic space, and its set of C_∞-valued points.

2. The j-line ([19], [11], [16]).

(2.1) An *elliptic point* e on Ω is one whose stabilizer $\Gamma(1)_e$ in $\Gamma(1)$ is strictly larger than $\mathbb{F}_q^* \cong Z \hookrightarrow \Gamma(1)$. Equivalently, e is $\Gamma(1)$-conjugate to some element of $\mathbb{F}_{q^2} - \mathbb{F}_q \hookrightarrow \Omega$, in which case $\Gamma(1)_e$ is isomorphic with $\mathbb{F}_{q^2}^*$. We choose once for all a fixed elliptic point $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ and let $S := \Gamma(1)_e$. By abuse of notation, we also write S for its isomorphic image in $G(N)$ under the natural map from $\Gamma(1)$ to $G(N)$.

(2.2) A *modular form of weight* k (and type 0, see [16]) for $\Gamma(1)$ is some function $f : \Omega \longrightarrow C_\infty$ that

(i) satisfies $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)$ (i.e., $f_{[\gamma]_k} = f$),

(ii) is holomorphic, and

(iii) is bounded on $\{z \in \Omega \mid |z|_i \geq 1\}$.

(The last condition is equivalent with the familiar "holomorphy at ∞" condition, since $\Gamma(1)$ has only one cusp, see (2.5) and (3.3).)

(2.3) The *Eisenstein series of weight* k for $\Gamma(1)$ is defined as

$$E_k(z) = \sum_{(a,b) \in A \times A}{}' \frac{1}{(az+b)^k} \quad (\textstyle\sum' = \text{sum over } (a,b) \neq (0,0))$$

for $z \in \Omega$. The series converges locally uniformly and defines for $0 < k \equiv 0 \pmod{q-1}$ a non-zero modular form of weight k for $\Gamma(1)$. From these we get the following analytic functions on Ω:

$$\begin{aligned} g(z) &:= (T^q - T)E_{q-1}(z) \\ \Delta(z) &:= (T^{q^2} - T)E_{q^2-1}(z) + (T^{q^2} - T^q)E_{q-1}^{q+1}(z) \\ j(z) &:= g^{q+1}(z)/\Delta(z). \end{aligned} \tag{2.4}$$

Their most important properties are: g and Δ are modular forms of respective weights $q-1$ and q^2-1, Δ vanishes nowhere on Ω (so j is a well-defined holomorphic and $\Gamma(1)$-invariant function on Ω), and j induces a biholomorphic map labelled by the same symbol

$$j : \Gamma(1) \setminus \Omega \xrightarrow{\cong} C_\infty. \tag{2.5}$$

That is, the "Riemann surface" $\Gamma(1) \setminus \Omega$ has a structure as an algebraic curve $Y(1)$ isomorphic with the affine line over C_∞ and with j as a coordinate. Its natural "compactification" $X(1)$ is the projective line $\mathbb{P}^1(C_\infty) = C_\infty \cup \{\infty\}$, where the added "cusp" ∞ corresponds to $j = \infty$ and the class of elliptic points to $j = 0$.

3. Modular curves ([18], [13], [15]).

(3.1) For each congruence subgroup Γ, the Riemann surface $Y_\Gamma = \Gamma \setminus \Omega$ is a finite cover of $Y(1)$, and is thus endowed with a unique structure of smooth affine algebraic curve over C_∞. We let X_Γ be its smooth projective model. Such curves are labelled as *Drinfeld modular curves*. If Γ is one of the groups $\Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$, we write $Y(N)$, $Y_1(N)$, $Y_0(N)$ and $X(N)$, $X_1(N)$, $X_0(N)$ for Y_Γ and X_Γ, and call $Y_0(N)$ and $X_0(N)$ the (affine and projective, respectively) *Drinfeld modular curve of Hecke type* with conductor N.

(3.2) An *elliptic point* of X_Γ will be the class of an elliptic point of Ω in $Y_\Gamma \hookrightarrow X_\Gamma$. (This notation is unusual but practical for our purposes.) A cusp of X_Γ is a point of $X_\Gamma - Y_\Gamma$. Set-theoretically, we have (e.g. [15] V 2.4) $X_\Gamma = \Gamma \setminus (\Omega \cup \mathbb{P}^1(K))$, and therefore

$$\{\text{cusps of } X_\Gamma\} = \Gamma \setminus \mathbb{P}^1(K) = \Gamma \setminus \Gamma(1)/\Gamma(1)_\infty, \tag{3.3}$$

since $\Gamma(1)$ acts transitively on $\mathbb{P}^1(K)$. Here $\Gamma(1)_\infty = \{\gamma \in \Gamma(1) \mid \gamma(\infty) = \infty\}$ $= \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\} \subset \Gamma(1)$. Similarly,

$$\{\text{elliptic points of } X_\Gamma\} = \Gamma \setminus \Gamma(1)/S. \tag{3.4}$$

(3.5) Now suppose that Γ has conductor N, and let $\overline{\Gamma}$ be its image in $G(N)$. Note that the natural map from $\Gamma(1)$ to $G(N)$ is NOT surjective (a popular mistake even in published literature), but is onto $G'(N)$. Therefore, $X(N)/X(1)$ and $X(N)/X_\Gamma$ are Galois covers with groups $G'(N)/Z$ and $\overline{\Gamma}\cdot Z/Z$, respectively. Putting $(A/N)^2_{\text{prim}}$ for the set of primitive vectors in $A/N \times A/N$ (those that span a direct summand $\neq 0$), the rule $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \longmapsto (a,c)$ induces a bijection from $\{\text{cusps of } X(N)\} = \Gamma(N) \setminus \Gamma(1)/\Gamma(1)_\infty$ to $(A/N)^2_{\text{prim}}/\mathbb{F}_q^*$. The natural action of $G'(N)$ on this set extends to $G(N)$, where the stabilizer of the cusp ∞ (i.e., the class of $\infty \in \mathbb{P}^1(K)$, or of the element $(1,0)$ of $(A/N)^2_{\text{prim}}$) is $G(N)_\infty = J(N)$. We thus get bijections

$$\{\text{cusps of } X(N)\} = G'(N)/G'(N)_\infty = G(N)/G(N)_\infty \xrightarrow{\cong} (A/N)^2_{\text{prim}}/\mathbb{F}_q^*$$

and finally

$$\{\text{cusps of } X_\Gamma\} = \overline{\Gamma} \setminus G(N)/G(N)_\infty \xrightarrow{\cong} \overline{\Gamma} \setminus (A/N)^2_{\text{prim}}/\mathbb{F}_q^*. \tag{3.6}$$

Similarly,

$$\{\text{elliptic points of } X_\Gamma\} \xrightarrow{\cong} \overline{\Gamma} \setminus G'(N)/S, \tag{3.7}$$

where $S \cong \mathbb{F}_{q^2}^*$ is the image in $G'(N)$ of $\Gamma(1)_e$. In section 6, we will give formulas for the numbers of cusps and elliptic points of $X(N)$, $X_1(N)$, and $X_0(N)$.

4. The function fields. In this section, we describe the function fields over C_∞ and over K of our curves.

(4.1) Let Γ be a congruence subgroup of conductor N. A *modular form for* Γ is a function $f : \Omega \longrightarrow C_\infty$ that satisfies conditions analogous to those in (2.2), i.e., (2.2)(i) is supposed to hold for $\gamma \in \Gamma$ only, and (2.2)(iii) is replaced by "$f_{[\gamma]_k}$ is bounded on $\{z \in \Omega \mid |z|_i \geq 1\}$ for all $\gamma \in \Gamma(1)$", which takes care of all the cusps of X_Γ, since these are conjugate under $\Gamma(1)$. The only example we need of such a form is as follows.

(4.2) Let $u, v \in K$ be two elements, not both in A, and with N as a common denominator. Put

$$E_{u,v}(z) = \sum_{\substack{(a,b)\in K\times K \\ (a,b)\equiv(u,v) \pmod{A\times A}}} \frac{1}{az+b},$$

an Eisenstein series of weight one. It depends only on the class of (u, v) modulo $A \times A$ and satisfies

$$E_{u,v}(\gamma z) = (cz + d)E_{(u,v)\gamma}(z)$$

for $\gamma \in \Gamma(1)$. In particular, it is a modular form of weight one for $\Gamma(N)$, and has the additional property that it vanishes nowhere on Ω ([11] 3.3.5).

(4.3) The function

$$f_{u,v}(z) := \frac{g(z)}{E_{u,v}^{q-1}(z)}$$

is invariant under $\Gamma(N)$, that is, a meromorphic function on $X(N)$ with poles at most at cusps. Two such, $f_{u,v}$ and $f_{u',v'}$, agree if and only if $(u', v') \equiv (u, v)$ in $(N^{-1}/A)^2 \bmod \mathbb{F}_q^*$ (*loc. cit.*). The covering group $\Gamma(1)/\Gamma(N)\cdot Z = G'(N)/Z$ of $X(N)$ over $X(1)$ acts on the function field $C_\infty(X(N))$, and for an element of that group represented by $\gamma \in \Gamma(1)$ we get

$$f_{u,v}^{\gamma}(z) := f_{u,v}(\gamma z) = f_{(u,v)\gamma}(z). \tag{4.4}$$

(4.5) In order to state the next result, we need to introduce some more notation. Let $K(N)$ be the N-th cyclotomic field extension of K [21], which may be characterized as the field of N-division points of the Carlitz module ([20] ch. III+VII), or through abstract class field theoretical data. It is an abelian extension of K with group $(A/N)^*$, and which ramifies precisely in ∞ (provided that $q > 2$) and the places dividing N. Let further $K_+(N)$ be its "maximal real subfield", i.e., the splitting field of ∞, which is also the fixed field of $\mathbb{F}_q^* \hookrightarrow (A/N)^*$.

4.6 Theorem ([11] 3.4.1, [13] sect. 2).

(i) *The function field $C_\infty(X(N))$ of $X(N)$ is generated over $C_\infty(X(1)) = C_\infty(j)$ by the functions $f_{u,v}$ $((0,0) \neq (u,v) \in (N^{-1}/A)^2)$.*

(ii) *The algebraic closure of K in $C_\infty(X(N))$ is isomorphic with $K_+(N)$. Upon identifying, the field $\mathcal{K}(N) := K_+(N)(j, f_{u,v})$ provides a $K_+(N)$-model of $C_\infty(j, f_{u,v}) = C_\infty(X(N))$ and thus a $K_+(N)$-structure $X(N)/K_+(N)$ of $X(N)$.*

(iii) *The action of $G'(N)/Z = \mathrm{Gal}(C_\infty(X(N))/C_\infty(j)) = \mathrm{Gal}(K_+(N)(X(N))/K_+(N)(j))$ given by (4.4) extends to an action of $G(N)/Z$ given by the same formula, and which identifies $G(N)/Z$ with $\mathrm{Gal}(\mathcal{K}(N)/K(j))$.*

(iv) $G(N)/G'(N) \xrightarrow{\simeq} (A/N)^*/\mathbb{F}_q^*$ *acts on* $K_+(N)(j)$ *over* $K(j)$ *like the Galois group* $(A/N)^*/\mathbb{F}_q^*$ *of* $K_+(N)$ *over* K.

(v) *The cusps of* $X(N)$ *are* $K_+(N)$*-rational points.*

4.7 Remark. Note here an important difference with the case of the classical elliptic modular curve $X_{\text{ell}}(N)$, which is defined over the N-th cyclotomic field $\mathbb{Q}(e^{2\pi i/N})$ but not over its real subfield.

The assertion (4.6) for $X(N)$ implies similar ones for the curves $X_1(N)$ and $X_0(N)$.

4.8 Proposition.

(i) *The function* $f_{0,N^{-1}}$ *satisfies a* C_∞*-irreducible equation of degree* $\frac{\varphi(N)\epsilon(N)}{q-1}$ *with coefficients in* $K(j)$.

(ii) $C_\infty(X_1(N)) = C_\infty(j, f_{0,N^{-1}})$

(iii) *The field* $K(j, f_{0,N^{-1}})$ *provides a* K*-model* $X_1(N)/K$ *of* $X_1(N)$.

Proof. We see from (4.4) that $f := f_{0,N^{-1}}$ is invariant under $\gamma \in G(N)$ if and only if $\gamma \in I(N)$. Restricting to $G'(N)$, we get $C_\infty(X_1(N)) = C_\infty(X(N))^{H(N)} = C_\infty(j, f)$, since $\overline{\Gamma_1(N)} \cdot Z = G'(N) \cap I(N) = H(N)$, i.e., assertion (ii). That field has degree $[G'(N) : \overline{\Gamma_1(N)} \cdot Z] = \frac{\varphi(N)\epsilon(N)}{q-1}$ over $C_\infty(j)$. Let now ϕ be the "generic" Drinfeld module over $K(j)$ defined by $\phi_T(X) = TX + X^q + j^{-1}X^{q^2}$. Then $\phi_N(X) = NX + \cdots + j^{-(q^{2d}-1)/(q^2-1)}X^{q^{2d}}$ (with $d := \deg N$) has coefficients in $K(j)$, and may be written as

$$\phi_N(X) = j^{-(q^{2d}-1)/(q^2-1)} X \prod_M \tilde{\phi}_M(X^{q-1}),$$

where M runs through the non-constant monic divisors of N and $\tilde{\phi}_M$ collects the ϕ-division points of precise order M, grouped in orbits under $\mathbb{F}_q^*$. We have $\tilde{\phi}_M(X) \in K(j)[X]$, of degree $\frac{\varphi(M)\epsilon(M)}{q-1}$. Since f is a zero of $\tilde{\phi}_N$ ([11] p. 65), it is the minimal polynomial of f both over $K(j)$ and $C_\infty(j)$. This simultaneously shows (i) and (iii). $\square$

In a similar fashion ([14] 3.2), we may describe the function field of $X_0(N)$. Let j_N be the function $j_N(z) := j(Nz)$.

4.9 Proposition.

(i) *j_N is invariant under $\Gamma_0(N)$ and satisfies the equation $\Phi(j_N, j) = 0$ with the "modular polynomial" $\Phi_N(X, Y) \in A[X, Y]$.*

(ii) *$C_\infty(X_0(N)) = C_\infty(j, j_N)$*

(iii) *The field $K(j, j_N)$ provides a K-model $X_0(N)/K$ of $X_0(N)$.*

4.10 Remark. In both the cases of $X_1(N)$ and $X_0(N)$, the plane equations satisfied by j and $f_{0,N^{-1}}$ (resp. j and j_N) may be explicitly worked out. This is straightforward for $X_1(N)$; some material on the modular polynomial $\Phi_N(X, Y)$ may be found in [26], [1], [2] and also in [33], where the nature of its singularities is studied.

5. Reduction properties.

Quite generally, the curves $X(N)/K_+(N)$, $X_1(N)/K$ and $X_0(N)/K$ have good reduction at those places of their field of definition that do not divide the conductor N. This follows from their modular interpretation, i.e., the existence of a modular scheme, say, $\overline{M}^2(N)$ over A such that $X(N)/K_+(N)$ is one component of $\overline{M}^2(N) \times_A K_+(N)$. See [5] sect. 5, [3] II, III, or [25] for details.

If $P \in A$ is a prime not dividing N, the reduction $X_1(N)/\mathbb{F}_P$ is a (smooth, projective, geometrically connected) curve over $\mathbb{F}_P$ with the same genus as $X_1(N)/K$, and provided with a reduction map $\mathrm{red} : X_1(N)(K^{\mathrm{alg}}) \longrightarrow X_1(N)(\mathbb{F}_P^{\mathrm{alg}})$ on geometric points. (We have here already simplified the notation, omitting the obvious fields of definition K and $\mathbb{F}_P$.) Similarly, there are curves $X_0(N)/\mathbb{F}_P$ and affine curves $Y_1(N)/\mathbb{F}_P$ and $Y_0(N)/\mathbb{F}_P$ with analogous reduction mappings. The next two results again follow from the modular interpretation.

5.1 Proposition. *For $i = 0, 1$, the reduction maps* red *induce bijections*

$$\begin{aligned}
&\{\textit{cusps of } X_i(N)\} = X_i(N)(C_\infty) - Y_i(N)(C_\infty) \\
&= X_i(N)(K^{\mathrm{alg}}) - Y_i(N)(K^{\mathrm{alg}}) \xrightarrow[\mathrm{red}]{\cong} X_i(N)(\mathbb{F}_P^{\mathrm{alg}}) - Y_i(N)(\mathbb{F}_P^{\mathrm{alg}}) \\
&= \{\textit{cusps of } X_i(N)/\mathbb{F}_P\}.
\end{aligned}$$

A similar property holds for elliptic points. Note first that elliptic points on any modular curve are algebraic, as is obvious from definitions. If we *define* an elliptic point of $Y_i(N)/\mathbb{F}_P$ to be one that lies above the point $j = 0$ of $Y(1)/\mathbb{F}_P = \mathrm{Spec}\ \mathbb{F}_P[j]$, we have:

5.2 Proposition. *For $i = 0, 1$, the reduction maps induce bijections*

$$\{\textit{elliptic points of } X_i(N)\} \xrightarrow[\text{red}]{\cong} \{\textit{elliptic points of } X_i(N)/\mathbb{F}_P\}.$$

5.3 Remarks.

(i) Of course, similar reduction properties hold for $X(N)$. But since these involve constant field extensions, they are slightly more complicated to state, and are therefore omitted.

(ii) Roughly speaking, a point x on such a modular curve $X/\mathbb{F}_P$ corresponds to a Drinfeld module (with some supplementary structure) ϕ of rank two over $\mathbb{F}_P^{\text{alg}}$. We then have $\text{Aut}(\phi) \cong \mathbb{F}_{q^2}^*$ if x is elliptic and $\text{Aut}(\phi) \cong \mathbb{F}_q^*$ otherwise, regardless of the "characteristic" P of $\mathbb{F}_P$. In particular, these automorphism groups are always abelian. Hence there is no Drinfeld analogue to the occurrence of unusually large automorphism groups of supersingular elliptic curves in characteristics 2 and 3.

6. Number of (rational) cusps.

We also want to know the fields of definition of the cusps of $X_i(N)$ $(i = 0, 1)$, which lie between K and $K_+(N)$. Let us first make the following definition.

(6.1) According to personal taste, a *cuspidal prime divisor* of $X_i(N)$ will be either one of

(a) a scheme-theoretic point of $X_i(N)/K$ above the point $j = \infty$ of $X(1)/K$;

(b) a place of the function field $K(X_i(N))$ above $j = \infty$;

(c) an orbit under $\text{Gal}(K^{\text{alg}}/K)$ on $\{\text{cusps of } X_i(N)\}$.

(The three sets are in canonical bijection.)
For the curve $X_1(N)$ the following description results.

6.2 Proposition.

(i) *The cuspidal prime divisors of $X_1(N)/K$ correspond bijectively and canonically to $I(N) \setminus G(N)/G(N)_\infty$, whereas the cusps of $X_1(N)$ are given by $H(N) \setminus G(N)/G(N)_\infty$.*

(ii) *Let x be a cusp of $X(N)$, i.e., an element of $G(N)/G(N)_\infty$, with stabilizer $I(N)_x$ (resp. $H(N)_x$) in $I(N)$ (resp. $H(N)$). Let further $[x] = I(N) \cdot x$ be its orbit under $I(N)$, regarded (cf. (i)) as a cuspidal*

divisor $[x]$ *of* $X_1(N)$*, with residue class field* $K([x])$*. The isomorphism* $I(N)/H(N) \xrightarrow{\simeq} (A/N)^*/\mathbb{F}_q^*$ *induced by the determinant gives rise to an inclusion* $I(N)_x/H(N)_x \hookrightarrow (A/N)^*/\mathbb{F}_q^*$*, whose cokernel equals* $\mathrm{Gal}(K([x])/K)$*. In particular,* $[x]$ *corresponds to a* K*-rational point iff* $[I(N)_x : H(N)_x] = \frac{\varphi(N)}{q-1}$ *holds.*

Proof. (i) is obvious from (3.6), (4.6) and the descriptions of function fields and Galois groups, notably $\mathrm{Gal}(\mathcal{K}(N)/K(X_1(N))) = I(N)/Z$, which is a consequence of (4.8).
(ii) In the extension $\mathcal{K}(N)/K(X_1(N))$, the fixed field of $\overline{\Gamma_1(N)} \cdot Z/Z = H(N)/Z$ is the constant extension part. Hence $I(N)_x/H(N)_x =$ Galois group of $K_+(N)$ over $K([x])$, and the assertion follows. $\square$

With similar reasoning, we get the corresponding result for $X_0(N)$.

6.3 Proposition.

(i) *The cuspidal prime divisors of* $X_0(N)/K$ *correspond bijectively to* $B(N) \setminus G(N)/G(N)_\infty$*, whereas the cusps of* $X_0(N)$ *are given by* $B'(N) \setminus G(N)/G(N)_\infty$*.*

(ii) *If* $x \in G(N)/G(N)_\infty$ *is a cusp of* $X(N)$ *and* $[x]$ *the cuspidal divisor of* $X_0(N)/K$ *corresponding to the orbit* $B(N) \cdot x$*, then the cokernel of* $B(N)_x/B'(N)_x \underset{\det}{\hookrightarrow} (A/N)^*/\mathbb{F}_q^*$ *equals* $\mathrm{Gal}(K([x])/K)$*.*

(6.4) The double cosets that appear in (6.2) and (6.3) and their cardinalities may be determined as either

(a) the set of orbits of $I(N)$, $H(N)$, $B(N)$, $B'(N)$, acting from the left on $G(N)/G(N)_\infty = (A/N)^2_{\mathrm{prim}}/\mathbb{F}_q^*$, *or*

(b) the set of orbits of $G(N)_\infty = J(N)$ on $I(N) \setminus G(N)$, etc., acting from the right.

We restrict to giving the results of the (cumbersome but elementary) calculations, along with some comments. The quantities in the following formulas refer to the prime factorization (1.5) of N.

$$(6.5) \qquad \#\{\text{cusps of } X(N)\} = [G(N) : G(N)_\infty] = \frac{\varphi(N)\epsilon(N)}{q-1}$$

6.6 Proposition. (i) *The number of cusps of* $X_1(N)$ *is*

$$2\frac{\varphi(N)}{q-1} + \frac{\varphi(N)}{(q-1)^2}\left[\prod_{1\le i\le s}(r_i + 1 - \frac{r_i - 1}{q_i}) - 2\right].$$

(ii) *The number of K-rational cusps is* 2, *if* $\deg N = 1$, *and*

$$\frac{\varphi(N)}{q-1}+\frac{\varphi(N)}{(q-1)^2}[\#\{i \mid q_i = q \text{ and } r_i = 1\}+\frac{q-1}{q}\#\{i \mid q_i = q \text{ and } r_i > 1\}]+\alpha$$

otherwise. The quantity α vanishes unless $q = 2$ and $T(T-1)|N$, in which case it is $2^{-t}\varphi(N)$ with $t = 0, 1, 2$ if none, one, or two of T and $T-1$ are multiple divisors of N.

6.7 Proposition. (i) *The number of cusps of $X_0(N)$ is $2^s + \frac{\kappa(N)-2^s}{q-1}$.*
(ii) *If P_i is a prime divisor of N of degree one, put $t_i = 0, 1, 2$ if $r_i = 1, 2,$ larger or equal to* 3, *respectively. Then the number of rational cusps of $X_0(N)$ is*

$$2^s + 2^{s-1}\sum t_i + 2^{s-2}u,$$

where the sum is over the prime divisors of degree one of N and $u = t_1 \cdot t_2$ if ($q = 2$ and $P_1 = T$, $P_2 = T-1$ are divisors of N), and $u = 0$ otherwise.

6.8 Remarks. (i) (6.5) is of course trivial, and is included for completeness only.
(ii) The genus $g(X_\Gamma)$ and the number of cusps of a modular curve X_Γ agree with similar invariants of the almost-finite graph $\Gamma\backslash\mathcal{T}$, where $\mathcal{T}$ is the Bruhat-Tits tree of $\mathrm{PGL}(2, K_\infty)$, see [15] V, Appendix, for details. More precisely, we have $g(X_\Gamma) = h_1(\Gamma \setminus \mathcal{T})$ (= first Betti number of $\Gamma \setminus \mathcal{T}$), and the cusps of X_Γ are in bijection with the ends of $\Gamma \setminus \mathcal{T}$. Their calculation may therefore be carried out on the graph $\Gamma \setminus \mathcal{T}$, which is the point of view of [17].
(iii) The numbers of C_∞-rational (= $K_+(N)$-rational) cusps are calculated

- in [11] sect. 3.4 for $X_0(N)$, based on (6.4)(a);
- in [17] (2.14)–(2.16) for $X_0(N)$ and in [17] (5.2)(iii) for $X_1(N)$, based on approach (6.4)(b), and making use of our present remark (ii).

(iv) Note that the group we here call $\Gamma_1(N)$ is the group labelled $\Gamma_1^*(N)$ in [17].
(v) We take here the opportunity to rectify a misprint in [17] prop. 5.2(iii)(b). The formula in line 7 should read

$$\frac{\varphi(n)}{(q-1)^2}\prod_{\substack{1\le i\le s\\ 0<h_i<r_i}}\frac{q_i-1}{q_i},$$

i.e., the condition on i that $0 < h_i < r_i$ has erroneously been suppressed. The following formulas, in particular the one in line 11, are correct.
(vi) If N has no prime divisors of degree one, the numbers of K-rational

cusps simplify to $\frac{\varphi(N)}{q-1}$ for $X_1(N)$ and 2^s for $X_0(N)$. The special role of $q=2$ results from $\varphi(N) = 1 = q-1$ for $N = T, T-1, T(T-1)$ in this case.
(vii) The numbers of K-rational cusps stated in propositions 6.6 and 6.7 are so far nowhere in the literature. In order to obtain them, we must analyze the canonical maps between the double cosets in (6.2) and (6.3), respectively. This is again unpleasant but elementary, and is therefore omitted. However, for the convenience of the reader who wishes to check the calculations, we state below the two lemmas 6.10 and 6.11, which give the essential intermediate steps between #{cusps} and #{K-rational cusps}.

(6.9) For $M \in A$, let $h_i(M) \in \{0, 1, \dots, r_i\}$ be the truncated P_i-adic valuation of M, that is $h_i(M) = j$ if $P_i^j \| M$ and $j < r_i$, and $h_i(M) = r_i$ if $P_i^{r_i} | M$. For $x = (U, V) \in (A/N)^2_{\text{prim}}$, we put $h_i(x) := h_i(V)$ and $\underline{h}(x) := (h_1(x), \dots, h_s(x)) \in \mathbb{N}_0^s$, which is invariant under the action of $\mathbb{F}_q^*$ on $(A/N)^2_{\text{prim}}$. We specify which x under (3.6), (6.2) and (6.3) give rise to K-rational cusps of $X_1(N)$ or $X_0(N)$.

6.10 Lemma. *An element $x = (U, V)$ of $(A/N)^2_{\text{prim}}$ gives rise to a rational cusp of $X_1(N)$ if and only if*

either:	$\underline{h}(x) = (0, \dots, 0)$ *(i.e., V is a unit in A/N)*
or:	*there exists precisely one i $(1 \le i \le s)$ such that $h_i(x) > 0$, and then $h_i(x) = 1$ and $q_i = q$*
or:	*$q = 2$, and there are precisely two i such that $h_i(x) > 0$, and then $h_i(x) = 1$ and $q_i = q = 2$.*

6.11 Lemma. *Some x as above gives rise to a rational cusp of $X_0(N)$ if and only if the following holds: for each i $(1 \le i \le s)$, $h_i(x) \in \{0, r_i\}$ or $(d_i = \deg P_i = 1$ and $h_i(x) \in \{1, r_i - 1\})$, and there exists at most one i $(q > 2)$ or at most two i $(q = 2)$ such that $h_i(x) \notin \{0, r_i\}$.*

7. Number of elliptic points.

In a similar fashion, starting with (3.7), we calculate the numbers of elliptic points. Again, we content ourselves with writing down the results. The cases $X(N)$ and $X_1(N)$ are trivial or easy, respectively; the more complicated case of $X_0(N)$ has been treated in [11], pp. 77/78.

$$\#\{\text{elliptic points of } X(N)\} = [G'(N) : S] = \frac{\varphi(N)\epsilon(N)|N|}{q+1} \tag{7.1}$$

7.2 Proposition. *$X_1(N)$ has precisely $\frac{\varphi(N)\epsilon(N)}{q^2-1}$ elliptic points. These are all ramified over $X(1)$ with ramification index $q+1$.*

7.3 Proposition. *The number of elliptic points of* $X_0(N)$ *is* $\frac{\epsilon(N)+qr(N)2^{s(N)}}{q+1}$. *Among these, there are* $r(N)2^{s(N)}$ *unramified over* $X(1)$, *the others are ramified with index* $q+1$.

7.4 Remark. Similar to our investigation of cusps, we could work out the fields of definition of the elliptic points of $X(N)$, $X_1(N)$, $X_0(N)$. Both the statements and the proofs would require more material about the arithmetic of Drinfeld modules. Since we are mainly interested in the rationality of the corresponding points reduced modulo P, for which other arguments are available (see sect. 9), we reserve this for future work.

8. Genus formulas.

Using again the arithmetic functions introduced in (1.5), we can express the genera of our Drinfeld modular curves as follows.

8.1 Theorem.

(i) $g(X(N)) = 1 + \frac{\varphi(N)\epsilon(N)(|N|-q-1)}{q^2-1}$

(ii) $g(X_1(N)) = 1 + \frac{\varphi(N)}{(q^2-1)(q-1)}[\epsilon(N) - (q+1)(q-2+\prod_{1\le i\le s}(r_i+1-\frac{r_i-1}{q_i}))]$

(iii) $g(X_0(N)) = 1 + \frac{\epsilon(N)-(q+1)\kappa(N)-2^{s-1}[r(N)q(q-1)+(q+1)(q-2)]}{q^2-1}$

8.2 Remarks. (i) It follows from the description of the function fields of $X(N)$, $X_1(N)$, $X_0(N)$ over C_∞ and over $K_+(N)$, K, respectively, that these curves are conservative, i.e., their genera do not change under constant field extensions. A formal proof of this fact can be found in [27]. We therefore simply write $g(X)$ for the genus of such a curve X without specifying the field of constants.
(ii) Uniform proofs of the three formulas that use remark 6.8(ii) are given in [17] sections 2 and 5. These proofs depend on knowledge of the structure of the graphs $\Gamma \setminus \mathcal{T}$. In that paper, the fibers of the ramified graph coverings $\Gamma \setminus \mathcal{T} \longrightarrow \Gamma(1) \setminus \mathcal{T}$ are calculated for $\Gamma = \Gamma(N)$, $\Gamma_1(N)$, $\Gamma_0(N)$. The formula for $g(X(N)) = h_1(\Gamma(N) \setminus \mathcal{T})$ may also be found in [29] II 2.7. Proofs that avoid reference to the equality "$g(X_\Gamma) = h_1(\Gamma \setminus \mathcal{T})$" and work directly on the modular curve are given in [18] theorem 4.4 and [11] Satz 3.4.8 for $X(N)$ and in [11] Satz 3.4.18 for $X_0(N)$. These proofs are based on the Riemann-Hurwitz formula and proposition 8.3 below. It states that the canonical coverings of Drinfeld modular curves have the least amount of cuspidal ramification allowed by the group-theoretical structure of stabilizers of cusps. Since the only possible ramification is at the elliptic points (where it

is tame in view of $[S : Z] = q+1$) or at cusps, we can first calculate $g(X(N))$ from the covering $X(N) \longrightarrow X(1) = \mathbb{P}^1$ and then $g(X_\Gamma)$ from $X(N) \longrightarrow X_\Gamma$. Again, by lack of symmetry, the case of $X_0(N)$ is the most involved.

The next proposition, which is Satz 3.4.7 of [11], might be useful also for other purposes. We therefore state it separately.

8.3 Proposition. *Let x be a cusp of $X(N)$ and $\mathcal{G}_x$ its stabilizer in $\mathcal{G} := \mathrm{Gal}(X(N)/X(1)) = G'(N)/Z$. Then the second ramification group* ([28] IV) *$\mathcal{G}_{x,2}$ is trivial.*

Since all the cusps of $X(N)$ are conjugate under $\mathcal{G}$, we can restrict to considering $x = \infty$, in which case $\mathcal{G}_x = G'(N)_\infty/Z = H(N)/Z$, and for divisibility reasons, the first ramification group $\mathcal{G}_{x,1}$ is its p-Sylow subgroup $U(N) \cdot Z/Z$.

9. The elliptic argument.

Let P be a monic prime of A coprime with N. We put $\mathbb{F}_P^{(2)}$ for the quadratic extension of $\mathbb{F}_P = A/P$.

9.1 Proposition. *Suppose that P has odd degree. Then all the elliptic points of $X_0(N)/\mathbb{F}_P$ are $\mathbb{F}_P^{(2)}$-rational.*

Proof. Let x be such a point. Using the interpretation of $X_0(N)/\mathbb{F}_P$ as a coarse moduli scheme, x is represented by a triple (ϕ, u, ϕ'), where
(a) ϕ and ϕ' are rank-two Drinfeld A-modules over $\mathbb{F}_P^{\mathrm{alg}}$ with j-invariants $j(\phi) = j(\phi') = 0$, and
(b) $u : \phi \longrightarrow \phi'$ is a separable isogeny with kernel isomorphic with A/N.
This fact (i.e., that any point on the moduli scheme comes from a modular object) is similar to the analogous statement for elliptic curves. In that context, it is proved e.g. in [4] VI prop. 3.2, and the proof given there applies also, *mutatis mutandis*, to our case of Drinfeld modules. (It even drastically simplifies, cf. remark 5.3(ii).) Replacing ϕ and ϕ' by $\mathbb{F}_P^{\mathrm{alg}}$-isomorphic Drinfeld modules if necessary, we can assume that $\phi = \phi'$ and that P acts via ϕ as $\phi_P = F_P^2$, the square of the Frobenius F_P of $\mathbb{F}_P$. Here we use the fact ([12] Satz 5.9) that $j = 0$ is supersingular in characteristic P if $\deg P$ is odd, and therefore ϕ_P is purely inseparable. But then u commutes with F_P^2, i.e., has coefficients in $\mathbb{F}_P^{(2)}$, and x is $\mathbb{F}_P^{(2)}$-rational. $\square$

9.2 Remark. The assertion (9.1) may be considerably generalized, admitting primes P of arbitrary degree and replacing "x elliptic" by "x supersingular", i.e., the point x of $X_0(N)/\mathbb{F}_P$ lies above a point of $X(1)/\mathbb{F}_P$

with supersingular j-invariant ([12] sect. 5). Then again x is $\mathbb{F}_P^{(2)}$-rational, and the same proof works except that the Drinfeld modules ϕ and ϕ' in the triple (ϕ, u, ϕ') representing x are in general non-isomorphic. But still we can achieve $\phi_P = \phi'_P = F_P^2$ by replacing ϕ and ϕ' through suitable $\mathbb{F}_P^{\text{alg}}$-isomorphic modules, which has the same consequence that u has its coefficients in $\mathbb{F}_P^{(2)}$.

10. Conclusion: Asymptotically optimal series of curves over $\mathbb{F}_{q^2}$.

We keep the notation of the last section, i.e., $\mathbb{F}_T^{(2)} \cong \mathbb{F}_{q^2}$ is the quadratic extension of $\mathbb{F}_T$.

10.1 Theorem. *Let $(N_k)_{k\in\mathbb{N}}$ be any series of elements of A that are coprime with T and whose degrees tend to infinity. Then the series of curves $X_0(N_k)/\mathbb{F}_T^{(2)}$ is asymptotically optimal. That is, the ratio*

$$\frac{\#\{\mathbb{F}_T^{(2)} - \textit{rational points of } X_0(N_k)/\mathbb{F}_T\}}{g(X_0(N_k))} \quad \textit{tends to } q-1.$$

Proof. The precise value of $g(X_0(N_k))$ is given by (8.1)(iii); it is $\frac{\epsilon(N_k)}{q^2-1} + 0(|N_k|^{1/2})$, where $\epsilon(N_k) \geq |N_k|$. On the other hand, by (5.2), (7.3) and (9.1), we have $\frac{1}{q+1}[\epsilon(N_k) + qr(N_k)2^{s(N_k)}]$ $\mathbb{F}_T^{(2)}$-rational elliptic points and by (5.1) and (6.7) a certain number of $\mathbb{F}_T^{(2)}$-rational cusps on $X_0(N_k)/\mathbb{F}_T$, that is, more than $\epsilon(N_k)/(q+1)$ $\mathbb{F}_T^{(2)}$-rational points. We conclude with the Drinfeld-Vladut bound (0.3). $\square$

10.2 Example. Let $N_k = P^k$, where $P \neq T$ is a prime of degree one, e.g. $P = T - 1$. Then our formulas yield:

$$g(X_0(N_k)) = 1 + \tfrac{q^{k-1}-q}{q-1} - \begin{cases} 2\frac{q^{\frac{k-1}{2}}-1}{q-1} & k \text{ odd} \\ \frac{q^{\frac{k}{2}}+q^{\frac{k}{2}-1}-2}{q-1} & k \text{ even,} \end{cases}$$

$$\#\{\mathbb{F}_T^{(2)} - \text{rational points of } X_0(N_k)/\mathbb{F}_T\} \geq q^{k-1} + 4 \text{ if } k \geq 3.$$

The tower formed of the $X_0(N_k)$ is very close to Garcia-Stichtenoth's tower [9]. In particular, explicit equations for the $X_0(N_k)$ may be worked out without too much difficulty. For some related considerations, see Elkies' forthcoming paper [7].

10.3 Remark. Whereas towers $X_0(N_k)$ as in (10.1) are *asymptotically* optimal, the individual curves $X_0(N)/\mathbb{F}_T$ fail to present particularly high ratios $\#\{\mathbb{F}_T^{(2)} - \text{rational points}\}$ / genus for small genera g. For $g \leq 50$, these

ratios are usually in the range of 50–80% of the maximal values allowed e.g. by the tables in [10].

(10.4) In the following table, we present a few values for the curves of example 10.2, for $q = 2$ and 3, augmented by the maximal number known so far of $\mathbb{F}_{q^2}$-rational points for the given pair (q, g), and the theoretical upper bound for that number. The latter data are taken from [10].

Table:	k	$g(X_0(T^k))$	$\#\{\mathbb{F}_{q^2}$-rational points$\}$ larger or equal to	maximal # known	upper bound
$q = 2$	3	1	8	9	9
	4	3	12	14	14
	5	9	20	26	26
	6	21	36	41	47
	7	49	68	81	90
$q = 3$	3	2	13	20	20
	4	8	31	38	47
	5	42	85	118	161

References

[1] S. Bae: On the modular equation for Drinfeld modules of rank 2, J. Numb. Th. **42** (1992), 123–133.

[2] S. Bae and S. Lee: On the coefficients of the Drinfeld modular equation, J. Numb. Th. **66** (1997), 85–101.

[3] P. Deligne and D. Husemöller: Survey of Drinfeld modules, Contemp. Math. **67** (1987) 25–91.

[4] P. Deligne and M. Rapoport: Les schémas de modules de courbes elliptiques, Lecture Notes in Mathematics **349**, Springer 1973.

[5] V.G. Drinfeld: Elliptic modules, Math. USSR–Sbornik **23** (1976), 561–592.

[6] V.G. Drinfeld and S.G. Vladut: On the number of points of an algebraic variety, Funct. Analysis Appl. **17** (1983), 53–54.

[7] N.D. Elkies: Explicit towers of Drinfeld modular curves, Preprint Harvard University 2000.

[8] J. Fresnel and M. van der Put: Géométrie analytique rigide et applications, Progress in Mathematics **18**, Birkhäuser 1981.

[9] A. Garcia and H. Stichtenoth: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, Invent. Math. **121** (1995), 211–233.

[10] G. van der Geer and M. v.d. Vlugt: Tables of curves with many points, *http://www.wins.uva.nl/∼geer*.

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

[12] E.-U. Gekeler: Zur Arithmetik von Drinfeld-Moduln, Math. Ann. **262** (1983), 167–182.

[13] E.-U. Gekeler: Modulare Einheiten für Funktionenkörper, J. reine angew. Math. **348** (1984), 94–115.

[14] E.-U. Gekeler: Über Drinfeld'sche Modulformen vom Hecke-Typ, Comp. Math. **57** (1986), 219–236.

[15] E.-U. Gekeler: Drinfeld modular curves, Lecture Notes in Mathematics **1231**, Springer 1986.

[16] E.-U. Gekeler: On the coefficients of Drinfeld modular forms, Invent. Math. **93** (1988), 667–700.

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

[18] D. Goss: π-adic Eisenstein series for function fields, Comp. Math. **41** (1980), 3–38.

[19] D. Goss: The algebraist's upper half-plane. Bull AMS NS **2** (1980), 391–415.

[20] D. Goss: Basic structures of function field arithmetic, Ergeb. d. Math. **35**, Springer 1996.

[21] D. Hayes: Explicit class field theory for rational function fields, Trans. AMS **189** (1974), 77–91.

[22] Y. Ihara: Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Tokyo **28** (1981), 721–724.

[23] Y. Manin and S.G. Vladut: Linear codes and modular curves, J. Sov. Math. **30** (1985), 2611–2643.

[24] M. van der Put: The structure of Ω and its quotients $\Gamma \setminus \Omega$, in: Drinfeld modules, modular schemes and applications, E.-U. Gekeler et al. (eds.), World Scientific 1997.

[25] M. van der Put and J. Top: Algebraic compactification and modular interpretation, in: Drinfeld modules, modular schemes and applications, E.-U. Gekeler et al. (eds.), World Scientific 1997.

[26] A. Schweizer: On the Drinfeld modular polynomial $\Phi_T(X, Y)$, J. Numb. Th. **52** (1995), 53–68.

[27] A. Schweizer: Hyperelliptic Drinfeld modular curves, in: Drinfeld modules, modular schemes and applications, E.-U. Gekeler et al. (eds.), World Scientific 1997.

[28] J-P. Serre: Corps locaux, Hermann 1968.

[29] J-P. Serre: Trees, Springer 1980.

[30] J-P. Serre: Sur le nombre de points rationnels d'une courbe algébrique sur un corps fini, C.R. Acad. Sci. Paris **296** (1983), 397–402.

[31] M.A. Tsfasman, S.G. Vladut and Th. Zink: Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound, Math. Nachr. **109** (1982), 21–28.

[32] M.A. Tsfasman and S.G. Vladut: Algebraic-geometric codes, Kluwer 1991.

[33] J.-K. Yu: A class number relation over function fields, J. Numb. Th. **54** (1995), 318–340.