Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Preprint

Asymptotically optimal towers of curves over finite fields

Ernst-Ulrich Gekeler

Preprint No. 52

Saarbrücken 2002

Universität des Saarlandes

Fachrichtung 6.1 – Mathematik

Asymptotically optimal towers of curves over finite fields

Ernst-Ulrich Gekeler

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

submitted: February 19, 2002

Preprint No. 52

Saarbrücken 2002

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/

Asymptotically optimal towers of curves over finite fields

Ernst-Ulrich Gekeler

In friendship to Prof. Shreeram Abhyankar on the occasion of his 70^{th} birthday

1. Introduction

We let $N_q(g)$ be the maximal number of $\mathbb{F}_q$-rational points of a (smooth, projective, geometrically connected) algebraic curve X over the finite field $\mathbb{F}_q$. It is bounded by (see [24])

$$N_q(g) \leq q + 1 + g[2q^{1/2}]; \tag{1.1}$$

sharper estimates have been given by Ihara [18] and Oesterlé-Serre (*loc. cit.)*. On the other hand, if $(X_k)_{k \in \mathbb{N}}$ is a series of curves over $\mathbb{F}_q$ whose genera $g(X_k)$ tend to infinity, the ratio of numbers $N(X_k)$ of rational points and $g(X_k)$ satisfies

$$\limsup \frac{N(X_k)}{g(X_k)} \leq q^{1/2} - 1, \tag{1.2}$$

as has been proved by Drinfeld and Vladut [3]. Several authors have shown that equality can be achieved whenever q is a square; whether or not this holds for non-squares q is an open question. A series (X_k) of curves $X_k/\mathbb{F}_q$ that realizes the upper bound $q^{1/2} - 1$ is called *asymptotically optimal.* Such a series has been constructed through explicit equations by Garcia and Stichtenoth [5]. Namely, putting

$$F_1 := \mathbb{F}_{q^2}(x_1) \tag{1.3}$$

and for $k \geq 2$,

$$F_k := F_{k-1}(z_k),$$

where $z_k^q + z_k = x_{k-1}^{q+1}$, $x_k := z_k/x_{k-1}$, the fields F_k are the function fields of an a.o. series of curves X_k over $\mathbb{F}_{q^2}$. The curves X_k have been identified by Elkies as cyclic coverings of rather special Drinfeld modular curves [4]. In fact, all the known examples of a.o. series of curves are derived from some sort of (classical elliptic, Shimura, or Drinfeld) modular curves.

In the present contribution we will show that an arbitrary series of (Drinfeld or elliptic) modular curves $X_k = X_0(N_k)$ of Hecke type almost inevitably is asymptotically optimal. The results (Theorem 2.16 and 3.2) are far more complete in the case of Drinfeld modular curves, where we can give precise formulas for the relevant quantities, mainly the numbers of $\mathbb{F}_{q^2}$-rational points. This is why we focus on that case; quite generally, Drinfeld modular curves are somewhat simpler to manipulate compared to their elliptic counterparts. In particular, the appearance of non-abelian automorphism groups of some elliptic curves creates obstacles for calculating the precise numbers of rational points of elliptic modular curves reduced modulo the primes $p = 2$ or 3. The study of these cases, mathematically the most interesting, remains for future work.

2. Some data for Drinfeld modular curves

We recall the ingredients necessary to describe Drinfeld modular curves. Proofs and more detailed explanations may be found e.g. in [14], [9], [10], [11], [27]. See also [12] for some related questions. We put

$$
(2.1)\qquad
\begin{array}{lcl}
\mathbb{F}_q & = & \text{finite field with } q \text{ elements, of characteristic } p,\\
A & = & \mathbb{F}_q[T], \text{ the polynomial ring, and}\\
K & = & \mathbb{F}_q(T), \text{ the field of rational functions over } \mathbb{F}_q,\\
K_\infty & = & \mathbb{F}_q((T^{-1})), \text{ the completion of } K \text{ at its infinite}\\
 & & \text{place, supplied with its absolute value ``} |\ .\ | \text{''},\\
C_\infty & = & \text{the completed algebraic closure of } K_\infty,\\
\Omega & = & C_\infty - K_\infty, \text{ the Drinfeld upper half-plane,}\\
 & & \text{acted upon by the modular group}\\
\Gamma(1) & = & \mathrm{GL}(2,A), \text{ through } \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)(z) = \frac{az+b}{cz+d}.
\end{array}
$$

For some monic $N \in A$, we let

$$
\begin{array}{lcl}
\Gamma(N) & = & \{\gamma \in \Gamma(1) \mid \gamma \equiv 1 \pmod{N}\} \quad \text{and}\\
\Gamma_0(N) & = & \{\gamma \in \Gamma(1) \mid \gamma \equiv \left(\begin{smallmatrix} * & *\\ 0 & *\end{smallmatrix}\right) \pmod{n}\},
\end{array}
$$

the *full* and the *Hecke congruence subgroup* of conductor N. A *modular form* of weight k for $\Gamma(1)$ is some function $f : \Omega \longrightarrow C_\infty$ that satisfies

$$
(2.2)\qquad
\begin{array}{ll}
\text{(i)} & f(\frac{az+b}{cz+d}) = (cz+d)^k f(z),\ \left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right) \in \Gamma(1);\\
\text{(ii)} & f \text{ is rigid-analytically holomorphic (e.g. [27]; lect. 6, 7).}\\
\text{(iii)} & f \text{ is holomorphic at } \infty \text{ (which here means that}\\
 & f \text{ is bounded on the set } \{z \in \Omega \mid \inf_{x \in K_\infty} |z - x| \geq 1\}).
\end{array}
$$

The main example of modular form (the only one we presently need) is as follows (see [14]). Let

$$
(2.3)\qquad E_k(z) = \sum_{(0,0)\neq(a,b)\in A\times A} \frac{1}{(az+b)^k}
$$

be the *Eisenstein series* of weight k for $\Gamma(1)$. The sum converges for $z \in \Omega$ and $k > 0$, and is non-zero if $k \equiv 0 \pmod{q-1}$. The resulting function E_k is a modular form of weight k. Define further

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

The (g, Δ, j) are similar to the classical elliptic modular forms (g_2, g_3, Δ, j) for $\mathrm{SL}(2, \mathbb{Z})$. In particular, the Drinfeld discriminant Δ vanishes nowhere on Ω, and j defines a biholomorphic isomorphism

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

Let now $\Gamma \subset \Gamma(1)$ be a congruence subgroup, i.e., $\Gamma(N) \subset \Gamma$ for some $N \in A$. In view of (2.5), the set $\Gamma \setminus \Omega$ is the set of C_∞-valued points of some smooth affine algebraic curve Y_Γ:

$$(2.6)\qquad \Gamma \setminus \Omega = Y_\Gamma(C_\infty),$$

which can be defined over a finite extension K_Γ of the field $K = \mathbb{F}_q(T)$. We put X_Γ/K_Γ for the smooth projective model of Y_Γ/K_Γ. Curves of shape Y_Γ or X_Γ are referred to as *Drinfeld modular curves.* The set of C_∞-points of X_Γ is easily described:

$$(2.7)\qquad X_\Gamma(C_\infty) = \Gamma \setminus (\Omega \cup \mathbb{P}^1(K));$$

i.e., the *cusps* = points of $X_\Gamma - Y_\Gamma$ correspond canonically to the orbits of Γ on the projective line $\mathbb{P}^1(K)$.

2.8 Examples. (i) If $\Gamma = \Gamma(1)$ then by (2.5), $Y(1) := Y_{\Gamma(1)}$ is the affine line $\mathbb{A}^1$ and $X(1) := X_{\Gamma(1)} = \mathbb{P}^1$ with coordinate j, and X_Γ has one cusp, corresponding to $j = \infty$.
(ii) If $\Gamma = \Gamma(N)$ for some non-constant $N \in A$, then $X(N) := X_{\Gamma(N)}$ is a Galois cover of $X(1)$ with group $\Gamma(1)/\Gamma(N) \cdot Z \hookrightarrow \mathrm{GL}(2, A/N)/Z$, where $Z \cong \mathbb{F}_q^*$ is the group of scalar matrices with coefficients in $\mathbb{F}_q$. It is ramified above $j = 0$ (i.e., at the *elliptic points* of $X(N)$) and above $j = \infty$ (i.e., at the cusps). The cusps $\Gamma(N) \setminus \mathbb{P}^1(K)$ are in canonical bijection with the set $(A/N)^2_{\mathrm{prim}}/\mathbb{F}_q^*$, where $(A/N)^2_{\mathrm{prim}} = \{(a, b) \in (A/N)^2 \mid aA/N + bA/N = A/N\}$.
(iii) If $\Gamma = \Gamma_0(N)$ then $X_0(N) := X_{\Gamma_0(N)}$ is the quotient of $X(N)$ by the subgroup of upper triangular matrices in $\Gamma(1)/\Gamma(N) \cdot Z$. It is called a Drinfeld modular curve of Hecke type.

We collect some properties of the curves $X_0(N)$ and their “affine parts” $Y_0(N)$.

(2.9) First, $Y_0(N)$ solves a certain moduli problem, which explains the name. Viz., $Y_0(N)(C_\infty)$ corresponds one-to-one to the set of isomorphism classes of triples (ϕ, n, ϕ'), where ϕ and ϕ' are rank-two Drinfeld

A-modules and n is a cyclic isogeny of order N. (For definitions and general properties of Drinfeld modules, see [16] and [27].)

(2.10) All the curves $X_0(N)$ are defined over K and conservative, i.e., their genus is stable in constant field extensions [21]. The function field of $X_0(N)$ over K (or over C_∞) is generated over K (over C_∞) by j and j_N, where $j_N(z) = j(Nz)$. The functions j and j_N satisfy $\Phi_N(j, j_N) = 0$ with the modular polynomial $\Phi_N(X,Y) \in A[X,Y]$, which is symmetric in X, Y and explicitly computable ([1] [20] [17]). It provides a (singular) plane model for $X_0(N)$.

(2.11) $X_0(N)/K$ has good reduction at all primes $P \in A$ with $P \nmid N$. Putting $\mathbb{F}_P = A/(P)$ and L^{alg} for the algebraic closure of the field L, there results a reduction mapping

$$\mathrm{red}:\ X_0(N)(K^{\mathrm{alg}}) \longrightarrow X_0(N)/\mathbb{F}_P(\mathbb{F}_P^{\mathrm{alg}}),$$

which happens to be bijective on cusps (points above $j = \infty$) and on elliptic points (points above $j = 0$). Here $X_0(N)/\mathbb{F}_P$ denotes the curve $X_0(N)$ reduced mod P.

In order to state some quantitative properties, we introduce the following arithmetic functions. Let

$$N = \prod_{1 \le i \le s(N)} P_i^{r_i}$$

be the factorization of the monic $N \in A$ into pairwise different monic primes P_i, of degree d_i. Put $q_i := q^{d_i}$ and

$$(2.12)\qquad \begin{aligned} \varphi(N) &= \prod_i q_i^{r_i-1}(q_i-1) \\ \epsilon(N) &= \prod_i q_i^{r_i-1}(q_i+1) \\ \kappa(N) &= \prod_i (q_i^{[r_i/2]} + q_i^{[(r_i-1)/2]}) \quad (\text{“[.]” = Gauß bracket}) \\ r(N) &= 1, \text{ if all the } d_i \text{ are even, and 0 otherwise,} \end{aligned}$$

$t_i = 0, 1, 2$ if ($d_i = 1$ and $r_i = 1, 2, \ge 3$, respectively) and $t_i = 0$ if $d_i > 1$. Finally, $u(N) = t_1 \cdot t_2$ if ($q = 2$ and $P_1 = T$, $P_2 = T - 1$ are divisors of N), and $u(N) = 0$ otherwise.

2.13 Theorem. *With the above notation, the genus $g_0(N)$ of $X_0(N)$ is given by*

$$g_0(N) = 1 + \frac{\epsilon(N) - (q+1)\kappa(N) - 2^{s(N)-1}[r(N)q(q-1) + (q+1)(q-2)]}{q^2-1}.$$

The number of cusps of $X_0(N)$ is $2^s + \frac{\kappa(N)-2^s}{q-1}$. Among these, precisely $2^s + 2^{s-1}\sum_i t_i + 2^{s-2}u(N)$ are K-rational.

These three formulas are proved in [7] Satz 3.4.18, [13] 2.14–2.16 and [12] 6.3, 6.7, respectively.

Let now $P \in A$ be a monic prime coprime with N. We put $\mathbb{F}_P^{(2)}$ for the quadratic extension of $\mathbb{F}_P = A/(P)$ and $\mathbb{F}_P^{\mathrm{alg}}$ for its algebraic closure. Upon reducing modulo P, we get a curve $X_0(N)/\mathbb{F}_P$, on which a certain number of $\mathbb{F}_P^{(2)}$-rational points may be predicted.

(2.14) We let $\Sigma(P) \hookrightarrow \mathbb{F}_P^{\mathrm{alg}}$ be the set of *supersingular Drinfeld j-invariants* in characteristic P (see [8] and [10]). It is known (*loc. cit.*) that $\Sigma(P)$ is contained in $\mathbb{F}_P^{(2)}$ and has cardinality $(q^d-1)/(q^2-1)$ or $(q^d-q)/(q^2-1)+1$ if $d = \deg P$ is even or odd, respectively. Further, $0 \in \Sigma(P)$ if and only if d is odd.

2.15 Proposition. *Let $x \in X_0(N)/\mathbb{F}_P(\mathbb{F}_P^{\mathrm{alg}})$ be a supersingular geometric point, i.e., one above a supersingular point $s \in \Sigma(P) \hookrightarrow X(1)/\mathbb{F}_P(\mathbb{F}_P^{\mathrm{alg}}) \xrightarrow[j]{\cong} \mathbb{P}^1(\mathbb{F}_P^{\mathrm{alg}})$. Then x is already defined over $\mathbb{F}_P^{(2)}$.*

Proof. Here we assume the reader familiar with Drinfeld modules and their moduli theory. The point x is represented by a triple (ϕ, u, ϕ'), where ϕ and ϕ' are supersingular rank-two Drinfeld A-modules over $\mathbb{F}_P^{\mathrm{alg}}$ and $u : \phi \longrightarrow \phi'$ is a cyclic isogeny of order N. If F and F' denote the respective $\mathbb{F}_P$-Frobenius endomorphisms of ϕ and ϕ', then $F^2 = a \cdot \phi_P$, $F'^2 = a' \cdot \phi'_P$ with automorphisms a of ϕ and a' of ϕ'. Here ϕ_P resp. ϕ'_P describe the actions of P via the Drinfeld module structure ϕ resp. ϕ'. Recall that $\mathrm{Aut}(\phi) = \mathbb{F}_q^*$ if $j(\phi) \neq 0$ and $\mathrm{Aut}(\phi) = \mathbb{F}_{q^2}^*$ if $j(\phi) = 0$. In view of (2.14), we may assume that ϕ and ϕ' are defined over $\mathbb{F}_P^{(2)}$. Replacing ϕ and ϕ' by twists over $\mathbb{F}_P^{(2)}$ if necessary, we can achieve that moreover $a = 1 = a'$. The resulting triple (ϕ, u, ϕ') still represents the same point x of the modular curve. Now we see from $u \circ \phi_P = \phi'_P \circ u = u \circ F^2 = F'^2 \circ u$ that u has its coefficients in $\mathbb{F}_P^{(2)}$, and thus $x \in X_0(N)/\mathbb{F}_P(\mathbb{F}_P^{(2)})$. $\square$

The genus $g_0(N)$ of $X_0(N)/\mathbb{F}_P$ is given by (2.13), and (2.15) yields a lower bound for its number of $\mathbb{F}_P^{(2)}$-rational points. This suffices for the following assertion.

2.16 Theorem. *Let $(N_k)_{k\in\mathbb{N}}$ be a series of elements of A coprime with the prime P, and whose degrees tend to infinity. Then the series of curves $X_0(N_k)/\mathbb{F}_P$ is asymptotically optimal over $\mathbb{F}_P^{(2)}$.*

Proof. (i) Let $d = \deg P$. By (2.13), $g_0(N_k)$ is $\epsilon(N)/(q^2-1)+$ terms of smaller order of magnitude. We are thus done if we show that the number $\#_k$ of $\mathbb{F}_P^{(2)}$-rational points of $X_0(N_k)/\mathbb{F}_P$ satisfies

$$(*) \qquad \#_k \geq \frac{q^d-1}{q^2-1}\epsilon(N_k).$$

(ii) The canonical map $X_0(N_k) \longrightarrow X(1)$ has degree $\epsilon(N_k)$ and is unramified above $(j \neq 0, \infty)$. Above the point $(j = 0)$ of $X(1)$, there are precisely $r(N_k)2^{s(N_k)}$ geometric points of $X(N_k)$ which are unramified and $[\epsilon(N_k) - r(N_k)2^{s(N_k)}]/(q+1)$ points which are ramified with index $q+1$ ([7] p. 77/78). As follows from the interpretation of our curves as moduli schemes, this pattern remains unchanged upon reducing $(\mathrm{mod}\ P)$, i.e., for $X_0(N_k)/\mathbb{F}_P \longrightarrow X(1)/\mathbb{F}_P$. Hence we get

$$[\#(\Sigma(P)) - 1]\epsilon(N_k) + \frac{\epsilon(N_k) + qr(N_k)2^{s(N_k)}}{q+1} \quad \text{if } d := \deg P \text{ is odd,}$$

and

$$\#(\Sigma(P))\epsilon(N_k) \quad \text{if } d \text{ is even}$$

for the number of supersingular geometric points on $X_0(N_k)/\mathbb{F}_P$. These are all $\mathbb{F}_P^{(2)}$-rational by (2.15). In both cases (d even/odd), our inequality $(*)$ holds, as was to be shown. $\square$

2.17 Remark. Via reduction $(\mathrm{mod}\ P)$, the rational cusps of $X_0(N)/K$ yield $\mathbb{F}_P$-rational cusps of $X_0(N)/\mathbb{F}_P$. Their number is given by (2.13), taking (2.11) into account. While their asymptotic contribution is negligible, their presence is responsible for a certain number of record curves for fixed parameters q and g (see section 4). On the other hand, cusps of $X_0(N)/\mathbb{F}_P$ which are rational over $\mathbb{F}_P^{(2)}$ but not over $\mathbb{F}_P$ can occur only in very restricted cases.

3. Classical elliptic modular curves

The following well-known heuristical principle is frequently and fruitfully applied to shift information (in both directions) between the "characteristic zero" and the "characteristic $p > 0$" world: The data in the left and right column play similar parts in the respective arithmetics of $\mathbb{Q}$ and of $K = \mathbb{F}_q(T)$. (3.1)

Number field side		Function field side
$\mathbb{Q}$		$K = \mathbb{F}_q(T)$
$\mathbb{Z}$		$A = \mathbb{F}_q[T]$
$\mathbb{R}$, "$\lvert\,.\,\rvert$" = archimedean absolute value		K_∞, "$\lvert\,.\,\rvert$" = non-archimedean absolute value
$H =$ complex upper half-plane		$\Omega =$ Drinfeld upper half-plane
$\Gamma(1) = \mathrm{SL}(2, \mathbb{Z})$	modular group	$\Gamma(1) = \mathrm{GL}(2, A)$
$\Gamma(N)$, $\Gamma_0(N)$, $N \in \mathbb{N}$		$\Gamma(N)$, $\Gamma_0(N)$, $N \in A$
elliptic curves		Drinfeld A-modules of rank two
$X(N) = \Gamma(N) \setminus (H \cup \mathbb{P}^1(\mathbb{Q}))$		$X(N) = \Gamma(N) \setminus (\Omega \cup \mathbb{P}^1(K))$
	full level modular curves	
$X_0(N)$		$X_0(N)$
	elliptic/Drinfeld modular curves of Hecke type	
elliptic modular forms		Drinfeld modular forms
g_2, g_3, $\Delta = q\Pi(1-q^n)^{24}$, j		g, Δ, j as in (2.4)

For an extension of the table, which includes e.g. the arithmetic of cyclotomic extensions of $\mathbb{Q}$ and of K, see the book [16]. But there are also limitations to the analogy. For example, the elliptic modular curve $X(N)$ is defined over the N-th cyclotomic field $\mathbb{Q}(N) = \mathbb{Q}(e^{2\pi i/N})$, while the Drinfeld modular curve $X(N)$ is defined over $K_+(N)$, the counterpart of the maximal real subfield $\mathbb{Q}_+(N)$ of $\mathbb{Q}(N)$ (see [9]).

As a positive example, we translate Theorem 2.16 to classical modular curves. Of course, there is an abundance of old and new publications about this topic, but surprisingly, our Theorem 3.2 below seems not to have been recognized and explicitly stated before in the literature. In [26], only a special case is mentioned. Let us first fix some notation; our standard reference here is Shimura's book [25].

For $N \in \mathbb{N}$, let $X_0(N)$ be the elliptic modular curve of Hecke type of conductor N. It is a smooth projective curve over $\mathbb{Q}$ with set of $\mathbb{C}$-points $X_0(N)(\mathbb{C}) = \Gamma_0(N) \setminus (H \cup \mathbb{P}^1(\mathbb{Q}))$. If $p \in \mathbb{N}$ is a prime coprime with N then $X_0(N)$ has good reduction $(\bmod\ p)$, which yields a curve $X_0(N)/\mathbb{F}_p$.

3.2 Theorem *Let $(N_k)_{k\in\mathbb{N}}$ be a series of natural numbers coprime with the prime p and tending to infinity. Then the series of curves $X_0(N_k)/\mathbb{F}_p$ is asymptotically optimal over $\mathbb{F}_{p^2}$.*

Proof. The structure of proof is identical, *mutatis mutandis*, with that of (2.16), so we restrict to sketch the principal points.
(i) The genus of $X_0(N)$ is given in [25], Propositions 1.40 and 1.43, pp. 23–26. It is

$$g(X_0(N)) = \frac{\epsilon(N)}{12} + O(N^{1/2}\log\ N),$$

where $\epsilon(N) = \deg(X_0(N) : X(1)) \geq N$ is the obvious $\mathbb{Z}$-analogue of the former $\epsilon(N)$.
(ii) All the supersingular geometric points of $X_0(N)/\mathbb{F}_p$ are defined over $\mathbb{F}_{p^2}$. This is shown like (2.15); see [26] for a special case.
(iii) It now suffices to show that the number $\#(N)$ of supersingular points of $X_0(N)/\mathbb{F}_p$ satisfies

$$(*) \qquad \#(N) \geq \frac{p-1}{12}\epsilon(N).$$

(iv) The number $\#(1)$ of supersingular j-invariants in characteristic p is given by $\#(1) = 1$ for $p = 2$ and 3 and $\#(1) = \frac{p-1}{12}, \frac{p+7}{12}, \frac{p+5}{12}, \frac{p+13}{12}$ for $p \equiv 1, 5, 7, 11 \pmod{12}$. Some supersingular point $j \in X(1)/\mathbb{F}_p(\overline{\mathbb{F}}_p)$ is unramified in

$$\alpha_N :\ X_0(N)/\mathbb{F}_p \longrightarrow X(1)/\mathbb{F}_p$$

if j is non-elliptic, i.e., if $j \neq 0, 1728$. For such j, we have $\#(\alpha_N^{-1}(j)) = \epsilon(N)$.
(v) Let first $p > 3$, so $0 \neq 1728 \in \mathbb{F}_p$. Then $j = 0$ is supersingular if and only if $p \equiv 5, 11 \pmod{12}$, in which case $\#(\alpha_N^{-1}(j = 0)) \geq \frac{\epsilon(N)}{3}$, since all the points above $j = 0$ are ramified with index 1 or 3.
Similarly, $j = 1728$ is supersingular if and only if $p \equiv 7, 11 \pmod{12}$, in which case $\#(\alpha_N^{-1}(j = 1728)) \geq \frac{\epsilon(N)}{2}$, since the possible ramification indices are 1 or 2.
In all four cases, we get $\geq \frac{p-1}{12}\epsilon(N)$ supersingular points on $X_0(N)/\mathbb{F}_p$, i.e., $(*)$ holds.
(vi) Next, we consider the case $p = 2$. The only supersingular invariant is $j = 0$. The geometric automorphism group of an associated elliptic curve has order 24 (in fact, it is isomorphic with $\mathrm{SL}(2, \mathbb{F}_3)$, see [2]), hence all the points in $\alpha_N^{-1}(j = 0)$ are ramified with index a divisor of 12, which gives $\#(\alpha_N^{-1}(j = 0)) \geq \frac{\epsilon(N)}{12} = \frac{p-1}{12}\epsilon(N)$.

(vii) Finally, for $p=3$, the automorphism group corresponding to the only supersingular invariant $j=0$ has order 12, and so $\#(\alpha^{-1}(j=0)) \geq \frac{\epsilon(N)}{6} = \frac{p-1}{12}\epsilon(N)$. $\square$

3.3 Remark. The practical importance of (2.16) is in applying it with a prime P of degree one, without restriction, $P=T$ or $T-1$. Then it produces a wealth of essentially different asymptotically optimal series $(X_k)_{k\in\mathbb{N}}$ over $\mathbb{F}_P = \mathbb{F}_q$. Applying it to primes P of degree $d>1$ yields curves $X_k/\mathbb{F}_{q'}$ $(q'=q^d)$, which in general seem to have less rational points over $\mathbb{F}_{q'}^{(2)}$ than curves constructed over the same field with a prime P of degree one.

The situation is different with Thm. 3.2, since unlike the function field case, we cannot reduce the study of curves over $\mathbb{F}_{p'}$ with "large" primes p' to the study of such over $\mathbb{F}_p$ with "small" primes p through "base extension".

4. Examples

We restrict to presenting examples derived from (2.16) and some complementary results of Andreas Schweizer [23].

(4.1) We first let $P=T-1$ (then $\mathbb{F}_P=\mathbb{F}_q$) and $N_k=T^k$ $(k\geq 3)$. From (2.16),

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

and the number of supersingular points on $X_0(N_k)/\mathbb{F}_{T-1}$ is q^{k-1}. Depending on k and q, there are also some cusps on $X_0(N_k)/\mathbb{F}_{T-1}$ which are $\mathbb{F}_T^{(2)}$-rational (in most cases, already $\mathbb{F}_T$-rational). We give a few values, which show that the curves so found are not bad but fail to be optimal. The last two columns contain the maximal numbers known of rational points of curves for the given (q,g) and the theoretical upper bounds. These are taken from [6].

4.2 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	14	14	14
	5	9	24	26	26
	6	21	40	41	47
	7	49	72	81	90
$q=3$	3	2	13	20	20
	4	8	34	38	47
	5	32	91	92	130

We can considerably optimize the ratio $\frac{\text{rational points}}{\text{genus}}$, and effectively find some record curves, by passing from $X_0(N)$ to its quotient $X_+(N)$ by its canonical involution. We briefly describe the construction and some of its output. The theory necessary to determine the invariants of $X_+(N)$ has been developed by A. Schweizer, to whose papers [19] [20] [21] [22] [23] we refer for proofs, background, and more examples.

(4.3) Let $N \in A = \mathbb{F}_q[T]$ be non-constant and monic. On the modular curve $X_0(N)$ we have the *Fricke* or Atkin-Lehner involution $w = w(N)$, which may be described either through the matrix $\left(\begin{smallmatrix} 0 & 1 \\ N & 0 \end{smallmatrix}\right) \in \mathrm{GL}(2,K)$ (which normalizes $\Gamma_0(N)$ and therefore induces an involution on $\Gamma_0(N) \setminus (\Omega \cup \mathbb{P}^1(K)) = X_0(N)(C_\infty)$) or through its action on the objects of the moduli problem for $X_0(N)$. It is compatible with reduction (mod P) and therefore yields an involution $\overline{w} = \overline{w}(N)$ on $X_0(N)/\mathbb{F}_P$. Since the $X_0(N)$ are ordinary, the Hurwitz formula gives

$$g(X_+(N)) = \frac{1}{2}[g(X_0(N)) + 1 - a \cdot \#\{\text{fixed points of } w\}]$$

with $a = 1$ in characteristic two and $a = \frac{1}{2}$ otherwise. On the other hand,

$$\#\{\mathbb{F}_P^{(2)}\text{-rational points on } X_+(N)/\mathbb{F}_P\} \geq \\ \tfrac{1}{2}\#\{\mathbb{F}_P^{(2)}\text{-rational points of } X_0(N)/\mathbb{F}_P\}.$$

Hence the ratio becomes larger for $X_+(N)/\mathbb{F}_P$, and it is reasonable to search for "good" curves among them. Several problems arise:

(a) What is the number of fixed points of w?
(b) Describe the "reduction (mod P)-mapping" on fixed points!
(c) Which ones of the fixed points of $\overline{w}$ are $\mathbb{F}_P^{(2)}$-rational?

The numbers in (a) can be expressed through class numbers of A-orders in certain quadratic extensions L of K (see [19]), and are difficult to control in general. But in characteristic two, the relevant field L

becomes the inseparable extension $K(\sqrt{T}) = \mathbb{F}_q(\sqrt{T})$ of K, where the class number problem collapses, and Schweizer found an explicit formula (Lemma 3 in [23]) for the number in question. As to (b) and (c), although it seems difficult to give a uniform description, the number of different $\mathbb{F}_P^{(2)}$-rational fixed points of $\overline{w}$ can be calculated in all cases of modest size. As a result, we cite the following two examples from [23]. Both these curves realize the maximal number of rational points presently known for their parameters.

(4.4) Let $q = 2$ and $N = T^5(T^2+T+1)$. The curve $X_+(N)/\mathbb{F}_{T-1}$ has genus 27 and at least 50 rational points over $\mathbb{F}_{T-1}^{(2)} \cong \mathbb{F}_4$.

(4.5) Let $q = 4$ and $N = T^5+T^3+T+1$. The curve $X_+(N)/\mathbb{F}_T$ has genus 34 and at least 161 rational points over $\mathbb{F}_T^{(2)} \cong \mathbb{F}_{16}$.

4.6 Remark. Following the above strategy, one finds that for $q = 2$ the curves $X_+(T^{k+1})$ and $X_0(T^k)$ have the same genus (given in (4.1)). It deserves further investigation whether this is coincidence or has a structural reason. While the series $(X_0(T^k))$ has the advantage of being even a tower (which fails to hold for $(X_+(T^{k+1}))_{k\in\mathbb{N}}$), the $X_+(T^{k+1})/\mathbb{F}_{T-1}$ present slightly more (viz., $\geq 2^{k-1}+2^{k/2-1}+4$) rational points over $\mathbb{F}_{T-1}^{(2)}$, as compared to $2^{k-1}+8$ for $X_0(T^k)/\mathbb{F}_{T-1}$ ($k \geq 6$ even).

References

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

[2] P. Deligne: Courbes elliptiques: Formulaire, Lecture Notes in Mathematics **476**, Springer Verlag 1975.

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

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

[5] 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.

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

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

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

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

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

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

[12] E.-U. Gekeler: Invariants of some algebraic curves related to Drinfeld modular curves, J. Numb. Th., to appear.

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

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

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

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

[17] Liang-chung Hsia: On the coefficients of modular polynomials for Drinfeld modules, J. Numb. Th. **72** (1998), 236–256.

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

[19] A. Schweizer: Zur Arithmetik der Drinfeld'schen Modulkurven $X_0(\mathfrak{n})$, Doctoral dissertation Saarbrücken 1996.

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

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

[22] A. Schweizer: On elliptic curves over function fields of characteristic two, J. Numb. Th. **87** (2001), 31–53.

[23] A. Schweizer: On Drinfeld modular curves with many rational points over finite fields, manuscript Taipei 2000.

[24] 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.

[25] G. Shimura: Introduction to the arithmetic theory of automorphic functions, Publ. Math. Soc. Japan **11**, Tokyo–Princeton 1971.

[26] 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.

[27] Drinfeld modules, modular schemes, and applications, E.-U. Gekeler et al. (eds.), World Scientific 1997.