Trends in Mathematics
Information Center for Mathematical Sciences
Volume 4, Number 2, December 2001, Pages 1–6

SOME APPLICATIONS OF DRINFELD MODULAR CURVES

ANDREAS SCHWEIZER

Abstract. We give a somewhat informal account of some recent applications of Drinfeld modular curves to the classification of elliptic curves over $\mathbb{F}_q(T)$ and to the construction of curves over finite fields with many rational points.

Being asked to write a short survey article on my research, I have decided to concentrate on some applications of Drinfeld modular curves outside the theory of Drinfeld modules. I hope this will make the subject also interesting to people who are not directly working on number theoretic aspects of function fields.

1. A very brief review of Drinfeld modular curves. Throughout this paper we denote by A the polynomial ring $\mathbb{F}_q[T]$ over the finite field $\mathbb{F}_q$ with q elements and by K the quotient field $\mathbb{F}_q(T)$.

The well-known analogy between A and $\mathbb{Z}$ and between their quotient fields K and $\mathbb{Q}$ can be extended much further. The completion $K_\infty = \mathbb{F}_q((\frac{1}{T}))$ of K at the "infinite" place ∞ (= degree valuation) is an analogue of $\mathbb{R}$. And the completion C_∞ of an algebraic closure of K_∞ is a field that is complete and algebraically closed and plays the role of $\mathbb{C}$. Finally, $\Omega = C_\infty - K_\infty$ is called the Drinfeld upper halfplane. (Actually this is more like $\mathbb{C} - \mathbb{R}$, the union of the complex upper and lower halfplane.) For $\mathfrak{n} \in A$ the group

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

acts on Ω through $\binom{a\ b}{c\ d} z = \frac{az+b}{cz+d}$.

We would like to have an analytic structure on Ω which makes the quotient space $\Gamma_0(\mathfrak{n})\backslash\Omega$ into something like a Riemann surface over C_∞. This is definitely more complicated than in the case of classical modular curves. Since the points of K_∞ are scattered all over C_∞, we cannot use everywhere convergent power series like the Fourier expansion of modular forms and modular functions on the complex upper halfplane. On the other hand, being locally expandable in a power series is much too weak a notion, since Ω as a topological space is totally disconnected.

To make things work one has to use a rigid analytic structure, i.e., defining holomorphy locally with respect to a very restricted system of open subsets. We refer to [GeRe] and the Alden Biesen proccedings [AB] for an extensive treatment of this aspect.

It turns out that the rigid analytic space $\Gamma_0(\mathfrak{n})\backslash\Omega$ can be compactified by adding a finite number of "cusps", namely the orbits of $\mathbb{P}^1(K) \subseteq \mathbb{P}^1(C_\infty)$ under the action

2000 *Mathematics Subject Classification.* 11G09, 11G05, 11G20,14G15.

Key words and phrases. Drinfeld modular curve, elliptic curve, curves with many points, asymptotically optimal towers.

Received May 2, 2001.

of $\Gamma_0(\mathfrak{n})$. As in the classical theory, this compact "Riemann surface" over C_∞ then is equivalent to a smooth, projective, algebraic curve over C_∞, the Drinfeld modular curve $X_0(\mathfrak{n})$.

Gekeler has given a closed formula for the genus of $X_0(\mathfrak{n})$, investigating the ramification of the covering $X_0(\mathfrak{n}) \to X_0(1) \cong \mathbb{P}^1$. This is more difficult than for the classical modular curves, because the cusps may be wildly ramified. He also showed that as an algebraic curve $X_0(\mathfrak{n})$ is already defined over the field K.

In this paper we are only interested in $X_0(\mathfrak{n})$ as an algebraic curve over K. Once the most important properties of $X_0(\mathfrak{n})$ are established, many things (for example the applications we want to discuss) can be done without recurrence to its analytic origins. We refer to [Ge4] for an account of all important facts on Drinfeld modular curves without ballast.

However, one word of warning is in order. By its construction via $\Gamma_0(\mathfrak{n})$ the curve $X_0(\mathfrak{n})$ is associated to a ring $A = \mathbb{F}_q[T]$, and each q has its own Drinfeld modular curves. For example, the Drinfeld modular curve $X_0(T^3)$ for $q = 2$ considered as a curve over $\mathbb{F}_4(T)$ is not the Drinfeld modular curve $X_0(T^3)$ for $q = 4$. To see this just note that the genus of $X_0(T^3)$ is $q - 1$.

As for classical modular curves, the main interest in Drinfeld modular curves comes from their moduli interpretation. Namely, the points of $\Gamma_0(\mathfrak{n}) \backslash \Omega$ represent Drinfeld modules with some additional structure. We suppress discussing this point here, since it would require developing some details on Drinfeld modules. One important fact, coming from this moduli interpretation, is that $X_0(\mathfrak{n})$ has good reduction at all "finite" places of K that do not divide $\mathfrak{n}$.

2. Applications to elliptic curves. We write the conductor of an elliptic curve E over $K = \mathbb{F}_q(T)$ multiplicatively. Thus it has the form $cond(E) = \infty^e \cdot \mathfrak{n}$ with $e \geq 0$ and a monic $\mathfrak{n} \in A$. The exponent of a place v in $cond(E)$ is 0, 1, or $2 + f_v$, respectively, depending on whether E has good, multiplicative, or additive reduction at v. Here f_v is a measure of the wild ramification of the Galois representation. Actually, $f_v = 0$ if the characteristic is ≥ 5. But in characteristic 2 and 3 it can be arbitrarily large, although there is a congruence condition in characteristic 3 ([Ge3]). If an equation of E is given, $cond(E)$ can be calculated mechanically by Tate's algorithm [Ta].

The connection between elliptic curves over K and Drinfeld modular curves is established by the following theorem, which is actually older than Wiles' famous paper on the modularity of elliptic curves over $\mathbb{Q}$.

Theorem. *Every elliptic curve E over K with conductor $\infty \cdot \mathfrak{n}$ and split multiplicative reduction at ∞ is an isogeny factor of the Jacobian $J_0(\mathfrak{n})$ of the Drinfeld modular curve $X_0(\mathfrak{n})$.*

The condition $cond(E) = \infty \cdot \mathfrak{n}$ is not as restrictive as it might at first appear. If $j(E) \notin \mathbb{F}_q$, then we can find a quadratic twist E' of E which has multiplicative reduction at some place $\mathfrak{p}$. Say $deg(\mathfrak{p}) = d$. Over $\mathbb{F}_{q^d}(T)$ the prime divisor $\mathfrak{p}$ decomposes into prime divisors of degree 1, and using a Moebius transformation we can map one of these to ∞.

The theorem is discussed in great detail in [GeRe] and in [Ge1]. It allows to find (the isogeny classes of) the elliptic curves over $\mathbb{F}_q(T)$ with conductor $\infty \cdot \mathfrak{n}$

by splitting $J_0(\mathfrak{n})$ into its factors. This can be done in practice, for fixed q and $\mathfrak{n}$ provided they are not too big, by diagonalizing certain operators on the homology of an almost finite graph associated to the group $\Gamma_0(\mathfrak{n})$. We won't need this in the sequel and therefore refrain from giving the quite involved details. But see the examples at the end of [GeRe] and [Ge1].

More interesting than the calculation of isolated examples is finding explicit equations for a whole series, e.g. for all curves with given places of bad reduction. This was first done in [Ge2], where all elliptic curves in characteristic 2 with conductor $\infty \cdot T^n$ were described. The principal idea, which is also central to all subsequent papers, is that one should first control the zeroes and poles of the possible j-invariants.

Of course, every pole of $j(E)$ is a place of bad reduction. And in characteristic 2 and 3 the zeroes of $j(E)$ which are not places of bad reduction are precisely the places of supersingular reduction of E. This follows immediately from the fact that 0 is the only supersingular invariant in these characteristics.

Now let E be an elliptic curve over K with $cond(E) = \infty \cdot \mathfrak{n}$. We may assume (possibly after an unramified quadratic twist) that E has split multiplicative reduction at ∞. If $\mathfrak{p}$ is a place of supersingular reduction of E, then the Jacobian $J_0(\mathfrak{n})$, of which E is an isogeny factor, cannot have ordinary reduction at $\mathfrak{p}$. Thus the first step (and the main difficulty) is to control the places of non-ordinary reduction of $X_0(\mathfrak{n})$.

Lemma. [Ge3] *The Drinfeld modular curves $X_0(T^n)$ have good and ordinary reduction at all places different from ∞ and T.*

Since the covering $X_0(T^{n+1}) \to X_0(T^n)$ is not galois for $q > 2$, this has to be proved by an induction process involving a somewhat more complicated Drinfeld modular curve than $X_0(T^n)$.

Corollary. [Ge3] *If the characteristic of $\mathbb{F}_q$ is 2 or 3, then every elliptic curve E over K with conductor $\infty \cdot T^n$ has j-invariant εT^m with a positive integer m and $\varepsilon \in \mathbb{F}_q^*$.*

Proof: $j(E)$ must have a pole at ∞. And since there are no places of supersingular reduction, the only possible zero is T.

Once one has enough control over the j-invariant, one can use certain normal forms, twists, and the Tate-algorithm [Ta] to find explicit equations. We explain this on a simple example.

In characteristic 3 every elliptic curve E with non-zero j-invariant has a model

$$Y^2 = X^3 + \alpha X^2 - \frac{\alpha^3}{j(E)}.$$

Over K we can assume that the twist α lies in A and is squarefree.

Now in our situation $j(E) = \varepsilon T^m$, if m is divisible by 3, then E is obtained via Frobenius from another elliptic curve E' over K which has the same conductor and $j(E') = \delta T^{\frac{m}{3}}$. So we can suppose $3 \not| m$.

If $\mathfrak{p}$ is a prime divisor of α, then the curve $Y^2 = X^3 + \alpha X^2 - \frac{\alpha^3}{\varepsilon T^m}$ has bad reduction at $\mathfrak{p}$; and if $\alpha = T$ (up to a unit), then the reduction at ∞ is additive. Hence we are left with $\alpha \in \mathbb{F}_q^*$, and one easily checks that in this case the conductor is $\infty \cdot T^{m+2}$. Thus we have shown

Proposition. [Ge3] *Elliptic curves E over fields $\mathbb{F}_q(T)$ of characteristic 3 with cond$(E) = \infty \cdot T^n$ exist if and only if $n \not\equiv 2$ mod 3 and $n \geq 3$. They have the form*

$$Y^2 = X^3 + \alpha X^2 - \frac{\alpha^3}{\varepsilon T^{n-2}}$$

with $\alpha, \varepsilon \in \mathbb{F}_q^*$.

In [Sch1] we gave explicit equations for all elliptic curves in characteristic 2 with conductor $\infty \cdot \mathfrak{n}$ where $deg(\mathfrak{n}) = 3$. In order to control the places of supersingular reduction we used the fact that in this case the curves $X_0(\mathfrak{n})$ are hyperelliptic. Despite its late publication this paper was written before [Sch2], where we describe the elliptic curves with conductor $\infty \cdot T^n(T-1)$.

The most recent of these papers, [Sch3], favours a completely elementary approach, which ironically works much better. The title of that paper comes from the fact that the results can be reinterpreted in terms of elliptic surfaces.

The central point, somewhat hidden amidst all the calculations, is Lemma 2.4. Roughly, it tells us that if k is any perfect field of characteristic 2 or 3, and E is any elliptic curve over $k(T)$, then the mere knowledge of the bad places of E suffices to effectively and explicitly control the possible zeroes and poles of $j(E)$.

Although this supersedes all results obtained with the help of Drinfeld modular curves, one can clearly say that it ultimately owes its existence to the inspiration drawn from the Drinfeld modular curve approach.

The method of [Sch3] has not been fully exploited yet, in the sense that for some further types of conductors one would only need the patience to carry out the calculations in order to explicitly write down all equations.

Contrary to what is sometimes believed, wild ramification doesn't seem to cause additional problems. Rather, the complexity of the calculations is governed by the squarefree kernel of the conductor, that is, by the number of bad places over $\overline{\mathbb{F}_q}(T)$.

3. Applications to curves with many points.

It is standard to denote the maximal possible number of $\mathbb{F}_q$-rational points on a curve of genus g over $\mathbb{F}_q$ by $N_q(g)$. A classical result assures that

$$N_q(g) \leq q + 1 + 2g\sqrt{q}.$$

But in general this bound is not sharp, as can be seen for example from the following asymptotic result:

$$\limsup_{g\to\infty} \frac{N_q(g)}{g} \leq \sqrt{q} - 1 \quad \text{(Drinfeld-Vladut bound)}.$$

Consequently, a sequence $\{X_k\}$ of curves over $\mathbb{F}_q$ with $g(X_k) \to \infty$ is called asymptotically optimal if $\lim\limits_{k\to\infty} \frac{\#(\mathbb{F}_q-rational\ points\ of\ X_k)}{g(X_k)} = \sqrt{q} - 1$.

All known asymptotically optimal towers are related to reductions of (classical, Shimura or Drinfeld) modular curves (compare [E]).

In general it is not easy to write down an equation for a modular curve. But the moduli interpretation allows to predict certain points, in particular the supersingular points (see [Ge5]), which is exactly what tends to make the reductions asymptotically optimal.

Theorem. [Ge5] *Let $\mathfrak{p} \in A$ be irreducible and let $\{\mathfrak{n}_k\}$ be a sequence of polynomials in A with $\mathfrak{p} \not| \mathfrak{n}_k$ and $\lim\limits_{k\to\infty} deg(\mathfrak{n}_k) = \infty$. Then the sequence of curves $X_0(\mathfrak{n}_k)$ mod $\mathfrak{p}$ is asymptotically optimal over the quadratic extension of $A/\mathfrak{p}$.*

In recent years there has been renewed interest in the construction of curves over finite fields with many rational points. We refer to [vGvV] for a long list of references and for a table with the known records in the range $g \leq 50$ and q a small power of 2 or 3.

Admittedly, the fact that a sequence $\{X_k\}$ is asymptotically optimal implies literally nothing for an individual curve from this sequence. But morally it is a good candidate for a curve with many points.

It seems that reductions of Drinfeld modular curves $X_0(\mathfrak{n})$ have not been investigated under this aspect before, and it looks as if they do in general not give the best results. We know only one case that beats the records in [vGvV], namely

Example. If $q = 3$, the Drinfeld modular curve $X_0(T^3(T+1)^2)$ has genus 42. Its reduction modulo $T-1$ has at least 122 rational points over the quadratic extension of $\mathbb{F}_3[T]/(T-1)$. Namely, by [Ge4, Propositions 7.3 and 9.1] there are 108 elliptic points, and one can check that all 14 cusps also become rational.

The best known result in [vGvV] for a curve of genus 42 over $\mathbb{F}_9$ is 118 rational points.

The central idea in [Sch4] is the following: If we can divide an already good curve of genus g with n rational points by an involution which has many fixed points, then the number of rational points on the quotient curve will be at least $\frac{1}{2}n$, but by the Hurwitz formula the genus will be smaller than $\frac{1}{2}g$. So the quotient curve will have a better ratio $\#\{\textit{rational points}\}/\textit{genus}$.

This is not guaranteed to make things any better, because for smaller genus we actually need a better ratio. Indeed, it is very plausible, at least from the tables in [vGvV], that the function $\frac{N_q(g)}{g}$ is monotonely decreasing from almost $(\sqrt{q}+1)^2$ for $g = 1$ to $\sqrt{q} - 1$. But it is worth a try, especially if many of the fixed points of the involution are rational, which further increases the ratio.

On $X_0(\mathfrak{n})$ we have the Atkin Lehner involution $W_\mathfrak{n}$. The formula for the number of its fixed points involves class numbers of quadratic orders over A, which makes calculations somewhat awkward. But in characteristic 2 one can unwrap the class numbers and give an explicit formula. Another delicate point is that fixed points might fall together on the reduction. See [Sch4] for a precise treatment.

Anyhow, one can calculate the genus of $X_+(\mathfrak{n}) := W_\mathfrak{n}\backslash X_0(\mathfrak{n})$ and predict certain points on its reductions. Searching for cases where $W_\mathfrak{n}$ has many fixed points, we could improve 3 of the entries in [vGvV].

Example. [Sch4] If $q = 2$, the curve $X_+(T^5(T^2+T+1))$ has genus 27 and at least 50 rational points over the quadratic extension of $\mathbb{F}_2[T]/(T+1)$ (i.e. over $\mathbb{F}_4$), one more than the record in [vGvV].

References.

[AB] *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

[E] N. Elkies: Explicit towers of Drinfeld modular curves, *preprint* arXiv:math.NT/0005140 v2 24May2000

[Ge1] E.-U. Gekeler: Jacquet-Langlands theory over K and relations with elliptic curves, *in* [AB], pp. 224-257

[Ge2] E.-U. Gekeler: Highly ramified pencils of elliptic curves in characteristic two, *Duke Math. J.* **89** (1997), 95-107

[Ge3] E.-U. Gekeler: Local and global ramification properties of elliptic curves in characteristics two and three, *in: Algorithmic Algebra and Number Theory,* (B. H. Matzat, G.-M. Greuel, G. Hiß, eds.), Springer, Berlin-Heidelberg-New York, 1998, pp. 49-64

[Ge4] E.-U. Gekeler: Invariants of some algebraic curves related to Drinfeld modular curves, *J. Number Theory,* **90** (2001), 166-183

[Ge5] E.-U. Gekeler: Asymptotically optimal towers of curves over finite fields, *in: Proceedings of the Conference on Algebra and Algebraic Geometry (Abhyankar 70),* Purdue 2000, Springer-Verlag, to appear

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

[vGvV] G. van der Geer and M. van der Vlugt: Tables of curves with many points, *Math. Comp.* vol. 69, number 230, (2000), 797-810
Updated version at: `http://www.wins.uva.nl/~geer`

[Sch1] A. Schweizer: On elliptic curves over function fields of characteristic two, *J. Number Theory* **87** (2001), 31-53

[Sch2] A. Schweizer: On elliptic curves in characteristic 2 with wild additive reduction, *Acta Arith.* **91** (1999), 171-180

[Sch3] A. Schweizer: Extremal elliptic surfaces in characteristic 2 and 3, *Manuscripta Math.* **102** (2000), 505-521

[Sch4] A. Schweizer: On Drinfeld modular curves with many rational points over finite fields, *submitted*

[Ta] J. Tate: Algorithm for determining the type of a singular fiber in an elliptic pencil, *Modular Functions of One Variable IV,* Springer LNM 476, Berlin-Heidelberg-New York, 1975, pp. 33-52

Korea Institute for Advanced Study (KIAS) 207-43 Cheongryangri-dong, Dongdaemun-gu Seoul 130-012, Korea

E-mail address: `schweiz@kias.re.kr`