Elliptic curves in function field arithmetic

Dinesh S. Thakur[1]

Abstract: We will describe the theory of elliptic curves and Drinfeld modules in the function field setting. Both of these objects share some of the properties of the elliptic curves familiar in the number fields setting. There are some interesting contrasts as well as interaction between them. We develop the basics, describe analogies, give examples and survey and compare the main results and some open questions.

By a function field, we will mean a function field of one variable over a finite field, i.e., a finite extension of some $\mathbb{F}_q(t)$. Number theory studies number fields and function fields together as global fields. By a theorem of Artin and Whaples [A], the global fields are essentially the only fields having the notions of various sizes (or absolute values) linked by a product formula and having at least one discrete prime divisor with finite number of residue classes.

In view of the various analogies that exist inspite of some basic differences (in the characteristic, in the existence or non-existence of archimedian places or in the possibilities of differentiation), the back and forth interaction helps separate the relevant issues, suggests conjectures and techniques to solve them. We are going to restrict to the issues surrounding elliptic curves.

We will see that in function field arithmetic, two separate objects, elliptic curves over function fields themselves and Drinfeld modules, share the properties of elliptic curves over number fields.

We will assume familiarity with the basics of the theory of elliptic curves over a field, and will only compare the main results and questions in the number field case (references for which can be found in [Si], [T3]) with those in the function field case.

But we will not assume familiarity with Drinfeld modules and hence we will give a quick introduction to Drinfeld modules. (For

[1]Supported in part by NSF and NSA grants

2000 *Mathematics subject classification.* Primary: 11G05, 11G09.

more detailed accounts, see [D1, D2, DH] and the books [Go2, GoHR, GPRG, G1, Lau]).

1. Notation and basic analogies

We let

$\mathbb{F}_q$: a finite field of characteristic p having q elements

X: a smooth, complete, geometrically irreducible curve over $\mathbb{F}_q$

K: the function field of X

∞: (a distinguished) degree one place of K (degree assumption is only for simplicity)

A: the ring of elements of K with no pole outside ∞

K_∞: the completion of K at ∞

C_∞: the completion of an algebraic closure of K_∞

A_v: the completion of A at a place $v \neq \infty$

We will consider ∞ to be distinguished place at infinity and call the other places v the finite places. They can be given by a (nonzero) prime ideal $\wp$ of A.

Then C_∞ is known to be both complete and algebraically closed. We can think of analogs

$$K \leftrightarrow \mathbb{Q}, \quad A \leftrightarrow \mathbb{Z}, \quad K_\infty \leftrightarrow \mathbb{R}, \quad C_\infty \leftrightarrow \mathbb{C}$$

Instead of $\mathbb{Q}$ we can also have an imaginary quadratic field with its unique infinite place and the corresponding data.

We will see that analogies are even stronger when X is the projective line over $\mathbb{F}_q$ and the usual ∞, so that $K = \mathbb{F}_q(t)$, $A = \mathbb{F}_q[t]$, $K_\infty = \mathbb{F}_q((1/t))$.

The Dedekind domain A sits discretely in K_∞ with compact quotient, in analogy with $\mathbb{Z}$ inside $\mathbb{R}$ or the ring of integers of imaginary quadratic field inside $\mathbb{C}$.

2. Drinfeld modules

The abelian algebraic groups, such as those provided by points of multiplicative group, elliptic curves or abelian varieties, are $\mathbb{Z}$-modules and by the analogy above we will seek algebraic groups which are A-modules. Then we can talk about a torsion for $a \in A$, instead of n-torsion for $n \in \mathbb{Z}$ and can hope to get $\wp$-adic Galois representations, for $\wp$ a prime of A in a similar fashion to p-adic representations obtained via Tate modules.

Since p is zero in A, to embed it in the endomorphism ring, instead of the multiplicative group, the algebraic group we use is the additive group. Being in characteristic p, now it has a huge (non-commutative) endomorphism ring $F\{\tau_p\}$ consisting a polynomials in p-th power map τ_p (which is additive in characteristic p).

Since A is not a canonical base like $\mathbb{Z}$, we decree it to be a base by giving an A-field structure of F, i.e., a homomorphism $\iota : A \to F$. The kernel of ι is called the characteristic of ι, in analogy with the classical situation. The characteristic is a prime ideal $\wp$ of A. (A simple example of characteristic $\wp$ situation would be $F = A/\wp$ with ι, the canonical map). If it is the zero ideal, ι is called of generic characteristic to avoid confusion with field-theoretic zero characteristic. Non-generic characteristic is also called finite characteristic. Unless otherwise stated, when we use extensions such as K, K_∞, C_∞ of K as our F, we assume that ι is the usual embedding.

Definition: Let F be an A-field (also called a field over A) $\iota : A \to F$ of characteristic $\wp$. Then Drinfeld A-module over F (of characteristic $\wp$) is a ring homomorphism $\rho : A \to F\{\tau_p\}$, (we write ρ_a for the image of $a \in A$) with the coefficient of τ^0 in ρ_a being $\iota(a)$ and which is non-trivial in the sense that it does not factor through F, i.e., $\rho \neq \iota$.

In fact, ρ is injective. Hence, Drinfeld A-modules are essentially just non-trivial embeddings of A's into the non-commutative ring $F\{\tau_p\}$ or just non-trivial A-module structures on the additive group in characteristic p. If we let $\tau := \tau_q$ to denote the q-th power map, then the image of ρ is inside $F\{\tau\}$ (defined similarly as above) and it is a $\mathbb{F}_q$-algebra homomorphism.

We put $\deg(x) = -d_\infty v_\infty(x)$ and $|x|_\infty = q^{\deg(x)}$ as usual, so that for $a \in A$, we have $|a|_\infty = |A/a|$.

It can be shown that there is a positive integer r with the property that $\deg_\tau(\rho_a) = r\deg(a)$ for all $a \in A$. It is called the *rank* of ρ.

For ρ of finite characteristic $\wp$, there is a positive integer h with the property that $\mathrm{ord}_\tau(a) = hv_\wp(a)\deg(\wp)$ for all $a \in A$. It is called the *height* of ρ.

Definition A *morphism* $\phi : \rho \to \rho'$ between two Drinfeld A-modules over F is $\phi \in F\{\tau\}$ such that $\phi\rho_a = \rho_a\phi$ for all $a \in A$. A non-zero morphism is called an *isogeny*. An invertible morphism is called an isomorphism.

A simple count of degrees shows that isogenies can occur only among Drinfeld modules of the same rank and characteristic.

Examples: (1) Let $A = \mathbb{F}_q[t]$. As t generates A over $\mathbb{F}_q$, a general Drinfeld A-module ρ over F, of rank r over F can be fully described by $\rho_t = \sum_{i=0}^{r} f_i \tau^i$, where $f_i \in F$, f_r is non-zero and $f_0 = \iota(t)$. It is of generic characteristic, if f_0 is transcendental over $\mathbb{F}_q$. If $f_0 = 0$, it is of characteristic t. More generally, if $\wp$ is the minimal polynomial of f_0 over $\mathbb{F}_q$, then it is of characteristic $\wp$. The rank one module $C_t = t + \tau$ of generic characteristic is called Carlitz module, after Carlitz who developed it in 1930's. It is isomorphic to $\rho_t = t + f_1\tau$ by the isomorphism $f_1^{1/(q-1)}$, which in general is defined only over an extension of $\mathbb{F}_q(t, f_1)$. So there is only one isomorphism class of rank one A-modules of generic characteristic in this case of $A = \mathbb{F}_q[t]$, which is of class number one.

(2) Let $A = \mathbb{F}_2[x, y]$ with $y^2 + y = x^3 + x + 1$. Then we have $h_A = d_\infty = g = 1$ and $\deg(x) = 2$, $\deg(y) = 3$. Then, as x and y generate A over $\mathbb{F}_2$, $\rho_x = x + (x^2 + x)\tau + \tau^2$ and $\rho_y = y + (y^2 + y)\tau + x(y^2 + y)\tau^2 + \tau^3$ defines a rank one generic characteristic Drinfeld A-module over A, because it is easy to see that using the commutation relations that $\rho_x \rho_y = \rho_y \rho_x$ and of course, $\rho_{y^2+y} = \rho_{x^3+x+1}$. Here and sometimes below, by abuse of notation, we will use identification by dropping ι from notation.

We repeat the *basic analogies*: For $a \in A$, $x \mapsto \rho_a(x)$ is analog of power or multiplication maps $x \mapsto x^n$, $P \mapsto [n]P$ for multiplicative group or elliptic curves respectively, as well as complex multiplication map $P \mapsto z \circ P$ for complex multiplications z. The first and third analogy is strongest for the rank one situation, whereas the second one for the rank two. The higher rank theory has no straight analog in the classical case.

3. Analytic description

One way to show quickly that Drinfeld modules exist in abundance for any A, and to draw a parallel with more well-known analytic theory of elliptic curves is the analytic description of Drinfeld modules over C_∞ via lattices.

Definition An A-lattice L is a finitely generated, discrete A-submodule of C_∞ (considered as an A-module with the usual multiplication). Its rank is defined to be the rank of this finitely generated, torsion-free and so projective module. If F is a finite extension of

K_∞ in C_∞, then we say that L is an A-lattice over F, if further, L is contained in F^{sep} and invariant under $\mathrm{Gal}(F^{sep}/F)$.

Important thing to notice is that, unlike the classical case over $\mathbb{C}$, where the lattices can have only rank one or two, as $[\mathbb{C}:\mathbb{R}]=2$, now lattices of arbitrarily high rank do exist.

Similar to Weierstrass theory, we can associate the so-called exponential function $e_L(z) := z\prod'_{l\in L}(1-z/l)$ to a lattice L. The discreteness immediately implies that the product converges for all z, giving us an entire (and thus surjective, see the last section) function. Further, writing it as a limit over finite products, where we restrict the product over $\mathbb{F}_q$-vector space of l's of degree less than a given bound (to get $\mathbb{F}_q$-linear polynomials), we see that $e_L(z)$ is $\mathbb{F}_q$-linear function. Since e_L vanishes on lattice L by construction, it is periodic with L as a period lattice and gives isomorphism from C_∞/L onto C_∞ because of the surjection. Clearly, e_L has coefficients in F.

Theorem 1. *Let F be a finite extension of K_∞ in C_∞. The category of Drinfeld A-modules ρ of rank r over F (so necessarily of generic characteristic) is isomorphic to the category of rank r A-lattices L over F (with morphism from lattice L to L' being z such that $zL\subset L'$).*

Proof: We show how to get from one data to the other and leave the rest as an exercise. Given L, let e_L be the corresponding exponential. For a non-zero a, put

$$\rho_a^L(x) = ax\prod_{0\neq l\in a^{-1}L/L}(1-x/e_L(l)).$$

As A is a Dedekind domain, and L is projective of rank r, L is isomorphic to $A^{r-1}\oplus I$, for a non-zero ideal I of A. This implies that $a^{-1}L/L$ is isomorphic to the sum of r copies of $A/(a)$. Thus $e_L(a^{-1}L/L)$ is a finite $\mathbb{F}_q$-vector space of dimension $r\deg(a)$ and thus $\rho_a(x)$ is a $\mathbb{F}_q$-linear polynomial of degree $q^{r\deg(a)}$. By comparing the divisors and the derivatives (i.e., the linear terms) of the two sides of the following, we get the equality

$$e_L(ax) = \rho_a^L(e_L(x)).$$

Now $\rho_{ab}^L = \rho_a^L\rho_b^L = \rho_b^L\rho_a^L$ follows from applying it to $e_L(x)$ and we see that in fact that ρ_a^L is a Drinfeld module of rank r over F.

Conversely, given ρ, we first show that there exists a corresponding exponential $e(x) = e_\rho(x) = \sum e_i x^{q^i}$, which is, by definition, a $\mathbb{F}_q$-linear entire function satisfying

$$e_\rho(ax) = \rho_a(e_\rho(x)), \text{ for all } a \in A$$

and normalized to have $e_0 = 1$:

First we fix a non-constant a and write $\rho_a = \sum_{i=0}^d a_i \tau^i$. Solving the functional equation $e(x) = \rho_a(e(a^{-1}x))$ formally by equating coefficients we get a unique solution $e_n(a^{q^n} - a) = \sum_{i=1}^n a_i e_{n-i}^{q^i}$, inductively starting with $e_0 = 1$.

Next we show that the functional equation is now automatically satisfied for any $b \in A$: We have $\rho_b e b^{-1} = \rho_b(\rho_a e a^{-1})b^{-1} = \rho_a(\rho_b e b^{-1})a^{-1}$, so that both e and $\rho_b e b^{-1}$ satisfy our functional equation and hence are the same by uniqueness, showing $\rho_b e = eb$, as required.

Next we estimate the coefficient size to show that $e(x)$ converges for all $x \in C_\infty$: Since $a_i = 0$ for $i > d$, for $n \geq d$, we have $e_n(a^{q^n} - a) = \sum_{i=1}^d a_i e_{n-i}^{q^i}$. Write $r_n = |e_n|^{q^{-n}}$. It is enough to show that $r_n \to 0$. Taking q^n-th root of the recursion, we see that $|a| r_n \leq \max(|a_i|^{q^{-n}} r_{n-i})$, so that for large n, $r_n \leq \theta \max_{1 \leq i \leq d} r_{n-i}$, for some $\theta < 1$. This implies $r_n \to 0$ as required. Now define $L = L_\rho$ to be the kernel of e. It is then clearly discrete. By the functional equation of e, it is an A-module. Since $e'(x) = e_0 = 1$, it is in separable closure of F and Galois stable. Separability of e also implies that all the zeros are simple and thus $e_L = e\rho$. Hence ρ_a is given by formula above in terms of L. So $|A/a|^r = |a^{-1}L/L|$ and hence its rank is r.

The morphism corresponding to z is given by the τ polynomial corresponding to ρ_z defined by the formula above. •

From the general description of A-lattices given above, we see that class group acts on isomorphism classes of lattices and thus of Drinfeld modules. In rank one, we see that there are h_A-isomorphism classes of Drinfeld modules over C_∞, one corresponding to each ideal class, parallel to the complex multiplication situation.

Drinfeld A-module over F is an object 'over F with multiplications by A'. If the rank over A is one, it is analogous to complex multiplications by A. On the other hand, as we saw the rank 2 situation is closer to elliptic curves. So, for example, $\rho_t = t + \tau^2$ defines a rank two Drinfeld $\mathbb{F}_q[t]$ module over $\mathbb{F}_q(t)$ (in fact over $\mathbb{F}_q[t]$), which is rank one $\mathbb{F}_{q^2}[t]$ Drinfeld module. In the quadratic extension $\mathbb{F}_{q^2}(t)$

the infinite place extends uniquely in somewhat analogous way to the quadratic imaginary situation. Another example, where the infinite place is ramified rather than inert is rank one $\mathbb{F}_q[\sqrt{t}]$ Drinfeld module $\rho_{\sqrt{t}} = \sqrt{t} + \tau$, considered as complex multiplication for the rank two Drinfeld $\mathbb{F}_q[t]$ module $\phi_t = t + (\sqrt{t} + \sqrt{t}^q)\tau + \tau^2$.

In fact, a good analog of the Chowla-Selberg formula, which expresses the period of the complex multiplication elliptic curves in terms of gamma values at fractions with denominators having to do with the imaginary quadratic fields, is proved in [Th1] (along with generalization to some higher rank situations).

Jing Yu [Y] has proved various analogs of the transcendence theory of periods.

For a fixed a, the coefficient of τ^i in ρ_a, considered as a function of the lattice L corresponding to ρ, is a *modular form* (see below for more analytic details) of weight $q^i - 1$. This follows from the commutation relations $\tau^i c = c^{q^i}\tau^i$. For example, if we write a rank 2 Drinfeld module ρ for $\mathbb{F}_q[t]$ by $\rho_t = t + gF + \Delta F^2$, then as $L \to \lambda L$, $(g, \Delta) \to (\lambda^{1-q}g, \lambda^{1-q^2}\Delta)$ This should be compared with $y^2 = x^3 - g_2 x - g_3$, with modular forms g_2, g_3. See [T3]. In fact, $j := g^{q+1}/\Delta$ is a weight 0 modular function parameterizing the isomorphism classes of these Drinfeld modules, again parallel to the elliptic curve situation. Algebraicity and transcendence properties [Y] of this j-function, as well as factorizations of singular moduli are in parallel with the elliptic curves case. Also note that if Δ vanishes, we get a degeneration (bad reduction) of the Drinfeld module to rank one. This corresponds to the fact that Δ, which plays the role of the discriminant, is a cusp form. (Note that for general A, there are several Δ's, essentially one for each a).

Let us now see how the structural properties of the torsion and endomorphism rings (especially for the rank two) mirror those in the elliptic curves theory.

4. Torsion points

Definition. Let $\rho[a] := \{z \in \overline{F} : \rho_a(z) = 0$ be the set of a-torsion points of ρ, i.e., the kernel of ρ_a. For a (non-zero) ideal I of A, we write $\rho[I] := \{z : \rho_i(z) = 0, \text{for all } i \in I\} = \cap_{i \in I}\rho_i$ be the set of I-torsion points of ρ.

Clearly, $\rho[(a)] = \rho[a]$. Note that 0 is always a-torsion, for any a, just as 1 is n-th root of unity for any n, in the classical case. The torsion is a $\mathbb{F}_q$-vector space and A-module.

If ρ is understood, we sometimes write Λ_a for $\rho[a]$ and λ_a for an a-torsion point, in analogy with the classical notations μ_n and ζ_n or $E[n]$.

For a rank one Drinfeld A-module ρ over an extension of K_∞, with the corresponding period lattice $\tilde{\pi}I$ say, using the corresponding exponential, we can give an analytic description of the torsion module as in the classical case: $\rho[a] = \{e_\rho(\tilde{\pi}b/a)\}$.

We have the following basic simple theorem.

Theorem 2. *Let $\wp$ be a non-zero prime ideal of A. Let d be the dimension of $A/\wp$-vector space $\rho[\wp]$. Then $d = r$, if $\wp \neq char(\rho)$ and $d = r - h$, otherwise.*

In particular, in finite characteristic, just as in the elliptic curves case, if we are in rank 2 situation, we have good reduction for all but finitely many places, and for these we have ordinary and supersingular cases depending on number of torsion points. In higher ranks, as in the abelian varieties, there are intermediate possibilities.

Consider an elliptic curve E over $\mathbb{Q}$. If it has complex multiplications, Deuring proved that it has ordinary reduction for half (in terms of density) the primes and supersingular for the rest of the places of good reduction. See [Si]. On the other hand, Elkies [E] proved the existence of infinitely many supersingular primes in general. In [B2], the existence of infinitely many supersingular primes is proved for 'most' of the rank two, generic characteristic Drinfeld $\mathbb{F}_q[t]$-modules. In [Po3], the list of possible exceptions in [B2] is corrected, examples are provided (eg., $\rho_t = t(1-\tau)^2$) which have no supersingular prime and representation theoretic obstructions (which do not exist for number fields) for infinitude are explained. The general situation is an interesting open question.

5. Explicit class field theory

Let us see how the explicit class field theory works here [H] with rank one Drinfeld modules, now for any K, considered parallel (by choosing only one place at infinity) to the case of rational number field or the imaginary quadratic field. See [S] for the classical case.

At the simplest level, the field of definition of rank one ρ (of generic characteristic) is the Hilbert class field of A, defined as the maximal abelian unramified extension of K in which ∞ splits completely. This should be compared to the way j-invariant of the elliptic curve with complex multiplication generates the Hilbert class field of the complex multiplication field.

One important difference is that though elliptic curves with complex multiplication have potential good reduction, it is usually not achieved over the Hilbert class field, in contrast to the Theorem 15.9 of [H] in the rank one situation. In fact, the coarse moduli of rank one Drinfeld A-modules is the spectrum of the ring of integers of the Hilbert class field of A, but since the Drinfeld modules have non-trivial automorphisms in general (for $q > 2$), that does not even guarantee existence of a Drinfeld module over the Hilbert class field of A. But learning of the Hayes proof (sketched in the letter to the author), Deligne then introduced extra structure to get a fine moduli scheme and thus giving another proof of existence over the ring of integers (i.e., with good reduction at all places).

Now let ϕ be a Drinfeld A-module over F. For an ideal I of A, consider the left ideal of $k\{\tau\}$ generated by ϕ_i, $i \in I$. Since we have a division algorithm, this ideal is principal. We denote its monic generator by ϕ_I. Then $\phi[I]$ is clearly the kernel of ϕ_I.

Then for a normalized rank one ρ, the constant coefficient of ρ_I generates the ideal I in the integral closure of A in this Hilbert class field, thus providing an explicit version of the principal ideal theorem of the class field theory in this situation.

The maximal abelian extension of K is obtained explicitly, by adjoining to K all a-torsion points of suitably normalized rank one A-module ρ (for every non-zero $a \in A$), for two different A's (and corresponding two different ρ's) corresponding to (any) two different places ∞. This should be compared with Kronecker-Weber theorem, as well as situation [S] in complex multiplication theory, where we adjoin (co-ordinates of) n-torsion points.

Drinfeld [D1] obtained the (ring of integers of) the maximal abelian extension totally split at ∞ from a suitable moduli space of rank one Drinfeld A-modules and later [D2] obtained it for the full maximal abelian extension by using certain coverings, by putting in missing 'level structure at ∞'. Hayes produced the first extension by more visible analogy with the classical case [S], as the compositum of all Hilbert class fields for complex multiplication orders.

6. Endomorphisms

Let us start with some simple observations and examples:

Examples: Since $\tau f = f\tau$ for $f \in \mathbb{F}_q$, we have $\mathbb{F}_q^* \subset \mathrm{Aut}(\rho)$ for any ρ. Similarly, $\mathbb{F}_{q^r}^* \subset \mathrm{Aut}(\rho)$, for $\mathbb{F}_q[t]$-module $\rho_t = t + \tau^r$. Also, if ρ is defined over $\mathbb{F}_q$, then $\mathrm{End}_{\mathbb{F}_q}(\rho)$ which, in general, is a subset of (commutative ring) $\mathbb{F}_q\{\tau\}$, in fact, is equal to it.

The definitions immediately show that $\rho(A) \subset \mathrm{End}(\rho)$, just as $\mathbb{Z}$ sits in the endomorphism ring of the multiplicative group or of an elliptic curve. The theorem below immediately implies that for Carlitz module, this is the full ring of endomorphisms, while for $\rho_t = t + \tau^r$, the full ring is $\mathbb{F}_{q^r}[t]$ of rank r over A. We consider this as a complex multiplication analog. Let us consider $\rho_t = \tau^r$ of characteristic t and rank and height equal to r, then we have rank r^2 ring $\mathbb{F}_{q^r}\{\tau^r\}$ in the endomorphism ring.

We have the following basic theorems, as in the elliptic curves case.

Theorem 3. *Given an isogeny $\phi : \rho \to \rho'$, there exists an isogeny $\psi : \rho' \to \rho$ such that $\psi\phi = \rho_a$, and $\phi\psi = \rho'_a$, for some $a \in A$.*

Proof: We only prove this assuming that ϕ is a separable isogeny. Then it is of smallest degree killing its kernel, which is a finite A-module and hence killed by ρ_a for some a. By division algorithm in $F\{\tau\}$, we then see that $\rho_a = \psi\phi$. Now $\psi\rho'\phi = \psi\phi\rho = \rho_a\rho = \rho\rho_a = \rho\psi\phi$, so that $\psi\rho' = \rho\psi$ and ψ is isogeny from ρ' to ρ as claimed. Now $\phi\psi\phi = \phi\rho_a = \rho'_a\phi$, so cancellation gives the second equality. •

Theorem 4. *Let ρ be a Drinfeld A-module over algebraically closed field F of rank r. Then End(ρ) is a projective A-module of rank at most r^2. It is commutative of rank at most r, if ρ is of generic characteristic.*

7. Drinfeld modules over finite fields

Now we focus on Drinfeld modules defined over finite A-fields. Again there are many similarities with the theory of elliptic curves over finite fields, where the theory is simpler because complex multiplication is available. The *Riemann hypothesis* is now a little simpler, almost built in in the formalism.

Let ρ be a rank r Drinfeld A-module of characteristic $\wp$ over F of cardinality q_1, which is then equal to $q^{m \deg \wp}$, where $m = [F :$

$A/\wp]$. We identify A with its image $\rho(A)$ in the non-commutative ring $F\{\tau\}$. Let π be the (q_1-th power) Frobenius endomorphism of ρ. Since π commutes with ρ, $K(\pi)$ is a commutative field, even though $K\{\tau\}$ inside the quotient division ring of $F\{\tau\}$ is, in general, not commutative.

Under the identification of A with its image, ρ_a (choose a non-constant) has the normalized absolute value (controlled by the top τ-degree term $\tau^{r\deg(a)}$) $q^{\deg(a)}$, so that π has (or rather 'should have', as this passage from absolute value to commutative A to commutative $A(\pi)$ inside non-commutative $\mathbb{F}_q\{\tau\}$ needs some justification) absolute value $q_1^{1/r}$.

Note that the weights in rank r are $1/r$, whereas elliptic curves which are of rank 2 give only weight $1/2$.

Since we are in characteristic $\wp$, $\rho_\wp$ has factor τ, so its high power is divisible by π. Hence, π lies over $\wp$.

Hence the norm of π from $K(\pi)$ to K is power of $\wp$, and equals $\wp^{m[K(\pi):K]/r}$ by comparing the degrees. Now π being an endomorphism of A-module of degree r, is integral of degree at most r over A, since its satisfies its characteristic polynomial.

Much more can be proved efficiently and rigorously, as in the elliptic curves case, by using the well-developed theory of skew-fields, division algebras etc. See [D2, G2, Yu, Go2], where the proof of the following main theorem of *Honda-Tate theory* can also be found.

Call an element π of $\overline{K}$ to be a *Weil number* over F of rank r, if (i) it is integral over A, (ii) there is only one place of $K(\pi)$ which is a zero of π and it lies above $\wp$, (iii) there is only one place of $K(\pi)$ above ∞, (iv) $|\pi| = q_1^{1/r}$, where the absolute value is the unique extension to $K(\pi)$ of the normalized absolute value at ∞ of K, (v) $[K(\pi) : K]$ divides r.

Theorem 5. *Frobenius endomorphism over F gives a bijective map from the set of isogeny classes of Drinfeld A-modules of rank r over F (as above) onto the set of conjugacy classes of Weil numbers of rank r.*

Remark: Given a Weil number π, we use its properties to get an embedding of $K(\pi)$ into the quotient division ring of $F\{\tau\}$, which by the restriction to A gives the Drinfeld module with desired properties to show the surjectivity.

8. Rational points

The analogy with elliptic curves suggests studying structure of the set of *rational points* of Drinfeld module ρ. But this is just an additive group of F, considered as A-module via ρ. For a finite extension F of K over which ρ is defined, it is not finitely generated. So we do not have a nice analog of Mordell-Weil theorem giving a finite rank of rational points.

In fact, using the height functions developed by Denis and himself, Poonen [Po1] proved that it is isomorphic to the direct sum of a free module of countable rank with a finite torsion module.

In a major breakthrough study, Mazur had shown boundedness of rational torsion for any elliptic curve over a given number field by studying the rational points on modular curves $X_1(n)$ (whose non-cuspidal points classify elliptic curves with a point of order n) and in particular proved a complete list of possibilities over $\mathbb{Q}$, thus settling Levi-Ogg conjecture. Building on this and work of Kamienny, Merel proved uniform boundedness where we just fix a degree of a number field rather than the number field.

In the Drinfeld modules setting, Poonen [Po2] studied the corresponding questions and proved uniform boundedness for rank one as well as analog of the result of Manin bounding $\wp$-primary part of rational torsion for the rank two $\mathbb{F}_q[t]$-modules over a given F: Having such a $\wp^n$-torsion, gives a F-rational point on Drinfeld modular curve $X_1(\wp^n)$, which has only finitely many F-rational points by analog of Mordell conjecture over function fields proved by Samuel and for each corresponding j-invariant, the rational torsion over the Drinfeld modules having that j is uniformly bounded.

The stronger conjectures are still open.

9. Modular forms

We have already mentioned the coefficients of the Drinfeld modules arising as (C_∞-valued rather than $\mathbb{C}$-valued) modular forms. The automorphic forms considered by Weil, Jacquet, Langlands, Drinfeld are basically $\mathbb{C}$-valued (or F-valued for any characteristic zero field F, since in the absence of archimedian places no growth conditions needed and all arise from those over $\mathbb{Q}$ by tensoring) functions ϕ on $G(K)\backslash G(\mathcal{A})/\mathcal{K}Z(K_\infty)$, where $G = GL_2$ say. See [DH, GR, Te] for the discussion in Drinfeld modules settings as well as comparison.

Following analogies with the classical upper half plane approach, as well as moduli space approach, Goss [Go1, G1] considered C_∞-valued modular forms on Drinfeld upper half-plane $\Omega := C_\infty - K_\infty$ (compare $\mathcal{H}^{\pm} = \mathbb{C} - \mathbb{R}$) in the rank 2 situation which we will focus on. (The automorphic forms, on the other hand, live on a tree (=Bruhat-Tits building for $Gl_2(K_\infty)$= tree of norms) (and its quotients) constructed as a nerve of special covering of Ω. See [D1, DH, Te]).

We replace Ω by $\Omega^{r-1} := \mathbb{P}^{r-1}(C_\infty)$ minus all K_∞-rational hyperplanes, for the general rank r situation.

Put $\mathrm{I}m(z) := \mathrm{I}nf_{x\in K_\infty}|z-x|$. Then $\mathrm{I}m(\gamma z) = |\mathrm{D}et(\gamma)||cz+d|^{-2}\mathrm{I}m(z)$ for $\gamma \in GL_2(K_\infty)$. The sets $\Omega_c := \{z \in \Omega : \mathrm{I}m(z) \geq c\}$ give open admissible neighborhoods of ∞ (not to be confused with the place ∞ of K) in the rigid analytic topology. Ω is connected but not simply connected.

Let e denote the exponential for the Carlitz module, i.e., corresponding to $\Lambda = \tilde{\pi}A$. Then $q_\infty(z) = 1/e(\tilde{\pi}z)$ is a uniformizer which takes a neighborhood of ∞ to the neighborhood of origin and since it is invariant with respect to translations from A, it can be used for q_∞-expansions (analogs of $q = e^{2\pi i z}$-expansions).

Modular form of weight k (nonnegative integer), type m (integer modulo $q-1$ (or rather the cardinality of $\mathrm{D}et(\Gamma) \subset \mathbb{F}_q^*$)) for Γ is $f : \Omega \to C_\infty$ satisfying $f(\gamma z) = (Det(\gamma))^{-m}(cz+d)^{-k}f(z)$, for $\gamma \in \Gamma$ and which is rigid holomorphic and holomorphic at cusps.

Since $dq_\infty = -\tilde{\pi}q_\infty^2 dz$ (in contrast to $dq = (2\pi i)q dz$), the holomorphic differentials correspond to double-cuspidal forms.

The Hecke operators can be defined similarly, but they turn out to be totally multiplicative: The usual term in the recursion relation for $T_{\wp^n}$ involves a multiplication by p, which makes it disappear in our context.

As an analog of the Dedekind product formula for the discriminant modular form $\Delta(z)$ into cyclotomic factors:

$$\Delta(z) = (2\pi i)^{12} q \prod_{n\in\mathbb{Z}_{>0}} (1-q^n)^{24} = (2\pi i)^{12} q \prod ((q^{-n}-1)q^{\mathrm{Norm}(n)})^{24},$$

for the Δ as above, Ernst Gekeler [G3] proved

$$\Delta = -\tilde{\pi}^{q^2-1} q_\infty^{q-1} \prod_{a\in A+} (C_a(q_\infty^{-1})q_\infty^{\mathrm{Norm}(a)})^{(q^2-1)(q-1)}.$$

For $A = \mathbb{F}_q[t]$ and $\Gamma = GL_2(A)$, the algebra of modular forms of type 0 is $C_\infty[g, \Delta]$ and the algebra for all types is $C_\infty[g, h]$, where

h is a Poincare series of type 1 and weight $q+1$ defined by Gekeler [G4]. We have $h^{q-1} = -\Delta$.

Eisenstein series $E^{(k)}(z) = \sum'_{a,b\in A}(az+b)^{-k}$ are of weight k and type 0.

The constant terms, by construction, are zeta values. But in general, the coefficients of q_∞-expansions of modular forms, which are very rich arithmetically in the classical case, are very poorly understood objects so far.

10. Galois representations and Finiteness theorems

For Drinfeld modules over finite fields, the analog of Tate isogeny theorem was proved by Drinfeld. For Drinfeld modules of generic characteristic, the analog of Tate conjecture/Faltings theorem was established by Taguchi [Tag3] and Tamagawa [Tam]. Taguchi also proved [Tag1, 2] the semisimplicity of the Galois representation on the Tate module, for both finite and generic characteristic Drinfeld modules. Taguchi proved that a given L-isogeny class contains only finitely many L-isomorphism classes, for L a finite extension of K.

Now over number fields, the Tate isogeny conjecture and Shafarevich finiteness conjectures follow from each other for abelian varieties. On the other hand, in our case, we see immediately that the family $\rho_t = t + g\tau + \tau^2$ depending on g contains infinitely many non-isomorphic rank 2 Drinfeld modules, with good reduction everywhere (so not only the support of the discriminant is bounded, but the discriminant is one).

This is in contrast to the classical situation, where (by the Faltings theorem, which was known as the Shafarevich conjecture) there are only finitely many isomorphism classes of abelian varieties over a given number field K and of given dimension, with a good reduction outside a fixed finite set of places of K. (Usually, in the literature, this is stated in the original version which also fixed a polarization degree, but that hypothesis can be removed by using the Zarhin trick mentioned in Faltings paper). The fact that the discriminant (for any non-constant a, the corresponding discriminant, i.e., the top coefficient for ρ_a, is enough for our purposes, since ρ_a determines ρ by the commutation relations in the definition) is quite unrestricted here in contrast to the classical case where the bound on the discriminant also bounds g_2 gives this different behavior in the reduction theory. In fact, we do not have any good definition for a 'conductor' of a

Drinfeld module: The usual way to get the exponent at p from l-adic representations fails as for all $\wp$'s we are still in characteristic p. A crude candidate like the product of primes in the support of the minimal discriminant is an isogeny invariant, but fails to give any refined information and it does not satisfy any Szpiro conjecture type bounds: The naive analogies suggest exponent $q+1$ in place of 6 in Szpiro conjecture. But even in semistable case, where classically the conductor is exactly this product, the discriminant exponent can be arbitrary (as we can see in the example $\rho_t = t+\tau+\wp^n\tau^2$) and Szpiro type inequality does not hold for any exponent. More generally, we see that the local exponents in the conductors can not stay bounded, in contrast to $p>3$ case over number fields, if such an inequality is to hold.

Classically, there is a well-known theorem of Serre on the image of Galois representation obtained from torsion of elliptic curves. Pink [P] showed that if ρ has no more endomorphisms than A, then for a finite set S of places $v \neq \infty$, the image of $Gal(K^{sep}/K)$ in $\prod_{v\in S} GL_n(A_v)$ for the corresponding representation for rank n Drinfeld modules is open. Note that this is weaker than Serre type adelic version, but much stronger (unlike the classical case) than the case of one prime v, because we are dealing with all huge pro-p groups here, even though the primes v change. So the simple classical argument combining p-adic and l-adic information to go from the result for one place to the result for finitely many places does not work).

The finite characteristic valued L-series can be attached to these finite characteristic valued representations in a way analogous to the classical case, using the exponent space of David Goss. Interesting special values, zero distribution results have been established for analogs of Riemann and Dedekind zeta functions, but not yet in our rank two situation. So we will just refer to [Go2] for this theory including its analytic aspects. The cohomological aspects have been developed by Taguchi, Wan [TW] and more recently by Pink and Boeckle.

11. Elliptic curves

Now let us look at what is known about the elliptic curves E over function fields. For general references and a survey of more general situation of finite characteristic diophantine geometry, we refer to [V1] (and MathSciNet!). We focus here on some basic (or recent) results (and conjectures) on elliptic curves.

First note that to expect analogs of basic results we have to be careful with possible isotriviality of the elliptic curves. For example, if the positive genus (we have to define genus carefully too, as it can change by inseparable extensions, see [V1] for more discussion of both these issues) affine curve over a function field is in fact defined over its field of constants, say $\mathbb{F}_q$, then for any non-constant integral point P on it, we have infinitely many integral points obtained by taking q^n-th power of the co-ordinates of P. (The similar considerations are needed for formulating analogs of Szpiro [LS] or abc conjectures, because $a + b = c$ implies $a^{p^n} + b^{p^n} = c^{p^n}$ It is interesting to note that (characteristic zero) function field analogs of Szpiro and abc conjectures were proved by Kodaira and Stothers respectively and rediscovered a few times before the conjectures were made).

But with the proper definition of genus and conditions of non-isotriviality, we do get appropriate analogs of Mordell conjecture (proved by Samuel, Szpiro), Siegel finiteness of integral points theorem (as a corollary of Mordell rather than from diophantine approximation as usual, because of big differences in diophantine approximation situation), Shafarevich finiteness theorem (proved by Szpiro, Parshin, Zahrin) and Mordell-Weil theorem (proved by Lang and Neron).

In particular, we can again ask the basic questions about the rational torsion and Mordell-Weil rank, which is now finite, in contrast to the Drinfeld modules situation.

If we have non-isotrivial elliptic curve E over K with K-rational point of order n, then we get a non-constant map from $Spec(K)$ to the modular curve $X_1(n)$ extending to a morphism from X to $X_1(n)$. Since the genus of $X_1(n)$ tends to infinity with n, we get uniform bound on n in terms of the genus of X. For n divisible by the characteristic, we have to be more careful about the moduli problem computing the relevant genus of the special fiber (which drops, but still tends to infinity). For details see [L].

(The reason that such a proof does not work for the Drinfeld modules case is that Drinfeld modular curve $X_1(I)$ being a curve over $Spec(A)$, it only implies boundedness of L-torsion for rank 2 ('non-iso-trivial') Drinfeld A-modules, where L is now a function field over the 'constants' K, rather than a finite extension of K.)

The usual uniform boundedness statement is in terms of degree (rather than genus), which we interpret here as the degree of some cover of projective line. For characteristic zero function fields, such a statement [HS] is attributed to Frey who deduced it from Szpiro inequality, which is known in this case. Because of the differences in Szpiro inequality (see [LS]), it does not give such a uniform bound in finite characteristic.

Here is another approach: The smallest positive degree of the map from a given curve C to the projective line is called the gonality of C. Here is a basic fact: If a curve X admits a non-constant map to curve Y, then the gonality of Y is at most that of X: In fact, if f is an element of smallest positive polar degree, say d, in the function field of X, then its elementary symmetric functions with respect to Y (at least one of which would be non-constant) have polar degree at most d, as can be seen by pointwise degree check, because all the conjugates have the same absolute value, which is the extension degree-th root of the norm. Alternately, we can use the norm, whose polar divisor is just the push-forward, hence if the norm is non-constant, the claim is clear. If it is constant, we replace f by $f+c$ for an appropriate constant c. (Over a finite field, we may not have enough choice for c, but we can go to algebraic closure and use gonality over $\overline{\mathbb{F}_p}$ instead.)

Hence, if a curve C, which is a cover of a projective line of degree bounded by d, admits a non-constant map to $X_1(n)$, then $X_1(n)$ has gonality at most d.

In [Ab, Y] a lower bound, linear in its genus, on $\mathbb{C}$-gonality (and thus on $\mathbb{Q}$-gonality) is deduced from theorems on smallest eigenvalues of Laplacians. This then gives uniform boundedness for characteristic zero function fields, such as $\mathbb{Q}(t)$ and $\mathbb{C}(t)$.

For a function field over $\mathbb{F}_q$, even to deal with orders prime to the characteristic p, we need to show that $\mathbb{F}_q$-gonality of $X_1(n)$ tends to infinity as n (prime to p) tends to infinity and the gonality bound obtained above may drop, a priori, under such specialization.

But we can deduce this instead, by an argument essentially due to Ogg [O]: The number of supersingular points, in characteristic p, of $X_0(n)$ tends to infinity with n (prime to p). On the other hand, they are all defined over $\mathbb{F}_{p^2}$ and hence over $\mathbb{F}_q$, if q is an even power of p. Hence, comparison with the number of $\mathbb{F}_q$-points of the projective line shows that the $\mathbb{F}_q$-gonality of $X_0(n)$ tends to infinity with n. But then embedding in a quadratic extension, if necessary, it is true over any $\mathbb{F}_q$. Finally, with $X = X_1(n)$ to $Y = X_0(n)$, we see that the gonality of $X_1(n)$ tends to infinity with n. (The supersingular points of $X_1(n)$ are defined over $\mathbb{F}_{p^{2f}}$, where f is the order of p modulo n, so we can not argue directly with X_1 in place of X_0).

Now, if $n = p^k$, since the special fiber at p represents Drinfeld's notion of 'order n', rather than actual order n, we have to look at gonality of the Igusa curve for p^k. But since it has about p^n cusps, which are $\mathbb{F}_p$-rational, same argument as Ogg gives that gonality over $\mathbb{F}_q$ tends to infinity, as k tends to infinity. To do the general case, we just decompose the large n into p power part and a prime to p-part, one of which has to be large. So the uniform boundedness of rational torsion works in the case of elliptic curves over function fields over finite fields as in the case of elliptic curves over number fields, but by simpler arguments. (But since the gonality can drop in the extensions, this argument does not address whether gonality does tend to infinity over $\overline{\mathbb{F}_p}$).

As for the ranks, it is conjectured, but not known that Mordell-Weil ranks of elliptic curves over a fixed number field can be arbirarily large. Shafarevich and Tate [ST] showed that Mordell-Weil rank can be made arbitrarily high by choosing a suitable E. Their examples were non-constant, but isotrivial (i.e., over an extension they become isomorphic to constant). Shioda [Sh1, 2] gave non-isotrivial such examples over $\overline{\mathbb{F}_p}(t)$, for p congruent to 3 modulo 4. By modifying and extending his examples and techniques and calculating the zeta function (in this case it turns out that it does give the arithmetic rank), Doug Ulmer has recently proved (to appear in Annals of Math) such a result over $\mathbb{F}_p(t)$. An example is: Let p be a prime. The $\mathbb{F}_p(t)$-rank of $y^2 + xy = x^3 - t^{p^n+1}$ is at least $(p^n - 1)/2n$. The ranks in these examples asymptotically meet the known upper bounds for the ranks in terms of conductors, both in geometric (i.e., when the field of constants is enlarged to its algebraic closure) and arithmetic (i.e., over $\mathbb{F}_p$) case. This has led him to make a conjecture on the order of growth of the maximal rank with respect to conductor for elliptic curves over number fields.

As for how the Mordell-Weil ranks of the elliptic curves over a given number field are distributed, there is a large but inconclusive numerical evidence with various twists of a given elliptic curve or of many elliptic curves of small discriminant or conductor. The folklore conjecture (currently!) is that (ordered by the size of conductors) allmost all (density one) elliptic curves have lowest rank consistent with the sign of the functional equation (i.e., rank one, if the sign is -1 and zero otherwise).

Interesting theoretical evidence comes from the philosophy of Katz-Sarnak [KS], the idea is to look at a curve over a function field as a family of curves over finite fields and use Deligne's refined equidistribution results on Frobenius eigenvalues (see below for how Tate's results connect this to the analytic rank, which should be the rank by the Birch and Swinnerton-Dyer conjectures) to get the average behaviour, by calculation of the relevant geometric monodromy groups. In this direction, Katz shows (yet unpublished), for example, that for a fixed $p > 3$, as n tends to infinity, allmost all elliptic curves over $\mathbb{F}_{p^n}(t)$ with degrees of g_2 and g_3 (in the Weierstrass model) bounded by fixed large numbers have the lowest ranks consistent with the sign of their functional equations. He also gives results for families of twists of a given curve in his (upcoming) book 'Twisted L-functions and monodromy'.

Since the base is not fixed, the corresponding function field problem is still open and this can be compared rather with the average behaviour in cyclotomic (or $\mathbb{Z}_p$-) tower, in terms of Weil-Iwasawa analogies. (Corresponding statement is also unknown in the number field case).

Moving to other aspects, the analytic continuation and functional equations of Hasse-Weil (complex valued) L-functions of elliptic curves were proved by Grothendieck, with treatment of local constants given by Deligne [D].

A lot of progress has been made on the function field analog of Birch and Swinnerton-Dyer conjectures: First, Tate [T1] showed how it easily follows, from the basic machinery of the etale cohomology and cycle maps invented by Grothendieck and others to attack Weil conjectures, that independent points produce the correct Frobenius eigenvalues giving zeros of L-functions, thus showing that analytic rank (i.e., the order of vanishing of the L-function at 1) is at least the Mordell-Weil rank. He gave very general conjectures which imply equality in this case.

Artin and Tate [T2] further showed how the basic l-adic cohomology machinery also implies that getting the predicted leading term (up to sign and powers of p) is equivalent to the equality of the two ranks which is again equivalent to the finiteness of the l-primary component of the Tate-Shafarevich group for some prime l different from the characteristic. Using p-adic cohomology, Milne [M] then got the equivalence to the exact predicted leading term in odd characteristic. The finiteness of the Tate-Shafarevich group in general is a major open problem. See [T2, T3] (and MathSciNet) for some more evidence and progress.

Function field analog of Shimura-Taniyama-Weil modularity conjecture is a nice mixture of elliptic curves and Drinfeld module theories: It says that given an non-isotrivial elliptic curve over a function field F with split multiplication reduction at place (call it) ∞ admits a surjective morphism from the modular curve of rank two Drinfeld A-modules with certain level I structure, where I is the geometrical conductor (ignoring ∞) of E. It follows from the works of Weil, Grothendieck, Jacquet-Langlands, Deligne, Drinfeld and is explained in [GR].(See also [T4] for background). Note that if the elliptic curve is non-isotrivial, then its j-invariant is not a constant and it will have a split multiplicative reduction, at least after an appropriate quadratic extension, at a pole of j, so the condition we have is a mild one. In fact, it assures analog of Tate parametrization that we have in the similar p-adic situation, as well as in the complex situation.

In fact, Drinfeld (Lafforgue respectively) proved (recently announced the proof respectively) function field analog of Langlands conjecture for Gl_2 (Gl_n respectively) using moduli of Drinfeld modules and related objects. See [D1, D2, DH, GPRG, Lau] and Laumon's recent Bourbaki seminar talk (No. 873) for some background and references to a large body of relevant works.

Using the modular connection, we can use Heegner points machinery [GZ]. After a partial progress by Brown (see [B1], which has some errors), an analog of the Gross-Zagier theorem linking the value of the derivative of the L-series to the height of Heegner point was proved in [RT1, 2] in the $\mathbb{F}_q[t]$ case. Some progress towards more general setting of the function fields has been made recently by Ulmer and by Ambrus Pal in a slightly different setting.

To mention another recent result, Voloch [V2] gave the proof of function field analog of Mahler-Manin conjecture (original conjectures were proved soon afterwards, see [BDGP], [W]) proving that the period q (this standard notation for the period should not be confused with the power of p) of the Tate elliptic curve $y^2 + xy = x^3 + a_4x + a_6$, with

$$a_4 := \sum_{n\geq 1} \frac{-5n^3q^n}{1-q^n}, \qquad a_6 := \sum_{n\geq 1} \frac{-(7n^5+5n^3)q^n}{12(1-q^n)}$$

over the function field $F := \mathbb{F}_p(a_4, a_6)$ is transcendental over its field of definition F. Whereas the proof in [BDGP] used Mahler method, Voloch used Igusa theory, and [Th2], [AT] gave proofs using automata criterion for algebraic power series.

Using the modularity, as well as Teitelbaum's [Te] construction of certain measures allows to associate a finite characteristic valued L-series to the elliptic curve (and in general to modular forms). Its special values should contain some interesting information. But almost nothing is known.

Finally we should mention interesting work of Perrin-Riou (in complex multiplication case) and Bertilloni-Darmon on Birch and Swinnerton-Dyer conjecture in the p-adic non-archimedian setting, in part inspired by the function field results mentioned above and Iwasawa analogies.

This is the written version of the plan of the talks which I was supposed to deliver at the Advanced instructional workshop on algebraic number theory, with special reference to elliptic curves and the International conference on number theory, at the Harish-Chandra Research Institute, November 8-29, 2000. At the last moment, I could not attend it. I thank the editors S. D. Adhikari, B. Ramakrishnan and S. A. Katre for still requesting the article for the proceedings. I am grateful to Pierre Deligne, Noam Elkies, Nick Katz, Barry Mazur and Bjorn Poonen for explaining me various issues regarding uniform boundedness for elliptic curves and giving references.

References

[Ab] D. Abramovich, *A linear bound on the gonality of modular curves*, Intern. Math. Res. Notices (1996), 1005–1011.

[AT] J.-P. Allouche and D. Thakur, *Automata and transcendence of the Tate period in finite characteristic*, Proceedings of American Mathematical Society, 127 (1999), 1309–1312.

[A] E. Artin, Algebraic numbers and Algebraic functions, Gordon and Breach, New York 1967.

[B1] M. Brown, *On a conjecture of Tate for elliptic surfaces over finite fields*, Proc. London Math. Soc. **69** (1994), 489–514.

[B2] M. Brown, *Singular moduli and supersingular moduli of Drinfeld modules*, Invent. Math. **110** (1992), 419–439.

[BDGP] K. Barre-Sirieix, G. Diaz, F. Gramain, G. Philibert, *Une preuve de la conjecture de Mahler-Manin*, Invent. Math. **124** (1996), 1–9.

[C] L. Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), 137–168.

[D] P. Deligne, *Les constantes des equations fonctionelles des fonctions L*, Modular functions of one variable II, (Antwerp proccedings, 1972) 501–597, Lecture notes in Math. 349 (1973) Springer, Berlin.

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

[D1] V. Drinfeld, *Elliptic modules*, Math. Sbornik **94** (1974), 594–627, English transl.: Math. U.S.S.R. Sbornik **23** (1976), 561–592.

[D2] V. Drinfeld, *Elliptic modules II*, Math. *U.S.S.R. Sbornik* **31** (1977), 159–170.

[E] N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. 89 (1987), 561–567.

[G1] E.-U. Gekeler, *Drinfeld Modular Curves*, Lect. Notes in Math., **1231**, Springer (1986).

[G2] E.-U. Gekeler, *On finite Drinfeld modules* , *J. Algebra* **141** (1991), 187–203.

[G3] E.-U. Gekeler, *A Product expansion for the discriminant function of Drinfeld modules of rank two*, *J. Number Theory* **21** (1985), 135–140.

[G4] E.-U. Gekeler, *On the coefficients of Drinfeld modular forms*, *Invent. Math.* **93** (1988), 667–700.

[GPRG] Gekeler E.-U. et al - *Drinfeld modules, modular schemes and applications*, Proceedings of Alden-Biesen conference (1996), World Scientific Pub. River Edge NJ, (1997).

[GR] E.-U. Gekeler, M. Reversat, *Jacobians of Drinfeld modular curves*, *J. reine angew. Math.* (to appear).

[Go1] D. Goss, *Modular forms for* $\mathbb{F}_r[T]$, *J. reine angew. Math.* **317** (1980), 16–39.

[G02] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik, Springer-Verlag, Berlin, (1996).

[GoHR] D. Goss et al (Editors), *The Arithmetic of Function Fields* Proceedings of the Ohio-state conference (1991), Walter de Gruyter, NY (1992).

[GZ] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. 54 (1986), 225–320.

[H] D. Hayes, *A brief introduction to Drinfeld modules*, in [GoHR], 1–32.

[KS] N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues and Monodromy*, Amer. Math. Soc. Providence, R.I. (1999).

[L] M. Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. 90 (1968), 456–462.

[Lau] G. Laumon, *Cohomology of Drinfeld modular varieties I and II*, Cambridge University Press, Cambridge 1996, 1997.

[LS] Q. Liu and T. Saito, *Inequality for conductor and differentials of a curve over a local field*, J. Alg. geometry 9 (2000), 409–424.

[M] J. Milne, *On a conjecture of Artin and Tate*, Ann. Math. 102 (1975), 517–533.

[O] A. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449–462.

[P] R. Pink, *The Mumford-Tate conjecture for Drinfeld modules*, Publ. Res. Inst. Math. Sci. 33 (1997), 393–425.

[Po1] B. Poonen, *Local height functions and the Mordell-Weil theorem for Drinfeld modules*, *Compositio Math.* **97** (1995), 349–368.

[Po2] B. Poonen, *Torsion in rank* 1 *Drinfeld modules and the uniform boundedness conjecture*, Math. Ann. 308 (1997), 571–586.

[Po3] B. Poonen, *Drinfeld modules with no supersingular primes*, Intern. Math. Research Notices, (1998), 151–159.

[RT1] H. -G. Rück and U. Tipp, *A Gross-Zagier formula for function fields*, Algorithmic algebra and number theory, Heidelberg (1997), 121–137, edited by Matzat et al. Springer, Berlin 1999.

[RT2] H. -G. Rück and U. Tipp, *Heegner points and L-series of automorphic cusp forms of Drinfeld type*, Doc. Math. 5 (2000), 365–444.

[S] J. Serre, *Statements of results* in Seminar on complex multiplications, 1957/58, Ed. by A. Borel et al, Lecture Notes in Math. No. 21, Springer-Verlag, NY (1966).

[Sh1] T. Shioda, *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer. J. Math. 108 (1986), 415–432.

[Sh2] T. Shioda, *Mordell-Weil lattices and sphere packings*, Amer. J. Math. 113 (1991), 931–948.

[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer (1985).

[ST] I. Safarevich, J. Tate, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR 175 (1967), 770–773.

[T1] J. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row (1965), 93–110.

[T2] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Seminaire Bourbaki, (1966) vol. 9, Exp. 306, 415–440, Soc. Math. France, Paris (1995).

[T3] J. Tate, *The arithmetic of elliptic curves*, Inven. Math. 23 (1974), 179–206.

[T4] J. Tate, *Number theoretic background, in: Proceedings Symposia in Pure Mathematics* **33** *Part 2*, Amer. Math. Soc. (1979), 3–26.

[Tag1] Y. Taguchi, *Semi-simplicity of the Galois representations attached to Drinfeld modules of "infinite characteristics"*, *J. Number Theory* **44** (1993), 292–314.

[Tag2] Y. Taguchi, *Semi-simplicity of the Galois representations attached to Drinfeld modules of "finite characteristics,"* *Duke Math. J.* **62** (1991), 593–599.

[Tag3] Y. Taguchi, *The Tate conjecture for t-motives*, *Proc. Amer. Math. Soc.* **123** (1995), 3285–3287.

[TW] Y. Taguchi and D. Wan, *L-functions of ϕ-sheaves and Drinfeld modules*, J. Amer. Math. Soc. 9 (1996), 755–781.

[Tam] A. Tamagawa, *Generalization of Anderson's t-motives and Tate conjectures*, Moduli spaces, Galois represenations and L-functions, RIMS Kokyuroko, (Proc. RIMS), No. 884 (1994), 154–159.

[Te] J. Teitelbaum, *Rigid analytic modular forms: An integral transform approach*, in [GoHR], 189–207.

[Th1] D. Thakur, *Gamma functions for function fields and Drinfeld modules*, *Ann. of Math.* **134** (1991), 25–64.

[Th2] D. Thakur, *Automata-style proof of Voloch's transcendence result*, J. Number theory, 58 (1996), 60–63.

[V1] J. Voloch, *Diophantine geometry in characteristic p: a survey*, Arithmetic geometry, Cortona (1994), 260–278, Symposia Math. 37, Cambridge U. Press, Cambridge 1997.

[V2] J. Voloch, *Transcendence of elliptic modular functions in characteristic* p, J. Number Theory, 58 (1996), 55–59.

[W] M. Waldschmidt, *Sur la nature arithmétique des valeurs de fonctions modulaires*, Séminaire Bourbaki, Nov. 1996, Paris.

[Ya] S. T. Yau, *An application of eigenvalue estimate to algebraic curves defined by congruence subgroup*, Math. Res. Lett. 3 (1996), 167–172.

[Y] J. Yu, *Transcendence in finite characteristic*, in [GoHR], 253–264.

[Yu] J.-K. Yu, *Isogenies of Drinfeld modules over finite fields*, *J. Number Theory* **54** (1995), 161–171.