ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

ANDREAS SCHWEIZER

On singular and supersingular invariants of Drinfeld modules

Annales de la faculté des sciences de Toulouse 6e série, tome 6, nº 2 (1997), p. 319-334

<http://www.numdam.org/item?id=AFST_1997_6_6_2_319_0>

Annales de la Faculté des Sciences de Toulouse Vol. VI, n° 2, 1997

On singular and supersingular invariants of Drinfeld modules[*]

ANDREAS SCHWEIZER[1]

RÉSUMÉ. — Nous considérons les invariants j des $\mathbb{F}_q[T]$-modules de Drinfeld de rang 2 singuliers et supersinguliers. Après avoir donné une liste complète de tous les invariants singuliers $j \in \mathbb{F}_q[T]$, nous construisons des "invariants universels supersinguliers". Ce sont des ensembles $\mathcal{S}(0) \subset \mathcal{S}(1) \subset \mathcal{S}(2) \cdots$ d'invariants j singuliers, tels que pour tout premier $\mathfrak{p} \in \mathbb{F}_q[T]$ de degré $2n+1$, la réduction modulo $\mathfrak{p}$ est une bijection entre $\mathcal{S}(n)$ et les invariants supersinguliers en caractéristique $\mathfrak{p}$. Nous donnons une construction similaire pour les premiers de degré pair.

ABSTRACT. — We consider j-invariants of singular and supersingular $\mathbb{F}_q[T]$-Drinfeld modules of rank 2. After giving a complete list of all singular $j \in \mathbb{F}_q[T]$, we construct "universal supersingular invariants". These are sets $\mathcal{S}(0) \subset \mathcal{S}(1) \subset \mathcal{S}(2) \cdots$ of singular j-invariants, such that for every prime $\mathfrak{p} \in \mathbb{F}_q[T]$ of degree $2n+1$, reduction modulo $\mathfrak{p}$ is a bijection between $\mathcal{S}(n)$ and the supersingular j-invariants in characteristic $\mathfrak{p}$. A similar construction is given for primes of even degree.

0. Introduction

In [Sch1] it is proved that for every prime $\mathfrak{p} \in \mathbb{F}_q[T]$ of odd degree $d \geq 3$, reduction modulo $\mathfrak{p}$ of 0 and the q values $j_\beta = (T^q - T)(1-(T^q-\beta)^{q-1})$ with $\beta \in \mathbb{F}_q$, furnishes $q+1$ different supersingular invariants of Drinfeld modules in characteristic $\mathfrak{p}$. If $\deg(\mathfrak{p}) = 3$ these are even all of the supersingular invariants.

[*] Reçu le 9 octobre 1995

[1] FB 9 Mathematik, Universität des Saarlandes,
Postfach 151150, D-66041 Saarbrücken (Germany)
e-mail: schweizer@math.uni-sb.de

supported by DFG

It is well known that 0 is the j-invariant of the Drinfeld module having complex multiplication by $\mathbb{F}_{q^2}[T]$. The fact that j_β is the j-invariant of the Drinfeld module having complex multiplication by the order of conductor $T - \beta$ in $\mathbb{F}_{q^2}[T]$ (implicitly proved in [Sch1] led to the idea of "universal supersingular invariants". Starting with $\mathcal{S}(0) = \{0\}$ and $\mathcal{S}(1) = \mathcal{S}(0) \cup \{j_\beta \mid \beta \in \mathbb{F}_q\}$, these form a sequence of sets $\mathcal{S}(0) \subset \mathcal{S}(1) \subset \mathcal{S}(2) \subset \cdots$ of j-invariants of Drinfeld modules having complex multiplication by orders in the constant field extension such that for every prime $\mathfrak{p}$ of degree $2n+1$, reduction of $\mathcal{S}(n)$ modulo $\mathfrak{p}$ gives the supersingular invariants in characteristic $\mathfrak{p}$ in a one-to-one manner.

The idea to use quaternion algebras to establish injectivity of the reduction was inspired by a remark in [Ei2]; later I found out that [Ka] and [Da] contain similar calculations.

The main problem in our argumentation bears some resemblance to [Do], where the prime factorization of differences of singular invariants is calculated. But while Dorman treats only maximal orders, it is exactly the non-maximal ones we are interested in. On the other hand, much weaker statements suffice for our intentions; we only need to know that certain primes do not divide such a difference.

Many of our results (including Proposition 11) should carry over to supersingular invariants of elliptic curves without difficulty (if they are not already established). But calculation of some examples shows that the existence of universal supersingular invariants for elliptic curves is doubtful or at least not provable by our method.

1. Basic facts (compare [Ge1], [Ge4])

Let $\mathbb{F}_q$ be a finite field with q elements, $A := \mathbb{F}_q[T]$ the polynomial ring, and $K := \mathbb{F}_q(T)$ its field of fractions. Throughout this paper $\mathfrak{p} \in A$ will be a prime of degree d (i.e. a monic irreducible polynomial of degree d), and $\mathfrak{f}$ will be a monic element of A.

By K^{ac} (resp. K^{sep}) we denote the algebraic (resp. separable) closure of K and by $\mathfrak{B}$ the integral closure of A in K^{ac}. Finally, K_∞ is the completion of K at the place $\infty = T^{-1}$.

If L is an extension field of K or of $A/\mathfrak{p}$, we say that the A-characteristic of L is generic or $\mathrm{char}_A(L) = \mathfrak{p}$, respectively. For simplicity we assume that

L is algebraically closed and denote by $L\{\tau\}$ the twisted polynomial ring with the commutation rule $\tau \circ \ell = \ell^q \circ \tau$ for all $\ell \in L$.

A Drinfeld module (of rank 2) over L is an $\mathbb{F}_q$-algebra homomorphism $\phi : A \to L\{\tau\}$, $a \mapsto \phi_a$, defined by $\phi_T = \Delta\tau^2 + \lambda\tau + T$ with Δ, $\lambda \in L$ and $\Delta \neq 0$. The element $j(\phi) = \lambda^{q+1}/\Delta$ is called the j-invariant of ϕ. Interpreting τ as Frobenius endomorphism $\ell \mapsto \ell^q$ (i.e. associating to $u = \sum \ell_i \tau^i \in L\{\tau\}$ the polynomial $u(X) = \sum \ell_i X^{q^i} \in L[X]$), the Drinfeld module ϕ defines a new A-module structure on $(L, +)$ by $(a, \ell) \mapsto \phi_a(\ell)$.

If ϕ is a Drinfeld module in generic characteristic or in characteristic $\mathfrak{p}$ with $\mathfrak{p} \nmid \mathfrak{n}$, then its $\mathfrak{n}$-torsion $\ker(\phi_\mathfrak{n}) = \{\ell \in L \mid \phi_\mathfrak{n}(\ell) = 0\}$ is a free rank 2 $A/\mathfrak{n}$-module. The $\mathfrak{p}$-torsion for $\mathfrak{p} = \mathrm{char}_A(L)$ is isomorphic to $A/\mathfrak{p}$ or trivial.

A morphism from the Drinfeld module ϕ to the Drinfeld module ψ is an element u of $L\{\tau\}$ such that $u \circ \phi_T = \psi_T \circ u$. The kernel of a morphism is $\ker(u) = \{\ell \in L : u(\ell) = 0\}$. A morphism u from ϕ to ψ is called an $\mathfrak{n}$-isogeny, $\mathfrak{n} \in A$, if there exists a morphism v from ψ to ϕ such that $v \circ u = \phi_\mathfrak{n}$. Then v is an $\mathfrak{n}$-isogeny from ψ to ϕ. Every non-zero morphism is an $\mathfrak{n}$-isogeny for a suitable $\mathfrak{n}$. For example, if $u(X)$ is separable and $\ker(u) \subseteq \ker(\phi_\mathfrak{n})$ then u is an $\mathfrak{n}$-isogeny.

An isomorphism of Drinfeld modules is a morphism $u \in L^\times$. Two Drinfeld modules ϕ and ψ are isomorphic if and only if $j(\phi) = j(\psi)$.

An endomorphism of ϕ is an element of the centralizer of ϕ_T in $L\{\tau\}$. Clearly, $\phi_a \in \mathrm{End}(\phi)$ for all $a \in A$. Hence we may (via ϕ) consider A as a subring of $\mathrm{End}(\phi)$.

2. Rational singular invariants

In this section we specialize to the case $L = C$ where C is the completion of the algebraic closure of K_∞. As for elliptic curves over the complex numbers, the rank 2 Drinfeld modules over C are in one-to-one correspondence with the rank 2 A-lattices contained in C (compare [Gel]).

If ϕ and ψ are two Drinfeld modules over C and Λ_1, Λ_2 are the corresponding lattices, then the morphisms from ϕ to ψ are in bijection with the $c \in C$ such that $c\Lambda_1 \subseteq \Lambda_2$. In particular, ϕ and ψ are isomorphic if and only if $\Lambda_2 = c\Lambda_1$ for a $c \in C^\times$. The existence of an $\mathfrak{n}$-isogeny from ϕ to ψ is equivalent to the existence of a $c \in C^\times$ such that $\mathfrak{n}\Lambda_1 \subseteq c\Lambda_2 \subseteq \Lambda_1$.

Sometimes we will write $j(\Lambda)$ for the j-invariant of the Drinfeld module corresponding to Λ. If $\omega \in \Omega := C - K_{\infty}$, we may even write $j(\omega)$ instead of $j(A + A\omega)$.

This may be used to define for $\mathfrak{n} \in A$ the Hecke correspondence $\mathcal{H}_{\mathfrak{n}}$ on j-invariants. If $j = j(\Lambda_1)$ then $\mathcal{H}_{\mathfrak{n}}(j)$ consists of all $j(\Lambda_2)$ (counted with multiplicities) such that $\mathfrak{n}\Lambda_1 \subseteq \Lambda_2 \subseteq \Lambda_1$ and $\Lambda_2/\mathfrak{n}\Lambda_1$ is a free rank 1 $A/\mathfrak{n}$-module.

There exists a polynomial $\Phi_{\mathfrak{n}}(X,Y) \in A[X , Y]$ such that for $j \in C$ the divisor $\mathcal{H}_{\mathfrak{n}}(j)$ consists of the zeroes of $\Phi_{\mathfrak{n}}(X,j)$ counted with multiplicities. See [Bae] for more information and [Sch1] for some explicit calculations. The only facts we will need are summarized in the following theorem.

THEOREM 1 [Bae].— *If $\mathfrak{p}$ is a prime of degree d, then:*

(a) $\Phi_{\mathfrak{p}}(X,j)$ is a polynomial of degree $q^d + 1$ over $A[j]$;

(b) $\Phi_{\mathfrak{p}}(X,Y) \equiv (X^{q^d} - Y)(X - Y^{q^d}) \bmod \mathfrak{p}$ ("Kronecker congruence");

(c) $\Phi_{\mathfrak{p}}(X,X)$ is a polynomial of degree $2q^d$ with leading coefficient -1.

A Drinfeld module ϕ over C or its j-invariant is called singular if $\mathrm{End}(\phi)$ is strictly larger than A. From the interpretation on lattices one sees that then $\mathrm{End}(\phi)$ is an imaginary quadratic order, that is, a (not necessarily maximal) A-order B in a quadratic field L/K with $L \not\subseteq K_{\infty}$. We say that ϕ has complex multiplication by B.

Example 2.— Restricting the rank 1 $\mathbb{F}_q[\sqrt{T}]$-Drinfeld module defined by $\phi_{\sqrt{T}} = \tau + \sqrt{T}$ to $\mathbb{F}_q[T]$ gives a rank 2 $\mathbb{F}_q[T]$-Drinfeld module with complex multiplication by $\mathbb{F}_q[\sqrt{T}]$. From $\phi_T = \tau^2 + (\sqrt{T}^q + \sqrt{T})\tau + T$ one easily calculates its j-invariant, which in case q is even turns out to be $j_{\mathrm{ins}} := j(A[\sqrt{T}]) = j(\phi) = (T^q + T)^{(q+1)/2}$.

Obviously, two Drinfeld modules having complex multiplication by an order B are isomorphic if and only if the corresponding lattices are in the same ideal class of B. We define

$$H_B(X) := \prod_{\mathfrak{A} \in \mathrm{Cl}(B)} (X - j(\mathfrak{A})) .$$

Later we will need that the ideal class number of an order $B_{\mathfrak{f}}$ with conductor $\mathfrak{f}$ in a maximal order B is

$$h(B_{\mathfrak{f}}) = \frac{\varphi_L(\mathfrak{f})\, h(B)}{[B^* : B_{\mathfrak{f}}^*]}$$

where $*$ denotes the group of units, $h(B)$ is the ideal class number of B and φ_L is the relative Euler function of $L = \mathrm{Quot}(B)$. It is defined by

$$\varphi_L(\mathfrak{f}) = q^{\deg(\mathfrak{f})} \prod_{\mathfrak{p}|\mathfrak{f}} \left(1 - \chi_L(\mathfrak{p})\, q^{-\deg(\mathfrak{p})}\right)$$

where χ_L is the character of the quadratic extension L/K, that is, $\chi_L(\mathfrak{p})$ takes the values 0, 1, or -1 if $\mathfrak{p}$ is ramified, split, or inert in L, respectively.

THEOREM 3 [Gel].— *Let B be an imaginary quadratic order and $\mathfrak{A}$ an ideal of B. Then:*

(a) $j(\mathfrak{A})$ is an algebraic integer;

(b) $j(\mathfrak{A})$ is separable over $\mathrm{Quot}(B)$ *with minimal polynomial $H_B(X)$;*

(c) If $\mathrm{Quot}(B)$ *is separable over K, then $H_B(X) \in K[X]$ and hence $j(\mathfrak{A})$ is separable and algebraic over K of degree $h(B)$.*

Contrary to what is stated in [Gel], part (c) is not true if $\mathrm{Quot}(B)$ is inseparable over K.

LEMMA 4.— *If $2 \mid q$ and j has complex multiplication by the inseparable quadratic order $A[\mathfrak{f}\sqrt{T}]$, then j is algebraic over K with minimal polynomial $\left(H_{A[\mathfrak{f}\sqrt{T}]}(X)\right)^2$. Its degree of separability is $h\left(A[\mathfrak{f}\sqrt{T}]\right) = q^{\deg(\mathfrak{f})}$ and its degree of inseparability is 2.*

Proof.— In view of Theorem 3 it suffices to show that j is inseparable over K. Suppose $j \in K^{\mathrm{sep}}$. Then there exists a Drinfeld module ϕ over K^{sep} with invariant j. Since all torsion points of ϕ are in K^{sep}, the images of ϕ under isogenies are defined over K^{sep}. But one of these images has invariant $j_{\mathrm{ins}} \notin K^{\mathrm{sep}}$. □

LEMMA 5.— *Let ϕ be the Drinfeld module corresponding to the order $A[\omega]$ and let ψ be a Drinfeld module having complex multiplication by $A[\mathfrak{f}\omega]$.*

(a) If $A[\omega]$ is a maximal order and $\mathfrak{p} \nmid \mathfrak{f}$, then there exists an $\mathfrak{a}\mathfrak{f}$-isogeny from ϕ to ψ for some $\mathfrak{a}$ with $\mathfrak{p} \nmid \mathfrak{a}$.

(b) If $A[\omega]$ has ideal class number 1 , then $\mathcal{H}_{\mathfrak{f}}(j(\omega))$ contains all j-invariants of Drinfeld modules having complex multiplication by $A[\mathfrak{f}\omega]$.

Proof

(a) Every ideal class in $A[\mathfrak{f}\omega]$ contains an ideal $\mathfrak{A} = A\mathfrak{a} + A(b - \mathfrak{f}\omega)$ with $\mathfrak{a}, b \in A$ and $\mathfrak{p} \nmid \mathfrak{a}$. So there exists an $\mathfrak{a}\mathfrak{f}$-isogeny from ϕ to ψ.

(b) If ω is separable over K, then $j(\omega) \in K$ and $\Phi_{\mathfrak{f}}(X, j(\omega)) \in K[X]$. If ω is inseparable over K, then $j(\omega) = j_{\text{ins}}$ and $\Phi_{\mathfrak{f}}(X, j(\omega)) \in K(\sqrt{T})[X]$. Obviously $\mathcal{H}_{\mathfrak{f}}(j(\omega))$ contains $j(\mathfrak{f}\omega)$, so in either case $H_{A[\mathfrak{f}\omega]}(X)$ must divide $\Phi_{\mathfrak{f}}(X, j(\omega))$. □

Now we are ready to give the analogue of Weber's list of the 13 rational j-invariants of elliptic curves with complex multiplication (see for example [Hu, p. 233]).

THEOREM 6.— *The following table is a complete list of all singular $j \in \mathbb{F}_q[T]$ together with the endomorphism rings $A[\omega]$ of the corresponding Drinfeld modules. The entries in the table are subject to the conditions $\alpha \in \mathbb{F}_q^\times$, $\beta \in \mathbb{F}_q$, and $\mathbb{F}_{q^2} = \mathbb{F}_q(\gamma)$. Furthermore, ε is a non-square in $\mathbb{F}_q^\times$ and δ a generator of $\mathbb{F}_4^\times$. Finally $\mathfrak{f}$ denotes the conductor of the order $A[\omega]$, and g is the genus of the function field $K(\omega)$.*

q	$j = j(\omega)$	equation for $\omega \in \Omega$	$\mathfrak{f}$	g
any	0	$\omega = \gamma$	1	0
any	$j_\beta = (T^q - T)\big(1 - (T^q - \beta)^{q-1}\big)$	$\omega = \gamma(T - \beta)$	$T - \beta$	0
2	$T^3\big(T+1\big)^3(T^2+T+1)$	$\omega = \gamma(T^2+T+1)$	T^2+T+1	0
odd	$\big(T - \beta\big)^{\frac{q+1}{2}}\big((T-\beta)^{\frac{q-1}{2}} + 1\big)^{q+1}$	$\omega^2 = T - \beta$	1	0
odd	$-\big(T - \beta\big)^{\frac{q+1}{2}}\big((T-\beta)^{\frac{q-1}{2}} - 1\big)^{q+1}$	$\omega^2 = \varepsilon(T - \beta)$	1	0
2^n	$\alpha^{-1}\big(\ell^{2^n-1} + \ell^{2^n-2} + \cdots + \ell + 1\big)^{q+1}$	$\omega^2 + \omega = \alpha T + \beta = \ell$	1	0
2	$\big(T+1\big)^6$	$\omega^2 + T\omega = T^3$	T	0
2	T^6	$\omega^2 + (T+1)\omega = \big(T+1\big)^3$	$T+1$	0
2	$T^3\big(T+1\big)^3$	$\omega^2 + \omega = T^3 + T + 1$	1	1
2	$T^6\big(T+1\big)^6$	$\omega^2 + \omega = T^5 + T^3 + 1$	1	2
3	$T^4\big(T+1\big)^4\big(T-1\big)^4\big(T^3 - T - 1\big)^2$	$w^2 = T^3 - T - 1$	1	1
3	$-T^4\big(T+1\big)^4\big(T-1\big)^4\big(T^3 - T + 1\big)^2$	$w^2 = -T^3 + T - 1$	1	1
4	$\big(T^4 + T\big)^{10}$	$\omega^2 + \omega = T^3 + \delta$	1	1

Sketch of Proof

According to [McR], the function fields of the table are the only separable imaginary quadratic extensions of $\mathbb{F}_q(T)$ whose maximal orders $A[\omega]$ have ideal class number 1 . The corresponding values $j(\omega)$ can be calculated by the method of [DuHa] or looked up in [Ha], [Du] and [DuHa].

In some cases it is possible to descend to non-maximal orders of conductor $\mathfrak{f}$ whose ideal class number is still 1. The necessary and sufficient condition for this is $\varphi_{K(\omega)}(\mathfrak{f}) = q+1$ if $A[\omega] = \mathbb{F}_{q^2}[T]$, and $\varphi_{K(\omega)}(\mathfrak{f}) = 1$ otherwise. In any case $j(\mathfrak{f}\omega)$ lies in $\mathcal{H}_{\mathfrak{f}}(j(\omega))$. For deg(f) = 1 the values of $j(\mathfrak{f}\omega)$ have been found as zeroes of $\Phi_{\mathfrak{f}}(X, j(\omega))$. In the remaining case, $\mathcal{H}_{T^2+T+1}(0)$ has been calculated via isogenies using a computer. □

One sees that in general there are only three types of separable imaginary quadratic orders with ideal class number 1, namely: the maximal order in the constant field extension, orders with conductor of degree 1 in the constant field extension, and maximal orders in geometric extensions of genus 0 where the infinite prime is ramified. For small q there are some further orders whose ideal class number is 1 by accident.

3. Universal supersingular invariants

Throughout this section, $\mathfrak{p}$ will be a prime in A of degree d.

Let k be the algebraic closure of the field $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$. We consider Drinfeld modules in characteristic $\mathfrak{p}$ (i.e. Drinfeld modules $\phi : A \to k\{\tau\}$ defined by $\phi_T = \Delta\tau^2 + \lambda\tau + t$, where t is the image of T in $A/\mathfrak{p}$). Such a Drinfeld module or its j-invariant is called supersingular, if its $\mathfrak{p}$-torsion is trivial, or equivalently, if End(ϕ) is not commutative (compare [Ge4]). Then End(ϕ) is a maximal order in $\mathbb{H}_\mathfrak{p}$, the quaternion algebra over K ramified at $\mathfrak{p}$ and ∞.

The set of all supersingular invariants in characteristic $\mathfrak{p}$ (i.e. supersingular $j \in k$ for the chosen $\mathfrak{p}$) will be denoted by $\Sigma_\mathfrak{p}$. Furthermore, we write $\mathbb{F}_{\mathfrak{p}^2}$ for the (unique) quadratic extension of $\mathbb{F}_\mathfrak{p}$ in k.

THEOREM 7 ([Ge1], [Ge2], [Ge4])

(a) *The cardinality of* $\Sigma_{\mathfrak{p}}$ *equals the class number of* $\mathbb{H}_{\mathfrak{p}}$. *More explicitly we have*

$$\sharp\Sigma_{\mathfrak{p}} = \begin{cases} \dfrac{q^d-1}{q^2-1} & \text{if } d \text{ is even,} \\ \dfrac{q^d-q}{q^2-1}+1 & \text{if } d \text{ is odd.} \end{cases}$$

(b) $\Sigma_{\mathfrak{p}}$ *is contained in* $\mathbb{F}_{\mathfrak{p}^2}$ *and stable under* $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}^2}/\mathbb{F}_{\mathfrak{p}})$. *Hence* $\sharp\Sigma_{\mathfrak{p}} = \sigma_1(\mathfrak{p})+2\sigma_2(\mathfrak{p})$ *where* $\sigma_1(\mathfrak{p})$ *is the number of supersingular invariants in* $\mathbb{F}_{\mathfrak{p}}$ *and* $\sigma_2(\mathfrak{p})$ *is the number of pairs of conjugate supersingular invariants in* $\mathbb{F}_{\mathfrak{p}^2} - \mathbb{F}_{\mathfrak{p}}$.

(c) *If* $j \in K^{ac}$ *is the invariant of a Drinfeld module having complex multiplication by an order* B *and* $\wp$ *is a prime above* $\mathfrak{p}$ *in* $K(j)$, *then* $j \bmod \wp$ *is supersingular if and only if* $\mathfrak{p}$ *is ramified or inert in* $\mathrm{Quot}(B)$.

If we reduce all j-invariants of Drinfeld modules over C having complex multiplication by a certain order B, the reduced invariants are the zeroes of $H_B(X) \bmod \mathfrak{p}$. Hence the set of reduced invariants does not depend on the choice of $\wp$ above $\mathfrak{p}$. Therefore we will sometimes a bit inaccurately use the expression "reduction $\bmod\, \mathfrak{p}$".

By Theorem 7(c), invariants of Drinfeld modules having complex multiplication by an inseparable order become supersingular modulo $\mathfrak{p}$ for every prime $\mathfrak{p}$.

Every Drinfeld module is isomorphic to one of the form $\phi_T = \tau^2+\lambda\tau+T$. If ϕ is singular, then $\lambda \in \mathfrak{B}$ by Theorem 3(a).

If $\mathfrak{P}$ is a prime above $\mathfrak{p}$ in $K(\lambda)$ and $\overline{\lambda}$ denotes $\lambda \bmod \mathfrak{P}$, then the reduction of ϕ is $\overline{\phi} : A \to k\{\tau\}$ defined by $\overline{\phi}_T = \tau^2 + \overline{\lambda}\tau + t$. It is well known that the reduction maps $\mathrm{End}(\phi)$ injectively into $\mathrm{End}(\overline{\phi})$. If ϕ has complex multiplication by an order $B_{\mathfrak{f}}$ with conductor $\mathfrak{f}$ and $\overline{\phi}$ is supersingular, this induces an embedding ι of $\mathrm{Quot}(B_{\mathfrak{f}})$ into $\mathbb{H}_{\mathfrak{p}}$.

LEMMA 8.— *If* $\mathfrak{f} = \mathfrak{p}^e\tilde{\mathfrak{f}}$ *with* $\mathfrak{p} \nmid \tilde{\mathfrak{f}}$, *then* $\iota(\mathrm{Quot}(B_{\mathfrak{f}})) \cap \mathrm{End}(\overline{\phi}) = B_{\tilde{\mathfrak{f}}}$. *Especially, if* $\mathfrak{p} \nmid \mathfrak{f}$ *then* $\mathrm{End}(\phi)$ *is optimally embedded in* $\mathrm{End}(\overline{\phi})$.

Proof.— Clearly, $\iota(\mathrm{Quot}(B_{\mathfrak{f}})) \cap \mathrm{End}(\overline{\phi})$ is an order B containing $B_{\mathfrak{f}}$. If u is an element of $\mathrm{End}(\phi)$ such that $u/a \notin \mathrm{End}(\phi)$ for all non-constant $a \in A$, then $\ker(u)$ is cyclic. Then, of course, $\ker(\overline{u}) = \overline{\ker(u)}$ is cyclic, too. In other words: $\overline{u}/a \notin \mathrm{End}(\overline{\phi})$ for all non-constant $a \in A$ prime to $\mathfrak{p}$. This shows $B \subseteq B_{\tilde{\mathfrak{f}}}$. Since B is optimally embedded in the maximal order $\mathrm{End}(\phi)$ of $\mathbb{H}_{\mathfrak{p}}$, its conductor must be prime to $\mathfrak{p}$ ([Eil, Satz 6]). Hence $B = B_{\tilde{\mathfrak{f}}}$. □

Now we assume that ϕ and ψ are non-isomorphic Drinfeld modules having complex multiplication by orders $B_{\mathfrak{f}_1}$ and $B_{\mathfrak{f}_2}$ with conductors $\mathfrak{f}_1$ and $\mathfrak{f}_2$ in a maximal order B. If $j(\phi) \equiv j(\psi) \bmod \wp$ for a prime $\wp$ above $\mathfrak{p}$, then λ_1 and λ_2 in $\phi_T = \tau^2 + \lambda_1\tau + T$, $\psi_T = \tau^2 + \lambda_2\tau + T$ may be chosen in such a way that $\lambda_1 \equiv \lambda_2 \bmod \mathfrak{P}$ for a prime $\mathfrak{P}$ above $\wp$. Then ϕ and ψ reduce to the same Drinfeld module $\overline{\phi}$ and isogenies u from ϕ to ψ reduce to endomorphisms of $\overline{\phi}$.

LEMMA 9.— *Suppose ϕ and ψ are given as above, have supersingular reduction* $\bmod \mathfrak{p}$, *and* $\mathfrak{p} \nmid \mathfrak{f}_1\mathfrak{f}_2$. *If one of the conditions:*

- $\mathfrak{f}_1 \neq \mathfrak{f}_2$,
- $\mathfrak{p}$ *is inert in* $\mathrm{Quot}(B)$,
- B *is inseparable,*

is fulfilled, then $\mathrm{End}(\phi)$ *and* $\mathrm{End}(\psi)$ *are differently embedded in* $\mathrm{End}(\overline{\phi})$, *i.e.* $\mathrm{Quot}(B_{\mathfrak{f}_1}) \neq \mathrm{Quot}(B_{\mathfrak{f}_2})$ *in* $\mathbb{H}_{\mathfrak{p}}$.

Proof.— If $\mathfrak{f}_1 \neq \mathfrak{f}_2$, the assertion is clear from the fact that $\mathrm{End}(\phi)$ and $\mathrm{End}(\psi)$ are optimally embedded. So we may assume $\mathfrak{f}_1 = \mathfrak{f}_2$. Then by Lemma 5 there exists an $\mathfrak{n}$-isogeny u from ϕ to ψ with $\mathfrak{p} \nmid \mathfrak{n}$, namely the composition of the isogeny from ϕ to the Drinfeld module corresponding to B with the isogeny from this Drinfeld module to ψ.

If $\mathrm{End}(\phi) = A[\omega_1]$ with $\omega_1 = c_1 +$ (higher terms in τ) $\in \mathfrak{B}\{\tau\}$ and if $m(X) \in A[X]$ is the minimal polynomial of ω_1, then $\omega_2 = c_2 +$ (higher terms in τ) $\in \mathfrak{B}\{\tau\}$ defined by $u \circ \omega_1 = \omega_2 \circ u$ is a root of the same polynomial in $\mathrm{End}(\psi)$.

Now we assume $K(\overline{\omega}_1) = K(\overline{\omega}_2)$ in $\mathrm{End}(\overline{\phi})$. Then $\overline{\omega}_1$ and $\overline{\omega}_2$ are roots of $m(X)$ in $K(\overline{\omega}_1)$. If B is inseparable this implies $\overline{\omega}_1 = \overline{\omega}_2$. We want to proof this also for separable B. If $u = c_u +$ (higher terms in τ) $\in \mathfrak{B}\{\tau\}$, then $u \circ \omega_1 = \omega_2 \circ u$ implies $c_u c_1 = c_2 c_u$ and hence $\overline{c}_u\overline{c}_1 = \overline{c}_2\overline{c}_u$. But $\overline{u} \in \mathrm{End}(\phi)$ is separable (that is $\overline{c}_u \neq 0$), thus $\overline{c}_1 = \overline{c}_2$. Since $m(X) \bmod \mathfrak{p}$ is separable (here we use that $\mathfrak{p}$ is inert in B), we may conclude $\overline{\omega}_1 = \overline{\omega}_2$.

In any case $K(\overline{\omega}_1) = K(\overline{\omega}_2)$ implies $\overline{u} \circ \overline{\omega}_1 = \overline{\omega}_1 \circ \overline{u}$ and hence $\overline{u} \in K(\overline{\omega}_1) \cap \mathrm{End}(\overline{\phi}) = \overline{\mathrm{End}(\phi)}$, i.e. there exists $\eta \in \mathrm{End}(\phi)$ with $\overline{\eta} = \overline{u}$. As $\ker(u)$ contains no $\mathfrak{p}$-torsion, $\ker(\eta) = \ker(u)$ must hold. But then the images of ϕ under η and u would be isomorphic, in contradiction to $j(\phi) \neq j(\psi)$. So the assumption $K(\overline{\omega}_1) = K(\overline{\omega}_2)$ was wrong, and the lemma is proved. □

The conditions in Lemma 9 look somehow artificial and one might hope that the same lemma (with a modified proof) also holds if $\mathfrak{p}$ is ramified.

LEMMA 10.— *Suppose $B = A[\omega]$ is a maximal order and $X^2 + aX + b \in A[X]$ is the minimal polynomial of ω. Denote by $B_{\mathfrak{f}_i}$ the order of conductor $\mathfrak{f}_i$ in B. If there exist different embeddings ι_1 of $B_{\mathfrak{f}_1}$ and ι_2 of $B_{\mathfrak{f}_2}$ (not necessarily $\mathfrak{f}_1 \neq \mathfrak{f}_2$!) into a maximal order $\mathcal{O}$ of the quaternion algebra $\mathbb{H}_{\mathfrak{p}}$, then*

$$\deg(\mathfrak{p}) \leq \max\{\deg(a^2\mathfrak{f}_1\mathfrak{f}_2),\, \deg(b\mathfrak{f}_1\mathfrak{f}_2)\}\,.$$

Proof.— By assumption there exist $\omega_1, \omega_2 \in \mathcal{O}$ with $\omega_i^2 + a\mathfrak{f}_i\omega_i + b\mathfrak{f}_i^2 = 0$ and $\omega_2 \notin K(\omega_1)$. Hence $\tilde{\mathcal{O}} := A + A\omega_1 + A\omega_2 + A\omega_1\omega_2$ is a rank 4 A-submodule of $\mathcal{O}$. As A contains $s := \mathrm{Tr}(\omega_1\omega_2) = \omega_1\omega_2 + \omega_2\omega_1 + a^2\mathfrak{f}_1\mathfrak{f}_2 - a\mathfrak{f}_1\omega_2 - a\mathfrak{f}_2\omega_1$, one easily sees that $\tilde{\mathcal{O}}$ is actually an order. An unnerving calculation reveals that the discriminant of $\tilde{\mathcal{O}}$ is

$$\mathfrak{D}(\tilde{\mathcal{O}}) = -(s + 2b\mathfrak{f}_1\mathfrak{f}_2)(s - 2b\mathfrak{f}_1\mathfrak{f}_2)(s - a^2\mathfrak{f}_1\mathfrak{f}_2 + 2b\mathfrak{f}_1\mathfrak{f}_2)(s - a^2\mathfrak{f}_1\mathfrak{f}_2 - 2b\mathfrak{f}_1\mathfrak{f}_2)\,.$$

Now $\mathfrak{p}|\mathfrak{D}(\mathcal{O})|\mathfrak{D}(\tilde{\mathcal{O}}) \neq 0$. Therefore $\mathfrak{p}$ must divide one of the factors above and we may conclude $\deg(\mathfrak{p}) \leq \max\{\deg(s),\, \deg(a^2\mathfrak{f}_1\mathfrak{f}_2),\, \deg(b\mathfrak{f}_1\mathfrak{f}_2)\}$. The minimal polynomial of $\omega_1\omega_2$ is $X^2 - sX + b^2\mathfrak{f}_1^2\mathfrak{f}_2^2$. This implies $\deg(s) \leq \deg(b\mathfrak{f}_1\mathfrak{f}_2)$, for otherwise $K(\omega_1\omega_2)$ would be a real quadratic subfield of $\mathbb{H}_{\mathfrak{p}}$. □

If two orders B_1 and B_2 with $\mathrm{Quot}(B_1) \not\cong \mathrm{Quot}(B_2)$ are embedded in $\mathcal{O}$, a similar reasoning is possible but one obtains a weaker bound for $\deg(\mathfrak{p})$. Compare [Da, Theorem 6.1].

PROPOSITION 11.— *Suppose $2 \nmid q$ and $A[\sqrt{D}]$ is a maximal imaginary quadratic order. Denote by $S(n)$ the set of j-invariants of Drinfeld modules having complex multiplication by $A[\mathfrak{f}\sqrt{D}]$ with $\deg(\mathfrak{f}) \leq n$. If $\mathfrak{p}$ is inert in $K(\sqrt{D})$ and $\deg(\mathfrak{p}) > \deg(D) + 2n$, then reduction $\mathrm{mod}\,\mathfrak{p}$ is an injective mapping from $S(n)$ into $\Sigma_{\mathfrak{p}}$.*

Proof.— Clearly, the elements of $S(n)$ become supersingular upon reduction. Suppose j, $j' \in S(n)$ are different, but fall together $\operatorname{mod} \mathfrak{p}$. Then Lemma 9 in combination with Lemma 10 shows $\deg(\mathfrak{p}) \leq \deg(D) + 2n$. □

A similar result holds for even q.

Now we define $\mathcal{S}(n)$ as the set of all j-invariants of Drinfeld modules having complex multiplication by an order of conductor $\mathfrak{f}$ in $\mathbb{F}_{q^2}[T]$ with $\deg(\mathfrak{f}) \leq n$. We use the expression "universal supersingular invariants" for the elements of $\mathcal{S}(0) \subset \mathcal{S}(1) \subset \mathcal{S}(2) \subset \ldots$, because it will turn out that in this case reduction to $\Sigma_{\mathfrak{p}}$ is surjective for all primes of odd degree.

LEMMA 12.— $\sharp\mathcal{S}(n) - \sharp\mathcal{S}(n-1) = q^{2n-1}$.

Proof.— If L denotes the constant field extension $\mathbb{F}_{q^2}(T)$, then

$$\sharp\mathcal{S}(n) - \sharp\mathcal{S}(n-1) = \sum_{\deg(\mathfrak{f})=n} \frac{\varphi_L(\mathfrak{f})}{q+1},$$

so we have to show $\sum_{\deg(\mathfrak{f})=n} \varphi_L(\mathfrak{f}) = q^{2n}+q^{2n-1}$. The generating function

$$\Lambda(Z) := \sum_{n=0}^{\infty} \left(\sum_{\deg(\mathfrak{f})=n} \varphi_L(\mathfrak{f}) \right) Z^n$$

has the Euler-product $\Lambda(Z) = \prod_{\mathfrak{p}} \Lambda_{\mathfrak{p}}(Z)$ with

$$\Lambda_{\mathfrak{p}}(Z) = \sum_{n=0}^{\infty} \varphi_L(\mathfrak{p}^n) Z^{dn} = 1 + \left(1 - \frac{(-1)^d}{q^d}\right) \sum_{n=1}^{\infty} q^{dn} Z^{dn} = \frac{1-(-1)^d Z^d}{1-q^d Z^d}$$

where $d = \deg(\mathfrak{p})$. If we define

$$M(Z) := \sum_{n=0}^{\infty} q^n Z^n = \sum_{n=0}^{\infty} \left(\sum_{\deg(\mathfrak{f})=n} 1 \right) Z^n ,$$

then

$$M(Z) = \prod_{\mathfrak{p}} M_{\mathfrak{p}}(Z) \quad \text{with} \quad M_{\mathfrak{p}}(Z) = \sum_{n=0}^{\infty} Z^{dn} = \frac{1}{1-Z^d} .$$

Hence

$$\Lambda_{\mathfrak{p}}(Z) = \frac{M_{\mathfrak{p}}(qZ)}{M_{\mathfrak{p}}(-Z)} \quad \text{and} \quad \Lambda(Z) = \frac{M(qZ)}{M(-Z)}.$$

Now it is completely elementary to show

$$\left(1 + \sum_{n=1}^{\infty}(q^{2n} + q^{2n-1})Z^n\right) M(-Z) = M(qZ),$$

and the lemma follows. □

PROPOSITION 13.— *For any prime $\mathfrak{p} \in A$ of degree $2n+1$, reduction modulo $\mathfrak{p}$ is a bijection between $\mathcal{S}(n)$ and $\Sigma_{\mathfrak{p}}$.*

Proof.— From Lemma 10 one easily obtains $\sharp\mathcal{S}(n) = \sharp\Sigma_{\mathfrak{p}}$. Hence it suffices to show that the reduction map is injective. If q is odd this is the statement of Proposition 11. The proof for even q is almost the same. □

Example 14.— For $q = 2$ the set $\mathcal{S}(2)$ consists of the following 11 j-invariants:

$\mathfrak{f}$	j
1	0
T	$j_0 = T\big(T+1\big)^3$
$T+1$	$j_1 = T^3(T+1)$
T^2+T+1	$j_\square = T^3\big(T+1\big)^3(T^2+T+1)$
T^2	zeroes of $X^{-1}\Phi_T(X,j_0) =$ $= X^2 + T\big(T+1\big)^4(T^3+T+1)X + T\big(T+1\big)^6$
$\big(T+1\big)^2$	zeroes of $X^{-1}\Phi_{T+1}(X,j_1) =$ $= X^2 + T^4(T+1)(T^3+T^2+1)X + T^6(T+1)$
$T(T+1)$	zeroes of $\Phi_T(X,j_1) =$ $= \Phi_{T+1}(X,j_0)$ $= X^3 + T(T+1)(T^6+T^5+T^3+T^2+1)X^2$ $+ T^2\big(T+1\big)^2(T^2+T+1)X + T^3\big(T+1\big)^3$

By calculation of resultants and discriminants and by substituting 0, j_0, j_1, and $j_\square$ into the above polynomials, one can verify directly that these 11 values remain distinct modulo $\mathfrak{p}$ for any prime $\mathfrak{p}$ of odd degree $d > 3$.

If q is even, using the inseparable extension, we can also construct universal supersingular invariants for the primes of even degree.

PROPOSITION 15.— *For $2 \mid q$ denote by $\mathfrak{S}(n)$ the set of j-invariants of Drinfeld modules having complex multiplication by $A[\mathfrak{f}\sqrt{T}]$ with* $\deg(\mathfrak{f}) \leq n$. *Then for any prime $\mathfrak{p} \in A$ of degree $2n+2$, the reduction modulo $\mathfrak{p}$ is a bijection between $\mathfrak{S}(n)$ and $\Sigma_{\mathfrak{p}}$.*

Proof.— $\sharp\mathfrak{S}(n) = \sharp\Sigma_{\mathfrak{p}}$ is easily verified. The rest of the proof is the same as for Proposition 11. □

For $2 \nmid q$ there exists a weaker result.

PROPOSITION 16.— *Let $2 \nmid q$ and $D = \alpha T + \beta$ with $\alpha \in \mathbb{F}_q^{\times}$, $\beta \in \mathbb{F}_q$. If $S(n) := \{j(\phi) \mid \phi$ has complex multiplication by $A[\mathfrak{f}\sqrt{D}]$ with* $\deg(\mathfrak{f}) \leq n\}$, *then for every prime $\mathfrak{p}$ of degree $2n+2$ which is inert in $K(\sqrt{D})$, reduction* mod$\mathfrak{p}$ *is a bijection between $S(n)$ and $\Sigma_{\mathfrak{p}}$.*

Proof.— If $L = K(\sqrt{D})$, then proceeding as in the proof of Lemma 12 one obtains

$$\sum_{n=0}^{\infty}\left(\sum_{\deg(\mathfrak{f})=n} \varphi_L(\mathfrak{f})\right) Z^n = \left(\sum_{n=0}^{\infty} q^{2n} Z^n\right)\left(\sum_{n=0}^{\infty}\sum_{\deg(\mathfrak{f})=n} \chi_L(\mathfrak{f}) Z^n\right)^{-1}.$$

Writing $\mathfrak{f}$ as a polynomial in D one easily sees

$$\sum_{\deg(\mathfrak{f})=n} \chi_L(\mathfrak{f}) = 0 \quad \text{for all } n \geq 1\,.$$

Thus

$$\sum_{\deg(\mathfrak{f})=n} \varphi_L(\mathfrak{f}) = q^{2n}$$

and hence $\sharp S(n) = \sharp\Sigma_{\mathfrak{p}}$. The rest is clear from Proposition 11. □

It should be remarked, however, that there exist primes $\mathfrak{p}$ which are not inert in any field $k(\sqrt{\alpha T + \beta})$, for example $\mathfrak{p} = T^6 - T^4 + 1 \in \mathbb{F}_3[T]$.

If for a prime $\mathfrak{p}$ we define the Deuring polynomial $\mathcal{D}_{\mathfrak{p}}(X) := \prod(X - j)$, the product being taken over all supersingular invariants in characteristic $\mathfrak{p}$, then $\mathcal{D}_{\mathfrak{p}}(X) \in \mathbb{F}_{\mathfrak{p}}[X]$. Propositions 13, 15 and 16 may be reformulated as the following results.

COROLLARY 17

(a) If $B_{\mathfrak{f}}$ is the order with conductor $\mathfrak{f}$ in $\mathbb{F}_{q^2}[T]$, then

$$\prod_{\deg(\mathfrak{f})\le n} H_{B_{\mathfrak{f}}}(X) \bmod \mathfrak{p} = \mathcal{D}_{\mathfrak{p}}(X)$$

for all primes $\mathfrak{p}$ of degree $2n+1$.

(b) If $2 \mid q$ and $\mathfrak{p}$ is a prime of degree $2n+2$, then

$$\prod_{\deg(\mathfrak{f})\le n} H_{A[\mathfrak{f}\sqrt{T}]}(X) \bmod \mathfrak{P} = \mathcal{D}_{\mathfrak{p}}(X)\,,$$

where $\mathfrak{P}$ is the prime above $\mathfrak{p}$ in $K(\sqrt{T})$.

(c) If $2 \nmid q$ and $D = \alpha T + \beta$ with $\alpha \in \mathbb{F}_q^{\times}$, $\beta \in \mathbb{F}_q$, then

$$\prod_{\deg(\mathfrak{f})\le n} H_{A[\mathfrak{f}\sqrt{D}]}(X) \bmod \mathfrak{p} = \mathcal{D}_{\mathfrak{p}}(X)$$

for all primes $\mathfrak{p}$ of degree $2n+2$ which are inert in $K(\sqrt{D})$.

We also mention the construction in [Ge3, p. 697]. There, coming from a totally different direction, polynomials $A_d(X,Y) \in A[X\,,\,Y]$ are defined recursively, such that $A_d(1,Y) \bmod \mathfrak{p}$ is a simple transformation of $\mathcal{D}_{\mathfrak{p}}(Y)$ for all primes of degree d. This is also an efficient method to calculate $\mathcal{D}_{\mathfrak{p}}(X)$. These $A_d(X,Y)$ seem to bear no relation to complex multiplication, so the connection with our results is mysterious.

We conclude with some further results in the spirit of Corollary 17. Following the line of proof in the classical situation (for example [La, p. 143]), one can show the following proposition.

PROPOSITION 18

$$\Phi_{\mathfrak{p}}(X,X) = -\prod H_B(X)^{m(B)}$$

where the product is taken over all imaginary quadratic orders B containing an element whose norm is associated to $\mathfrak{p}$ and

$$m(B) = \begin{cases} 1 & \textit{if } 2 \nmid q \textit{ and } \mathfrak{p} \textit{ is ramified in } \mathrm{Quot}(B) \\ 2 & \textit{otherwise.} \end{cases}$$

Now the zeroes of $H_B(X) \bmod \mathfrak{p}$ are supersingular if and only if $\mathfrak{p}$ is ramified in Quot(B). *On the other hand, Kronecker's congruence implies*

$$\Phi_{\mathfrak{p}}(X,X) \equiv -(X^{q^d} - X)^2 = - \prod_{a \in A/\mathfrak{p}} (X-a)^2 \bmod \mathfrak{p}\,.$$

Combining the two, one easily obtains the following proposition.

Proposition 19

(a) If $2 \nmid q$ and $2 \mid d$ and ε is a fixed non-square in $\mathbb{F}_q^\times$, then

$$H_{A[\sqrt{\varepsilon\mathfrak{p}}]}(X) \bmod \mathfrak{p} = \prod_{\substack{j \in A/\mathfrak{p} \\ j \text{ supersingular}}} (X-j)^2\,.$$

(b) If $2 \nmid q$ and $2 \nmid d$ and ε is a fixed non-square in $\mathbb{F}_q^\times$, then

$$H_{A[\sqrt{\mathfrak{p}}]}(X)\, H_{A[\sqrt{\varepsilon\mathfrak{p}}]}(X) \bmod \mathfrak{p} = \prod_{\substack{j \in A/\mathfrak{p} \\ j \text{ supersingular}}} (X-j)^2\,.$$

(c) If $2 \mid q$ and $\mathfrak{p} = \mathfrak{s}^2 + T\mathfrak{t}^2$ with $\mathfrak{s}$, $\mathfrak{t} \in A$ not necessarily monic, then

$$\prod_{\mathfrak{f} \mid \mathfrak{t}} H_{A[\mathfrak{f}\sqrt{T}]}(X) \bmod \mathfrak{p} = \prod_{\substack{j \in A/\mathfrak{p} \\ j \text{ supersingular}}} (X-j)\,.$$

The supersingular invariants are closely related to Drinfeld modular curves (compare [Ge2]). In particular, $\sharp\Sigma_{\mathfrak{p}} - 1$ is the genus of $X_0(\mathfrak{p})$ and $\sigma_2(\mathfrak{p})$ is the genus of $X_+(\mathfrak{p})$. A quick look at the degrees of the polynomials in Proposition 19 shows the next corollary.

Corollary 20.— *The genus of the curve $X_+(\mathfrak{p})$ is*

$$g(X_+(\mathfrak{p})) = \begin{cases} \frac{1}{4}\left(2g(X_0(\mathfrak{p})) + 2 - h(\sqrt{\varepsilon\mathfrak{p}})\right) & \text{if } 2 \nmid q \text{ and } 2 \mid d, \\ \frac{1}{4}\left(2g(X_0(\mathfrak{p})) + 2 - h(\sqrt{\mathfrak{p}}) - h(\sqrt{\varepsilon\mathfrak{p}})\right) & \text{if } 2 \nmid q \text{ and } 2 \nmid d, \\ \frac{1}{2}\left(g(X_0(\mathfrak{p})) + 1 - \sum_{\mathfrak{f} \mid \mathfrak{t}} q^{\deg(\mathfrak{f})}\right) & \text{if } 2 \mid q \\ & \text{and } \mathfrak{p} = \mathfrak{s}^2 + T\mathfrak{t}^2\,. \end{cases}$$

We remark that this formula has already been proved in [Ge2] (for $2 \nmid q$) and [Sch2] (for $2 \mid q$), calculating the ramification of the covering $X_0(\mathfrak{p}) \to X_+(\mathfrak{p})$.

References

[Bae] BAE (S.) .— *On the Modular Equation for Drinfeld Modules of Rank* 2, J. Number Theory **42** (1992), pp. 123-133.

[Da] DAVID (C.) .— *Supersingular Reduction of Drinfel'd Modules*, Duke Math. J. **78** (1995), pp. 399-412.

[Do] DORMAN (D. R.) .— *On singular moduli for rank* 2 *Drinfeld modules*, Compositio Math. **80** (1991), pp. 235-256.

[Du] DUMMIT (D. S.) .— *Genus Two Hyperelliptic Drinfeld Modules over* $\mathbb{F}_2$, in: The Arithmetic of Function Fields, Proceedings of the Workshop at the Ohio State University (June 17-26, 1991); (D. Goss, D. Hayes, M. Rosen, eds) de Gruyter, Berlin, New York, 1992, pp. 117-129.

[DuHa] DUMMIT (D. S.) and HAYES (D.) .— *Rank one Drinfeld modules on elliptic curves*, Math. Comp. **62**, n° 206 (1994), pp. 875-883, plus 3 microfiches.

[Ei1] EICHLER (M.) .— *Zur Zahlentheorie der Quaternionen-Algebren*, J. Reine Angew. Math. **195** (1955), pp. 127-151; Berichtigung: J. Reine Angew. Math. **197** (1957), p. 220.

[Ei2] EICHLER (M.) .— *New formulas for the class number of imaginary quadratic fields*, Acta Arithmetica **49** (1987), pp. 35-43.

[Ge1] GEKELER (E. U.) .— *Zur Arithmetik von Drinfeld-Moduln*, Math. Annalen **262** (1983), pp. 167-182.

[Ge2] GEKELER (E. U.) .— *Über Drinfeld'sche Modulkurven vom Hecke-Typ*, Compositio Math. **57** (1986), pp. 219-236.

[Ge3] GEKELER (E. U.) .— *On the coefficients of Drinfeld modular forms*, Invent. Math. **93** (1988), pp. 667-700.

[Ge4] GEKELER (E. U.) .— *On finite Drinfeld modules*, J. Algebra **141** (1991), pp. 187-203.

[Ha] HAYES (D.) .— *On the reduction of rank-one Drinfeld modules*, Math. Comp. **57**, n° 195 (1991), pp. 339-349.

[Hu] HUSEMÖLLER (D.) .— *Elliptic Curves*, Springer GTM 111, Berlin Heidelberg New York, (1987).

[Ka] KANEKO (M.) .— *Supersingular* j*-invariants as singular moduli* mod p, Osaka J. Math. **26** (1989), pp. 849-855.

[La] LANG (S.) .— *Elliptic Functions*, Addison-Wesley, Reading, (1973).

[McR] MACRAE (R. E.) .— *On Unique Factorization in Certain Rings of Algebraic Functions*, J. Algebra **17** (1971), pp. 243-261.

[Sch1] SCHWEIZER (A.) .— *On the Drinfeld Modular Polynomial* $\Phi_T(X, Y)$, J. Number Theory **52** (1995), pp. 53-68.

[Sch2] SCHWEIZER (A.) .— *Hyperelliptic Drinfeld Modular Curves*, in: Drinfeld modules, modular schemes and applications, Proceedings of a workshop at Alden Biesen (September 9-14, 1996); (J. van Geel, E.-U. Gekeler, M. van der Put, M. Reversat, eds) World Scientific, Singapore, in press.