Comm. Korean Math. Soc. 6(1991), No. 1, pp. 27–30

ON THE SUPERSINGULAR REDUCTION OF DRINFEL'D MODULES WITH COMPLEX MULTIPLICATION

SUNGHAN BAE AND PYUNG-LYUN KANG

Let k be the rational function field $\mathbf{F}_q(T)$ and $A = \mathbf{F}_q[T]$. We assume that q is odd. Let ϕ be a Drinfel'd module of rank 2 over an A-field E (that is, we have a structure map $\gamma : A \to E$). When $E = C$, the completion of the algebraic closure of $\mathbf{F}_q((\frac{1}{T}))$, we say that ϕ has '*complex multiplication*'('singular' in the terminology of [G]) if $\mathrm{End}_C(\phi)$ is bigger than A. In fact, $\mathrm{End}_C(\phi)$ is an order of imaginary quadratic extension of $\mathbf{F}_q(T)$, i.e., a quadratic extension where ∞ does not split. When $\gamma : A \to E$ has kernel $(p(T))$ where $p(T)$ is a monic irreducible polynomial of degree d, we say that ϕ is *of characteristic* $(p(T))$. When ϕ is of characteristic $(p(T))$, we say that ϕ is 'supersingular' if

$$\phi_p(T) = \tau^{2d}.$$

From now on suppose that a rank 2 Drinfel'd module ϕ over C is given by

$$\phi_T = T + \lambda\tau + \tau^2, \tag{1}$$

where $\tau(a) = a^q$, has a complex multiplication by $\sqrt{p(T)}$, where $p(T)$ is an irreducible polynomial in A. Then $p(T)$ is either a polynomial of odd degree or a polynomial of even degree with leading coefficient in $\mathbf{F}_q - \mathbf{F}_q^2$. It is known ([H], p188) that we can find

$$\phi_{\sqrt{p(T)}} = \sqrt{p(T)} + a_1\tau + a_2\tau^2 \cdots + a_d\tau^d. \tag{2}$$

Since ϕ has complex multiplication, $j = \lambda^{q+1}$ is an algebraic integer and so is λ([G], (4.3)). Let $K = k(\sqrt{p(T)})$, $L = K(j)$ and $\widetilde{L} = K(\lambda)$. Let

Received June 28, 1990.

B and $\widetilde{B}$ be the integral closures of A in L and $\widetilde{L}$, respectively. Then $\phi_T \in \widetilde{B}\{\tau\}$ and from

$$\phi_{\sqrt{p(T)}}\phi_T = \phi_T\phi_{\sqrt{p(T)}}$$

we have $\phi_{\sqrt{p(T)}}$ has coefficients in $\widetilde{B}$([G], (3.3)).

One natural question is 'For which prime ideal $\mathfrak{q}$ of $\widetilde{B}$ is the reduced Drinfel'd module $\tilde{\phi}$ at $\mathfrak{q}$ supersingular?'

In the following we will show that the reduction of ϕ at the prime ideal $\mathfrak{p}$ of $\widetilde{B}$ lying above $(p(T))$ is supersingular.

Let

$$\phi_{p(T)} = \sum_{i=0}^{2d} b_i\tau^i.$$

From (2) we get

$$b_i = \sum_{j=0}^{i} a_j a_{i-j}^{q^j}. \tag{3}$$

Here we let $a_0 = \sqrt{p(T)}$ and $a_j = 0$ for $j > d$.

LEMMA. *For $j < \frac{d}{2}$, $a_j \equiv 0 \pmod{\mathfrak{p}}$.*

Proof. We know that $b_i \equiv 0 \pmod{\mathfrak{p}}$ for $i < d$ and $a_0 \equiv 0 \pmod{\mathfrak{p}}$. Assume that $a_k \equiv 0 \pmod{\mathfrak{p}}$ for $k < j < \frac{d}{2}$. Then

$$0 \equiv b_{2j} \equiv a_j^{q^j+1} + \sum_{\substack{k=0\\k\neq j}}^{2i} a_k a_{2j-k}^{q^k} \pmod{\mathfrak{p}} \tag{4}$$

For $k \neq j$, either k or $2j-k$ is less than j. Hence by induction hypothesis

$$a_j^{q^j+1} \equiv 0 \pmod{\mathfrak{p}}$$

and so

$$a_j \equiv 0 \pmod{\mathfrak{p}}$$

THEOREM. *The reduced Drinfel'd module at $\mathfrak{p}$ is supersingular.*

Proof. It suffices to show that $b_d \equiv 0 \pmod{\mathfrak{p}}$ by the elementary properties of Drinfel'd modules. From (3), we get

$$b_d = \sum_{k=0}^{d} a_k a_{d-k}^{q^k}. \tag{5}$$

If d is odd, either k or $d-k$ is less than $\frac{d}{2}$ for $k \leq d$. Therefore $b_d \equiv 0 \pmod{\mathfrak{p}}$ by the lemma. If $d = 2m$ is even, let $\bar{\phi}$ and $\bar{a}_i$ be the reductions modulo $\mathfrak{p}$. Then by the lemma,

$$\bar{\phi}_{\sqrt{p(T)}} = \bar{a}_m \tau^m + \bar{a}_{m+1}\tau^{m+1} + \cdots + \bar{a}_{2m}\tau^{2m}$$

$$\bar{\phi}_T \bar{\phi}_{\sqrt{p(T)}} = \bar{a}_m \overline{T} \tau^m + \text{higher terms}$$

$$\bar{\phi}_{\sqrt{p(T)}} \bar{\phi}_T = \bar{a}_m \overline{T}^{q^m} \tau^m + \text{higher terms.}$$

Since $\bar{\phi}_{\sqrt{p(T)}} \bar{\phi}_T = \bar{\phi}_T \bar{\phi}_{\sqrt{p(T)}}$, we have $\bar{a}_m \overline{T} = \bar{a}_m \overline{T}^{q^m}$. Hence

$$a_m(T^{q^m} - T) \equiv 0 \pmod{\mathfrak{p}}.$$

Suppose that $a_m \not\equiv 0 \pmod{\mathfrak{p}}$. Then $T^{q^m} - T \equiv 0 \pmod{\mathfrak{p}}$, which implies that $p(T)$ divides $T^{q^m} - T$. But this is impossible because $p(T)$ is irreducible polynomial of degree $2m$. Therefore $a_m \equiv 0 \pmod{\mathfrak{p}}$ and (5) implies that

$$b_d = b_{2m} \equiv a_m^{q^m+1} \equiv 0 \pmod{\mathfrak{p}}.$$

COROLLARY. *For every $j < d$, we have $a_j \equiv 0 \pmod{\mathfrak{p}}$*

Proof. We know from the Theorem that $b_i \equiv 0 \pmod{\mathfrak{p}}$ for every $i < 2d$. Hence the proof of Lemma holds for $j < d$.

It is shown that if d is even (resp. odd), then there are $\frac{q^d-1}{q^2-1}$ (resp: $q \cdot \left(\frac{q^d-1}{q^2-1}\right) + 1$) supersingular j-invariants in characteristic $(p(T))$ ([G], (5.9)). One may ask, "For each supersingular j-invariant in characteristic $(p(T))$ does there exists a Drinfel'd module over C with complex multiplication by $\sqrt{p(T)}$ whose reduction at $\mathfrak{p}$ has the given j-invariant?"

EXAMPLE. Let $q = 3$ and $p(T) = T^3 - T - 1$. Then

$$\phi_T = T + \sqrt{p(T)}(T^3 - T)\tau + \tau^2$$

has complex multiplication by $\sqrt{p(T)}$. In this case

$$\begin{aligned}\phi_{\sqrt{p(T)}} &= \sqrt{p(T)} + (p(T)^2 - p(T))\tau \\ &\quad + \sqrt{p(T)}(p(T) - 1)(p(T)(T^3 - T + 1)^2 - 1)\tau^2 + \tau^3.\end{aligned}$$

Then the reduced Drinfel'd module is given by

$$\phi_T = \overline{T} + \tau^2,$$

so that the reduced j-invariant is 0.

References

[G] Gekeler, E, *Zur Arithmetik von Drinfel'd-Moduln*, Math. Ann. **262** (1983), 167–182.
[H] Hayes, D, *Explicit class Field theory in Global Function Fields*, Studies in Algebra and Number Theory (Rota, G.C., ed.), Academic Press, New York, 1979.

Department of Mathematics
KAIST
Taejon 305-701, Korea
and
Department of Mathematics
Chungnam National University
Taejon 305-764, Korea