JOURNAL OF NUMBER THEORY 42, 123–133 (1992)

On the Modular Equation for Drinfeld Modules of Rank 2

SUNGHAN BAE

Department of Mathematics, KAIST, Taejon, 305-701, Korea

Communicated by Hans Zassenhaus

Received March 5, 1991; revised June 27, 1991

We give an analytic proof of the integrality of the j-invariant when the corresponding Drinfeld module has complex multiplication.

INTRODUCTION

In the classical theory of elliptic curves, the j-invariant of an elliptic curve is an algebraic integer if the elliptic curve has complex multiplication. There are two kinds of proof of this fact, one is algebraic using good reduction [7] and the other is analytic using the integrality of the Fourier coefficients of the q-expansion of j [6, 8].

The same statement is also true for the theory of Drinfeld modules of rank 2. An algebraic proof is given in [2]. In this note we will give an analytic proof following the methods in [6, 8].

1. PRELIMINARIES

Let K be the rational function field $\mathbf{F}_q(T)$ over the finite field $\mathbf{F}_q$ and $A=\mathbf{F}_q[T]$. Let K_∞ be the completion of K at $\infty=(1/T)$ and C the completion of the algebraic closure of K_∞.

An element

$$\alpha=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in $M_2(A)$, the set of 2×2 matrices with entries in A, is called *primitive* if $(a, b, c, d)=(1)$. Let n be a monic polynomial in A. Define

$$\Delta_n=\{\alpha\in M_2(A)\colon \det\alpha=\mu n \text{ for some } \mu\in\mathbf{F}_q^*\}$$
$$\Delta_n^*=\{\alpha\in\Delta_n\colon \alpha \text{ is primitive}\}.$$

0022-314X/92 $5.00

Then $\Gamma = GL_2(A) = \{\gamma \in M_2(A) : \det \gamma \in \mathbf{F}_q^*\}$ acts on Δ_n^* by left or right multiplication.

For the rest of the paper the letters a, b, c, d, n, p represent polynomials in $A = \mathbf{F}_q[T]$ and α, β, γ represent elements of $M_2(A)$.

We get the following theorem whose proof is exactly the same as the classical case.

THEOREM 1.1 *The group Γ operates left transitively on the right Γ-cosets, and right transitively on the left Γ-cosets of Δ_n^*.*

Also we can see that the elements

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

in $M_2(A)$ with a and d monic, $ad = n$, and $\deg b < \deg d$ form distinct left coset representatives of Δ_n^* for Γ.

In the following, the symbols a, d, n always denote monic polynomials in A, unless otherwise stated.

Let $\psi(n)$ be the number of left cosets of Δ_n^*. In the Appendix we compute $\psi(n)$, which is very much the same as the classical one.

In this article we are mainly concerned with the Drinfeld modules of rank 2 on A defined over C. Thus a Drinfeld module ϕ of rank 2 is completely determined by

$$\phi_T = TX + gX^q + \Delta X^{q^2}, \qquad g, \Delta \in C.$$

The j-invariant $j(\phi)$ of ϕ is defined to be g^{q+1}/Δ. The isomorphism classes of Drinfeld modules of rank 2 over C are in one to one correspondence with the similarity classes of discrete projective rank 2 A-submodules of C. A discrete projective A-submodule of C will be called an A-lattice. Hence it is parameterized by Γ-equivalence classes of $\Omega = C - K_\infty$. For $z \in \Omega$, we write $j(z)$ to denote the j-invariant of the Drinfeld module associated to the lattice $Az + A$.

2. MODULAR EQUATION

Let $L = \bar{\pi} A$ be the rank 1 A-lattice in C associated to the Carlitz module

$$\rho_T(z) = Tz + z^q,$$

and $t = t(z) = e_L^{-1}(\bar{\pi} z)$, where e_L is given by

$$e_L(z) = z \prod_{\lambda \in L - \{0\}} \left(1 - \frac{z}{\lambda}\right).$$

By a modular function we mean a meromorphic function on $\Omega = C - K_\infty$, invariant under Γ and having t-expansions at infinity. Then j is a modular function and holomorphic on Ω. It can be shown that j is of the form

$$\frac{1}{s} + h(s), \tag{1}$$

where $s = t^{q-1}$ and h is a power series with coefficients in A, using the result in [3, (6.6), (6.7)]. Because the only modular functions holomorphic on both Ω and infinity are constants, we get

THEOREM 2.1. *Let f be a modular function which is holomorphic on Ω with an s-expansion*

$$f = \sum c_i s^i.$$

Then f is a polynomial in j with coefficients in the module generated by c_i over A.

Let $\{\alpha_i\}_{i=1}^{\psi(n)}$ be the representatives of right cosets of Δ_n^* for Γ given in the previous section. Then Γ acts on the functions $j \circ \alpha_i$ transitively. Let

$$\Phi_n(X) = \prod_{i=1}^{\psi(n)} (X - j \circ \alpha_i).$$

Then the coefficients of $\Phi_n(X)$ are holomorphic on Ω, invariant under Γ, and meromorphic at infinity. Hence by Theorem 2.1, the coefficients of $\Phi_n(X)$ are polynomials in j.

We now consider the expansion of $j \circ \alpha$ for

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \Delta_n^*.$$

Let $j = 1/s + h(s)$. Then

$$j \circ \alpha = \left(\frac{1}{t((az+b)/d)}\right)^{q-1} + h\left(\left(t\left(\frac{az+b}{d}\right)\right)^{q-1}\right).$$

Let $u = u(z) = t((1/n)z) = e_L^{-1}(\bar{\pi} z/n)$.

Define the ath *inverse cyclotomic polynomial* $f_a(X) \in A[X]$, for $a \in A$ not necessarily monic, by

$$f_a(X) = \rho_a(X^{-1}) X^{|a|},$$

where $|a| = q^{\deg a}$. Then

$$t(az) = t^{|a|}/f_a(t).$$

It can be easily seen that the constant term of $f_a(X)$ is $l(a)$, the leading coefficent of a. We denote by Λ_n the kernel of ρ_n, i.e., $\Lambda_n = \{\lambda \in C: \rho_n(\lambda) = 0\}$.

LEMMA 2.2. *If $ad = n$, then $t(az/d) = e_L^{-1}(a\bar{\pi}z/d)$ is a power series in u with coefficients in A.*

Proof. Since $\rho_a(X)$ lies in $A[X]$, $f_a(X)$ lies in $A[X]$. Then $t(az/d) = t(z/d)^{|a|}/f_a(t(z/d))$ is a power series in $t(z/d)$ with coefficients in A because the constant term of $f_a(X)$ is a unit in A. Hence it suffices to show that $t(z/d)$ is a power series in u with coefficients in A. But $t(z/d) = t(az/n) = t(z/n)^{|a|}/f_a(t(z/n))$. So by the same reasoning as before, $t(z/d)$ is a power series in $u = t(z/n)$ with coefficients in A.

COROLLARY. *$j \circ \alpha$ lies in $A[\Lambda_n][[u]]$, where $A[\Lambda_n]$ is the ring generated by the elements of Λ_n over A.*

Proof.

$$\begin{aligned} t\left(\frac{az+b}{d}\right) &= \left(e_L\left(\frac{a\bar{\pi}z + \bar{\pi}b}{d}\right)\right)^{-1} \\ &= \left(e_L\left(\frac{a\bar{\pi}z}{d}\right) + e_L\left(\frac{\bar{\pi}b}{d}\right)\right)^{-1} \\ &= \frac{t((a/d)z)}{1 + e_L(\bar{\pi}b/d)\, t((a/d)z)} \\ &= \sum_{i=0}^{\infty} (-1)^i \left(e_L\left(\frac{\bar{\pi}b}{d}\right)^i t\left(\frac{a}{d}z\right)^{i+1}\right). \end{aligned}$$

Also

$$t\left(\frac{az+b}{d}\right)^{-1} = e_L\left(\frac{a\bar{\pi}z + \bar{\pi}b}{d}\right) = t\left(\frac{az}{d}\right)^{-1} + e_L\left(\frac{\bar{\pi}b}{d}\right).$$

But

$$j \circ \alpha = \left(\frac{1}{t((az+b)/d)}\right)^{q-1} + h\left(\left(t\left(\frac{az+b}{d}\right)\right)^{q-1}\right),$$

where h is a power series with coefficients in A. Hence $j \circ \alpha$ is a Laurent series in u with coefficients in $A[\Lambda_n]$ since $e_L(\bar{\pi}b/d)$ is an n-division point of ρ.

PROPOSITION 2.3. *The t-expansions of the coefficients of $\Phi_n(X)$ lie in* $A((t))$.

Proof. Let $r \in (A/(n))^*$. The automorphism σ_r on $K(\Lambda_n)$ is given by

$$\sigma_r(\lambda_n) = \rho_r(\lambda_n)$$

for $\lambda_n \in \Lambda_n$. Extend this action to $K(\Lambda_n)((u))$. Since $t(az/d) = t(a^2z/n) = u^{|a^2|}/f_{a^2}(u)$ and $f_{a^2}(X) \in A[X]$, σ_r acts on $t(az/d)$ trivially. But in the proof of the corollary of Lemma 2.2,

$$t\left(\frac{az+b}{d}\right) = \sum_{i=0}^{\infty} (-1)^i \left(e_L\left(\frac{\bar{\pi}b}{d}\right)^i t\left(\frac{az}{d}\right)^{i+1}\right).$$

Hence $\sigma_r(t((az+b)/d)) = \sum_{i=0}^{\infty} (-1)^i (e_L(\bar{\pi}br/d)^i \, t(az/d)^{i+1})$. But $e_L(\bar{\pi}br/d) = e_L(\bar{\pi}b'/d)$ where b' is an element in A such that $b' \equiv br \bmod d$ and $\deg b' < \deg d$. Therefore $(j \circ \alpha)^{\sigma_r} = j \circ \alpha'$ where

$$\alpha' = \begin{pmatrix} a & b' \\ 0 & d \end{pmatrix}.$$

Hence σ_r permutes the functions $j \circ \alpha_i$ and so the coefficients of $\Phi_n(X)$ are invariant under σ_r. Therefore the t-expansions of the coefficients of $\Phi_n(X)$ lie in $A((t))$.

Since we know that the coefficients of $\Phi_n(X)$ are polynomials in $A[j]$, we may view Φ_n as a polynomial in two variables X and j with coefficients in A. We write it as

$$\Phi_n(X, j) \in A[X, j].$$

THEOREM 2.4. (i) *$\Phi_n(X, j)$ is irreducible over $C(j)$ and has degree $\psi(n)$*

(ii) $\Phi_n(X, j) = \Phi_n(j, X)$

(iii) *if* $\deg n$ *is odd, then $\Phi_n(j, j)$ is a polynomial in j of degree* >1 *with leading coefficient* ± 1.

Proof. The proofs of (i) and (ii) are exactly the same as the classical case (see [6, p. 55]).

Assume that $\deg n$ is odd, so that if

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

is primitive and $ad = n$, then $\deg a \neq \deg d$. The u-expansion of j starts with $u^{-(q-1)q^{\deg n}}$ and the u-expansion of $j \circ \alpha$ starts with $u^{-(q-1)q^{2\deg a}}$, because

$t^{-1} = t^{-1}(n \cdot (z/n)) = f_n(u)/u^{q^{\deg n}}$ and $t^{-1}(az/d) = t^{-1}(a^2z/n) = f_{a^2}(u)/u^{q^{2\deg a}}$. Since $\deg n$ is odd, $\deg n \neq 2 \deg a$. Hence the polar term in $j - j \circ \alpha$ starts with $u^{-(q-1)q^{\deg n}}$ or $-u^{-(q-1)q^{2\deg a}}$. Hence the u-expansion for $\Phi_n(j, j)$ starts with c_ν/u^ν for some integer ν, with $c_\nu = \pm 1$.

COROLLARY. *For any $\alpha \in M_2(K)$, the function $j \circ \alpha$ is integral over $A[j]$.*

Proof. This is the same proof as in [6, p. 57].

THEOREM 2.5. *If $z \in K(\sqrt{n})$ where n is a square free monic polynomial of odd degree, then $j(z)$ is an algebraic integer. Here $\sqrt{n}$ means any root of $X^2 - n = 0$.*

Proof. Let $L = K(z)$ and $\mathcal{O} = A\omega + A$ be the ring of algebraic integers in L. Take $\eta = \sqrt{n}$. Then

$$\eta\omega = a\omega + b$$

$$\eta = c\omega + d$$

with a, b, c, and d in A. Then

$$\alpha' = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is primitive with determinant $ad - bc = -n$, and $\alpha'\omega = \omega$. Let $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then $\alpha\omega = -\omega$ and $j(-\omega) = j(\omega)$, hence $j(\omega)$ is a root of the polynomial $\Phi_n(X, X) \in A[X]$. But $\deg n$ is odd, $j(\omega)$ is integral over A by Theorem 2.3 (iii). Since $K(z) = K(\omega)$, $z = \beta\omega$ for some primitive $\beta \in M_2(A)$. Then, by construction, $j(z)$ is a root of the monic polynomial

$$\Phi_{\det(\beta)}(X, j(\omega)),$$

hence $j(z)$ is integral over $A[j(\omega)]$. Therefore $j(z)$ is integral over A.

Remark. Theorem 2.5 is also true for the square free polynomial n of the following types,

(1) $\deg n$ is odd and the leading coefficient of n is arbitrary.

(2) $\deg n$ is even and the leading coefficient of n is in $\mathbf{F}_q - \mathbf{F}_q^2$.

In such cases, $L = K(\sqrt{n})$ is called *imaginary quadratic* because ∞ does not split.

In any case we choose the representatives of right cosets of Δ_n^* for Γ, of the form

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

where a is monic and $l(d) = l(n)$. Here $l(n)$ denotes the leading coefficient of n. Then follow the previous arguments for the case of type (1). But for the case of type (2), the proof of Theorem 2.4 (iii) should be changed as follows.

Let n be an even degree polynomial with leading coefficient $l(n)$ not in $\mathbf{F}_q^2$. Let $\deg n = v$. The polar term of j is

$$\left(\frac{f_n(u)}{u^{q^v}}\right)^{q-1}$$

and the polar term of $j \circ \alpha$ is

$$\left(\frac{f_{a^2}(u)}{u^{q^{2\deg a}}}\right)^{q-1}.$$

If $v \neq 2 \deg a$, then $j - j \circ \alpha$ starts with $u^{-(q-1)q^v}$ or $-u^{-(q-1)q^{2 \deg a}}$. If $v = 2 \deg a$, then

$$v' = \deg (n - l(n) a^2) < v.$$

Hence, by the formula (4.7) of [3],

$$\begin{aligned} f_n(X) &= f_{l(n)a^2 + (n - l(n)a^2)}(X) \\ &= f_{l(n)a^2}(X) + X^{q^v - q^{v'}} f_{(n - l(n)a^2)}(X). \end{aligned}$$

Thus, we get

$$\frac{f_n(u)}{u^{q^v}} = \frac{f_{l(n)a^2}(u)}{u^{q^v}} + \frac{f_{(n-l(n)a^2)}(u)}{u^{q^{v'}}}.$$

Therefore the polar term of $j - j \circ \alpha$ starts with

$$-\left(\frac{l(n)}{u^{q^v}}\right)^{q-2} \cdot \frac{l(n - l(n)a^2)}{u^{q^{v'}}}.$$

But $-l(n)^{q-2} l(n - l(n)a^2) \in \mathbf{F}_q^*$. Therefore $\Phi_n(j, j)$ has leading coefficient in $\mathbf{F}_q$. Then the rest is exactly the same.

3. Kronecker Congruence Relation and Relations with Isogeny

THEOREM 3.1 (Kronecker Congruence Relation). *Let $p = p(T)$ be a monic irreducible polynomial of degree v in A. Then we have*

$$\begin{aligned} \Phi_p(X, j) &\equiv (X - \rho_p(j))(\rho_p(X) - j) \pmod p \\ &\equiv (X - j^{q^v})(X^{q^v} - j) \pmod p. \end{aligned}$$

Proof. The second congruence follows from the fact that $\rho_p(X) \equiv X^{q^\nu}$ $(\mathrm{mod}\, p)$. Representatives for the primitive matrices of determinant p are given by

$$\alpha_b = \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}, \qquad \deg b < \deg p$$

and

$$\alpha_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

For a modular function f, we shall write $f^*(t)$ for its t-expansion, and similarly for a u-expansion. Let $j^*(t) = \sum a_i t^i$. Then

$$\begin{aligned}(j \cdot \alpha_p)^*\,(t) &= \sum a_i t(pz)^i \\ &= \sum a_i \left(\frac{1}{\rho_p(1/t)}\right)^i.\end{aligned}$$

From $\rho_p(X) \equiv X^{q^\nu}$ $(\mathrm{mod}\, p)$, we have

$$\begin{aligned}(j \circ \alpha_p)^*\,(t) &\equiv \sum a_i t^{iq^\nu} \qquad (\mathrm{mod}\, p) \\ &\equiv \left(\sum a_i t^i\right)^{q^\nu} \qquad (\mathrm{mod}\, p) \\ &\equiv \rho_p(j) \qquad (\mathrm{mod}\, p).\end{aligned}$$

Let λ_p be a primitive pth root of ρ. Then

$$\begin{aligned}(j \circ \alpha_b)^*\,(t) &= \sum a_i t\left(\frac{z+b}{p}\right)^i \\ &\equiv \sum a_i t\left(\frac{z}{p}\right)^i \qquad (\mathrm{mod}\, \lambda_p).\end{aligned}$$

But

$$t = \frac{1}{\rho_p\left(\dfrac{1}{t(z/p)}\right)} \equiv t\left(\frac{z}{p}\right)^{q^\nu} \qquad (\mathrm{mod}\, p).$$

Therefore, as before,

$$\rho_p((j \circ \alpha_b)^*\,(t)) \equiv j^*\,(t) \qquad (\mathrm{mod}\, \lambda_p)$$

since λ_p divides p. But

$$\Phi_p(X, j) = (X - j \circ \alpha_p) \prod_{\substack{b \\ \deg b < \nu}} (X - j \circ \alpha_b).$$

Hence

$$\Phi_p(X, j) \equiv (X - \rho_p(j))(X^{q^\nu} - j) \qquad (\operatorname{mod} \lambda_p)$$

since $\rho_p(X) \equiv X^{q^\nu} \pmod{p}$, and so

$$\Phi_p(X, j) \equiv (X - \rho_p(j))(\rho_p(X) - j) \qquad (\operatorname{mod} p)$$

by the same argument as in [6, p. 58].

We now apply the modular equation to the isogenies. A finite A-module M is called *cyclic* of A-degree $n \in A$ if M is isomorphic to the cyclic module $A/(n)$. Then just the same method in [6] gives

THEOREM 3.2. *Let ϕ, ϕ' be Drinfeld modules over C. There exists an isogeny*

$$u \colon \phi' \to \phi$$

with cyclic kernel of A-degree n iff $j_{\phi'}$ is a root of the equation

$$\Phi_n(X, j_\phi) = 0.$$

Remark. In [1], an analog of another form of the Kronecker congruence relation, which can be applied to the theory of complex multiplication of Drinfeld modules of rank 2, is proved, using the action of ideal class groups of an order in an imaginary quadratic function field on the isomorphism classes of Drinfeld modules of rank 2.

Let $p = p(T)$ be a monic irreducible polynomial of degree ν in A, and $\mathcal{O}$ an order in an imaginary quadratic function field. For a proper ideal $\mathfrak{a}$ of $\mathcal{O}$, we let $j(\mathfrak{a})$ denote the j-invariant of the Drinfeld module associated to the rank 2 A-lattice $\mathfrak{a}$. Then

Kronecker Congruence Relation. Suppose that p does not divide the conductor of $\mathcal{O}$ such that

$$p\mathcal{O} = \mathfrak{p}\mathfrak{p}', \qquad \mathfrak{p} \neq \mathfrak{p}'.$$

Let M be a finite Galois extension of K containing all the numbers $j(\mathfrak{c})$, where $\mathfrak{c}$ ranges over the proper ideals of $\mathcal{O}$. Then

$$\rho_p(j(\mathfrak{a})) \equiv j(\mathfrak{a})^{q^\nu} \equiv j(\mathfrak{p}'\mathfrak{a}) \qquad (\operatorname{mod} \mathfrak{p}\mathcal{O}_M).$$

Here $\mathcal{O}_M$ is the integral closure of A in M.

APPENDIX

The Evaluation of $\psi(n)$. Let $\varphi(n)$ be the number of elements in $(A/(n))^*$. Then

(1) $\varphi(n_1 n_2) = \varphi(n_1)\,\varphi(n_2)$ if $(n_1, n_2) = (1)$.

(2) For an irreducible polynomial p of degree v,

$$\varphi(p^r) = q^{vr} - q^{v(r-1)}.$$

Given a monic d dividing n, $a = n/d$ is determined. Let $(e) = (a, d)$ where e is monic. Then there are

$$q^{\deg d - \deg e} \cdot \varphi(e)$$

possible values for b, so

$$\psi(n) = \sum_{d \mid n} q^{\deg d - \deg e} \varphi(e).$$

LEMMA 1. *Let n_1 and n_2 be two monic polynomials in A. If $(n_1, n_2) = (1)$, then*

$$\psi(n_1 n_2) = \psi(n_1)\,\psi(n_2).$$

Proof. Let $d_1 \mid n_1$, $d_2 \mid n_2$. Then $a_1 = n_1/d_1$, $a_2 = n_2/d_2$ are determined and so are $e_1 = (a_1, d_1)$ and $e_2 = (a_2, d_2)$. Since $(n_1, n_2) = 1$, $e_1 e_2 = (a_1 a_2, d_1 d_2)$. So

$$\begin{aligned}
\psi(n_1 n_2) &= \sum_{\substack{d_1 \mid n_1 \\ d_2 \mid n_2}} q^{\deg (d_1 d_2) - \deg (e_1 e_2)} \varphi(e_1 e_2) \\
&= \sum_{\substack{d_1 \mid n_1 \\ d_2 \mid n_2}} q^{\deg d_1 - \deg e_1 + \deg d_2 - \deg e_2} \varphi(e_1)\,\varphi(e_2) \\
&= \psi(n_1)\,\psi(n_2).
\end{aligned}$$

So it suffices to consider $n = p^r$ a prime power. Following the method in [5, p. 53], we see that

$$\psi(p^r) = q^{r \deg p}\left(1 + \frac{1}{q^{\deg p}}\right).$$

Hence

$$\psi(n) = q^{\deg n} \prod_{p \mid n}\left(1 + \frac{1}{q^{\deg p}}\right).$$

References

1. S. Bae and J. K. Koo, On the singular Drinfeld modules of rank 2, *Math. Z.* (1992), to appear.
2. E.-U. Gekeler, Zur Arithmetik von Drinfeld-Moduln, *Math. Ann.* **262** (1983), 167–182.
3. E.-U. Gekeler, On the coefficients of Drinfeld modular forms, *Invent. Math.* **93** (1988), 667–700.
4. D. Hayes, Explicit class field theory for rational function fields, *Trans. Amer. Math. Soc.* **189** (1974), 77–91.
5. D. Hayes, Explicit class fields theory in Global function field, *in* "Studies in Algebra and Number Theory" (G. C. Rota, Ed.), Academic Press, New York, 1979.
6. S. Lang, Elliptic functions, *in* "Graduate Texts in Math.," Vol. 112, Springer-Verlag, New York/Berlin/Heidelberg, 1987.
7. J. P. Serre and J. Tate, Good reduction of abelian verieties, *Ann. of Math.* **88** (1968).
8. G. Shimura, Introduction to the arithmetic theory of automorphic functions, *Publ. Math. Soc. Japan* **11** (1971).