COMPOSITIO MATHEMATICA

DAVID R. DORMAN

On singular moduli for rank 2 Drinfeld modules

Compositio Mathematica, tome 80, n° 3 (1991), p. 235-256

<http://www.numdam.org/item?id=CM_1991__80_3_235_0>

Compositio Mathematica **80**: 235–256, 1991.

On singular moduli for rank 2 Drinfeld modules

DAVID R. DORMAN[1]

Department of Mathematics, Middlebury College, Middlebury, Vermont 05753, U.S.A.

Received 22 February 1990; accepted 18 January 1991

0. Introduction

Let $\mathbb{F}_q$ be the finite field having $q = p^s$ elements and for simplicity we assume $p > 2$. Let $k = \mathbb{F}_q(T)$ (resp. $A = \mathbb{F}_q[T]$) be the field of rational functions (resp. the ring of polynomials) in the indeterminant T. Let C be the completion of an algebraic closure $\bar{k}_\infty$ of the completion k_∞, of k, at the infinite place $\infty = 1/T$. Finally, let $\mathfrak{H} = C - k_\infty$ denote the "upper half plane".

$\mathrm{GL}_2(A)$ acts on $\mathfrak{H}$ via linear fractional transformations and there is an analytic parametrization of the rigid analytic space $\mathrm{GL}_2(A)\backslash\mathfrak{H}$ to C (cf. Drin[3])

$$j: \mathrm{GL}_2(A)\backslash\mathfrak{H} \tilde{\to} C.$$

The function j is analogous to the classical j function of Dedekind and has many interesting arithmetic properties. In particular, for arguments $\tau \in \mathfrak{H}$ that are imaginary quadratic over k, that is, $k(\tau)$ is quadratic over k and ∞ is non-split in $k(\tau)$, the values $j(\tau)$ are algebraic integers over A. Such integers are called singular invariants since they correspond to isomorphism invariants of rank 2 Drinfeld A-modules having complex multiplication by an order in an imaginary quadratic extension of k. In this paper we give the prime factorization of such invariants.

The factorization of differences of singular moduli associated to elliptic curves defined over number fields was accomplished by Gross and Zagier [6] in the case of prime discriminants and extended by the author [2] to the case of relatively prime composite discriminants. Thus it is natural to study the function field setting via rank 2 Drinfeld A-modules to investigate the similarities and differences between the two settings. While there are similarities to the classical setting there are many more technical difficulties in the function field setting arising from the fact that there are $q-1$ units in $\mathbb{F}_q[T]$ while there are only 2 units in $\mathbb{Z}$. Consequently we consider only the factorization of $j(\tau)$ in this paper and hope to treat the more general case of differences of singular moduli in a

[1]Research partially supported by NSF grants RII-8610679 and DMS-8903463 and NSA grant MDA904-89-H-2033.

subsequent paper. Nevertheless, the case we study reveals all of the essential ingredients of the general setting while avoiding the burdensome detail.

1. The main result

Let $\tau \in \mathfrak{H}$ be imaginary quadratic over k. So τ satisfies a quadratic polynomial $a\tau^2 + b\tau + c = 0$ with $a, b, c \in A$ and relatively prime, and ∞ is non-split in the extension $k(\tau)/k$. The discriminant $b^2 - 4ac = d = \mathrm{disc}(\tau)$ is well defined up to the square of a unit in $\mathbb{F}_q$ and depends only on τ. So once and for all we consider d fixed and write $d = \mathrm{disc}(\tau)$. Moreover, we require that d be fundamental, that is d is also a field discriminant, or equivalently, square free. Let $h = h(d)$ denote the class number of the order $A[\sqrt{d}]$.

We now set some notation, relate some facts regarding $j(\tau)$, and state our main result.

Let $K = k(\tau) = k(\sqrt{d})$ so $d = d_K$ where d_K is the discriminant of K. Finally, let $\mathcal{O}_K$ be the integral closure of A in K.

Many interesting arithmetic facts regarding singular moduli of Drinfeld modules are contained in Gekeler [4] and Hayes [7]. Those most pertinent to our study are:

1. $j(\tau)$ is an algebraic integer of degree h over A.
2. The field $K(j(\tau))$ is the Hilbert class field of K which is split completely over K, and it is therefore abelian over K.
3. There exists a rank 2 Drinfeld A-module φ defined over $K(j(\tau))$, having complex multiplication by $\mathcal{O}_K$ with j invariant $j_\varphi = j(\tau)$.
4. The h Galois conjugates of $j(\tau)$ over $\mathcal{O}$ are the values $j(\tau')$ where τ' runs through the roots of all the distinct primitive quadratic polynomials of discriminant d.

Consider the product

$$J(d) = \prod_{\substack{[\tau] \\ \mathrm{disc}(\tau) = d}} j(\tau) \tag{1.1}$$

where $[\tau]$ denotes an equivalence class modulo $\mathrm{GL}_2(A)$. The norm $J(d)$ is in A and so has degree one over k.

The principal result of this study is a formula for $\mathrm{ord}_\mathfrak{p} J(d)$ where $\mathfrak{p}$ is any non-zero prime ideal of A.

To state the result we must introduce the constant field extension of k. Fix a non-square unit $u \in \mathbb{F}_q^*$. Then $H = k(\sqrt{u}) = \mathbb{F}_{q^2}(T)$ is the constant field extension and our formula for $\mathrm{ord}_\mathfrak{p} J(d)$ will depend on the arithmetic of $\mathfrak{p}$ in $\mathbb{F}_{q^2}(T)$. The

reason is that the rank 2 Drinfeld A-module, ρ, with complex multiplication by $\mathcal{O} = \mathbb{F}_{q^2}[T]$ has $j = 0$, so that (1.1) actually becomes

$$J(d) = \prod_{\substack{[\tau] \\ \operatorname{disc}(\tau) = d}} (j(\tau) - j(\rho)) = \prod_{\substack{[\tau] \\ \operatorname{disc}(\tau) = d}} (j(\tau) - 0) \tag{1.2}$$

and we are finding primes $\mathfrak{p}$ where φ becomes congruent to ρ. In practice this turns out to be possible due to the fact that $\mathbb{F}_{q^2}(T)$ has class number 1 and the endomorphism ring of ρ is easy to determine. The details are given in Section 5.

We remark that the techniques involved here should generalize to products of differences of j values, namely

$$J(d, d') = \prod_{\substack{[\tau],[\tau'] \\ \operatorname{disc}(\tau) = d \\ \operatorname{disc}(\tau') = d'}} (j(\tau) - j(\tau'))$$

with d and d' relatively prime. However, the flavor of the arguments can be gleaned from the case we treat and we hope to publish the results of the general case in a subsequent paper.

Next let $\mathfrak{a}$ be an ideal of A having factorization

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{m_i} \prod_j \mathfrak{q}_j^{n_j}$$

with $\mathfrak{p}_i$ split and $\mathfrak{q}_j$ inert in $\mathbb{F}_{q^2}(T)$. Define $R(\mathfrak{a})$ to be the number of ideals of $\mathbb{F}_{q^2}(T)$ having norm the ideal $\mathfrak{a}$. $R(\mathfrak{a})$ can be calculated by

$$R(\mathfrak{a}) = \begin{cases} \prod (m_i + 1) & \text{if all the } n_j \text{ are even} \\ 0 & \text{otherwise.} \end{cases} \tag{1.3}$$

THEOREM 1.4. *Let* $\mathfrak{p}$ *be a non-zero prime ideal of* A *and let* π *be a generator for* $\mathfrak{p}$. *Then*

$$\operatorname{ord}_{\mathfrak{p}} J(d) = \frac{q+1}{2} \sum_{m \in A} \sum_{n \geqslant 1} R\left(\frac{d - um^2}{\pi^{2n-1}}\right)$$

In Section 5 we show that this sum is finite. We also remark that the quantity $(d - um^2)/\pi^{2n-1}$ is to be interpreted as the generator of an ideal $\mathfrak{a}$. If $\mathfrak{a}$ is integral then $R(\mathfrak{a})$ is determined by (1.3) otherwise $R(\mathfrak{a})$ equals 0. In Section 5 we show a necessary condition for the above quotient to generate an integral ideal $\mathfrak{a}$ with $R(\mathfrak{a}) \neq 0$ is that degree $\pi \leqslant$ degree d. Having noted this we immediately obtain the striking corollary

COROLLARY 1.5. *If* $\pi \mid J(d)$ *then* degree $\pi \leqslant$ degree d.

Our proof relies on the work of Gekeler [4] connecting the endomorphism ring of a supersingular Drinfeld A-module of rank 2 in characteristic $\mathfrak{p}$ with a maximal order in the definite quaternion algebra over A ramified only at $\mathfrak{p}$ and ∞.

Section 3 relates the important facts concerning quaternion algebras that we will need. Section 4 contains the principal results of this paper leading up to the proof of Theorem 1.2 which is in Section 5. Finally, in Section 6 we provide a number of computational examples.

2. Drinfeld modules

We briefly review some of the basic facts regarding Drinfeld modules. Detailed discussions can be found in Deligne and Husemöller [1], Drinfeld [3], Gekeler [4], and Hayes [7].

Let L be a finite extension of k_∞. An A-lattice Λ in L is by definition a discrete, finitely generated A-submodule in L^{sep} which is invariant under the action of $\text{Gal}(L^{\text{sep}}/L)$. Thus Λ is projective and has fixed rank $= r$. The exponential function defined on Λ by

$$\mathrm{e}_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{z}{\lambda}\right)$$

is an entire, additive function and induces an isomorphism from $\bar{L}/\Lambda$ onto $\bar{L}$. Thus, we obtain an A-module structure on $\bar{L}$. Given $a \in A$, $a \neq 0$, by comparing divisors we find that

$$\mathrm{e}_\Lambda(az) = c \prod_{b \in 1/a\Lambda/\Lambda} (\mathrm{e}_\Lambda(z) - \mathrm{e}_\Lambda(b)) = \varphi_a(\mathrm{e}_\Lambda(z))$$

where φ_a is a polynomial function and c is a constant in C.

Having begun with an analytic object we obtain a purely algebraic one, φ_a. Moreover, we obtain an A-module structure on the additive group scheme $\mathbb{G}_a$ given by the natural embedding

$$\varphi\colon A \to \mathrm{End}_L(\mathbb{G}_a).$$

$\mathrm{End}_L(\mathbb{G}_a)$ is the ring of additive polynomials in an indeterminant X where the multiplication is given through substitution. Moreover, $\mathrm{End}_L(\mathbb{G}_a)$ is naturally isomorphic to the ring $L\{F\}$ of twisted polynomials generated by the elements of L and the Frobenius F satisfying the commutation relation $c^p F = Fc$ for all $c \in L$.

We finally can define Drinfeld modules.

DEFINITION 2.1. Let L be a field over A with a fixed morphism $\gamma: A \to L$. A Drinfeld A-module over L is a homomorphism $\varphi: A \to L\{F\}$, $a \mapsto \varphi_a$, such that the constant term of φ_a is $\gamma(a)$ and the image of φ is not contained in L, that is, φ is not $\varphi: A \to L \subset L\{F\}$.

φ is said to have generic or ∞ characteristic if γ is injective otherwise φ has characteristic equal to the kernel of γ.

A key theorem given below is due to Drinfeld [3, Thm. 3.1].

THEOREM 2.2. *If L is a finite extension of k_∞, then the category of Drinfeld A-modules of rank r over L is isomorphic to the category of rank r A-lattices over L.*

For k a Drinfeld A-module is completely determined by the image of T, that is, a Drinfeld A-module of rank r is given by the polynomial

$$\varphi_T = \sum_{0 \leqslant i \leqslant r} a_i F^i = \sum_{0 \leqslant i \leqslant r} a_i X^{q^i};\ a_i \in L,\ a_r \neq 0.$$

In particular the polynomial representation of a rank 2 Drinfeld module over k can be thought of as either

$$\varphi_T(F) = \gamma(T) + aF + bF^2; \quad a, b \in Lb \neq 0$$

or

$$\varphi_T(X) = \gamma(T)X + aX^q + bX^{q^2}; \quad a, b \in L,\ b \neq 0.$$

We write $\varphi_T(X) = (a, b)$, and following Drinfeld's original terminology we henceforth call rank 2 Drinfeld A-modules elliptic A-modules.

Let L/k be a finite extension of fields and let φ and ψ be two Drinfeld A-modules over L. A morphism between φ and ψ is an element $c \in L\{F\}$ with $c \circ \varphi_a = \psi_a \circ c$ for all a in A. An isomorphism is given by $c \in L^*$ such that $\psi_a = c \circ \varphi_a \circ c^{-1}$. Non-trivial morphisms exist only between Drinfeld A-modules of the same rank and they are called isogenies.

The isomorphism invariant of elliptic A-modules is revealed in the following lemma.

LEMMA 2.3. (1) *Two elliptic A-modules $\varphi = (a_1, b_1)$ and $\psi = (a_2, b_2)$ are isomorphic if and only if there exists $c \in L^*$ so that $a_1 = c^{q-1}a_2$ and $b_1 = c^{q^2-1}b_2$.*

(2) *Let L be algebraically closed. Then φ and ψ are isomorphic if and only if*

$$a_1^{q+1}/b_1 = a_2^{q+1}/b_2.$$

Proof. Gekeler [4, p. 175]. □

Since the quantities defined in part (2) of the above lemma are isomorphism

invariants for elliptic A-modules we define the j-invariant of $\varphi(a, b)$ as

$$j = j(\varphi) = a^{q+1}/b. \tag{2.4}$$

The analytic description in terms of lattices is as follows. Let Λ be the A-lattice in C corresponding to φ. Through multiplication by an element $c \in C^*$ one can write the lattice in the form $\langle w, 1\rangle = Aw \oplus A$ with $w \in \mathfrak{H}$. The functions

$$a_i: w \mapsto a_i \text{ (elliptic } A\text{-module associated to } \langle w, 1\rangle) \ (i = 1, 2)$$

are modular forms of weight $q^i - 1$ on $\mathfrak{H}$ and the modular function given by (2.4) is the analytic parametrization

$$j: \mathrm{GL}_2(A)\backslash\mathfrak{H} \to C$$

mentioned in Section 0, Gekeler [4, pp. 175–176].

There is a reduction theory for Drinfeld A-modules which is quite analogous to that for elliptic curves. Let L be a field, v an additive discrete valuation of L and $\mathcal{O}_v$ the valuation ring of v and assume that $\mathcal{O}_v$ has an A-algebra structure. Let φ_a be a Drinfeld A-module over L. We say that φ_a has integral coefficients at v if $\varphi_a \in \mathcal{O}_v[F]$ for all $a \in A$ and then the homomorphism $a \mapsto \varphi_a \pmod{\mathfrak{m}_v}$ defines a Drinfeld module over the residue field $\mathcal{O}_v/\mathfrak{m}_v$.

Finally an elliptic A-module φ, or the invariant $j(\varphi)$, is called singular when $\mathrm{End}_C(\varphi) \neq A$. As expected, the j-invariant of an elliptic A-module is called supersingular at a prime $\mathfrak{p}$ if the endomorphism ring of the corresponding reduced elliptic module is isomorphic to a maximal order in a quaternion algebra over k ramified at $\mathfrak{p}$ and ∞.

3. A counting theorem

Let W be a complete local A-module which is also a discrete valuation ring. Let μ be a prime of W and normalize the valuation v so that $v(\mu) = 1$. Assume the residue field $W/\mu W$ is algebraically closed and that the structure map $\gamma: A \to W$ is injective and the composition map $\eta: A \to W/\mu W$ has kernel $\mathfrak{p}A$. Let φ and φ' be two elliptic A-modules defined over W having good reduction modulo μ. Let $j = j(\varphi)$ and $j' = j(\varphi')$ be the modular invariants of φ and φ'.

The main result of this section, Theorem 3.5, is a formula for $v(j - j')$. This gives us a method of counting the number of isomorphisms between two elliptic A-modules.

Consider the elliptic A-module φ. Since φ has a good reduction modulo μ it has an equation of the form

$$\varphi = \varphi_T\colon TX + aX^q + bX^{q^2}$$

with $a \in W$ and $b \in W^*$. Recall, the j-invariant is $j = j(\varphi) = a^{q+1}/b$. We first count automorphisms modulo μ^n.

PROPOSITION 3.1.

$$\mathrm{Card}(\mathrm{Aut}_{W/\mu^n W}(\varphi)) = \begin{cases} q-1 & \text{if } a \not\equiv 0 \pmod{\mu^n} \\ q^2-1 & \text{if } a \equiv 0 \pmod{\mu^n}. \end{cases}$$

Proof. By the discussion preceding Theorem 2.2 as well as lemma 2.1 it is easy to see that

$$\mathrm{Aut}_{W/\mu^n W}(\varphi) = \left\{ \begin{matrix} \omega \in (W/\mu^n W)^*\colon b \equiv \omega q^{2-1} b \\ \text{and } a \equiv \omega^{q-1} a \pmod{\mu^n} \end{matrix} \right\}.$$

Since $b \in W^*$ the first congruence can be divided by b to yield

$$\omega^{q^2-1} \equiv 1 \pmod{\mu^n}. \tag{3.2}$$

Thus,

$$\mathrm{Aut}_{W/\mu^n W}(\varphi) \subseteq (W/\mu^n W)^*_{q^2-1} \cong \mathbb{Z}/(q^2-1)\mathbb{Z}.$$

The last isomorphism comes from the exact sequence

$$1 \to K_n \to (W/\mu^n W)^* \to (W/\mu W)^* \to 1.$$

The kernel K_n is unipotent and has no non-$\mathfrak{p}$ torsion hence the (q^2-1)-torsion of $(W/\mu^n W)^*$ and $(W/\mu W)^*$ are the same.

Now if $a \equiv 0 \pmod{\mu^n}$ the only restriction on ω is the congruence (3.2). This congruence has q^2-1 solutions giving the second half of the claim. If $a \not\equiv 0 \pmod{\mu^n}$ dividing the second congruence by a yields the additional condition that $\omega^{q-1} \equiv 1 \pmod{\mu^n}$. This congruence has $q-1$ solutions establishing the first part of the claim. □

Next consider a second elliptic A-module defined over W and having good reduction mod μ. Let its equation be

$$\varphi' = \varphi_{T'}\colon TX + a'X^q + b'X^{q^2}$$

so that its j invariant is $j' = j(\varphi') = (a')^{q+1}/b'$. We are interested in computing $\mathrm{Card}(\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi'))$. Clearly this number may equal zero and this occurs precisely when there does not exist an element $\omega \in (W/\mu^n W)^*$ such that $a \equiv \omega^{q-1}a'$ and $b \equiv \omega^{q^2-1}b'$ (mod μ^n). This case out of the way we have

PROPOSITION 3.3. *Assume* $\mathrm{Card}\{\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')\} \neq 0$. *Let*

$$\sigma \in \mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi') \quad \textit{and} \quad M = \{\sigma \circ \xi\colon \xi \in \mathrm{Aut}_{W/\mu^n W}(\varphi)\}.$$

Then $\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi') = M$.

Proof. Clearly $M \subseteq \mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')$. Now let $\eta \in \mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')$. Then $\sigma^{-1} \circ \eta = \tau \in \mathrm{Aut}_{W/\mu^n W}(\varphi)$ so $\eta = \sigma \circ \tau \in M$ proving the proposition. □

COROLLARY 3.4.

$$\mathrm{Card}\{\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')\} = 0,\ q-1,\ \text{or}\ q^2-1.$$

Proof. If the cardinality is 0 we are done. If not combining the results of Propositions 3.1 and 3.3 give the result. □

We now come to the principal result of this section, the computation of $v(j - j') = v((b'a^{q+1} - b(a')^{q+1})/bb')$.

THEOREM 3.5.

$$v(j - j') = \frac{1}{q-1} \cdot \sum_{n \geq 1} \mathrm{Card}\{\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')\}.$$

Proof. If φ and φ' are not isomorphic mod μ then both sides of the equation are 0 proving the result.

Consequently, assume φ and φ' are isomorphic mod μ. We may normalize these modules so that $b = b' = 1$. This can always be done since the equation $\lambda^{q^2-1} = b^{-1}$ can be solved in the algebraically closed field $W/\mu W$, and Hensel's lemma allow the solution to be lifted to W. So $j = a^{q+1}$ and $j' = a'^{q+1}$. Normalize

further by multiplying a and a' by an appropriate $(q+1)^{st}$ root of unity so that $v(a-a')$ is maximal.

By Proposition 3.1 we know the set

$$\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi') = \left\{ \begin{matrix} \omega \in (W/\mu^n W)^* : \omega^{q^2-1} \equiv 1 \,(\mathrm{mod}\, \mu^n) \\ \text{and } a\omega^{q-1} \equiv a' \,(\mathrm{mod}\, \mu^n) \end{matrix} \right\}$$

has cardinality $q-1$ if $a \not\equiv 0 \pmod{\mu^n}$ and q^2-1 if $a \equiv a' \equiv 0 \pmod{\mu^n}$.

Assume first that $a \not\equiv 0 \pmod{\mu^n}$. Then $a\omega^{q-1} \equiv a' \pmod{\mu^n}$ and raising to $q+1$ *gives* $a^{q+1}\omega^{q^2-1} \equiv (a')^{q+1} \pmod{\mu^n}$. However since $\omega^{q^2-1} \equiv 1 \pmod{\mu^n}$ it follows that $a^{q+1} \equiv (a')^{q+1} \pmod{\mu^n}$ yielding $j \equiv j' \pmod{\mu^n}$. Thus, $\mathrm{Card}\{\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')\}/q-1 = 1$.

Second, if $a \equiv a' \equiv 0 \pmod{\mu^n}$ but $a \not\equiv 0$ and $a' \not\equiv 0 \pmod{\mu^{n+1}}$ then $a^{q+1} \equiv (a')^{q+1} \pmod{\mu^{n+1}}$. Thus

$$j \equiv j' \,(\mathrm{mod}\, \mu^{n+1}) \quad \text{and} \quad \mathrm{Card}\{\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')\}/q-1 = q+1.$$

From this we see

$$\begin{aligned} v(j-j') &= v(a^{q+1} - (a')^{q+1}) \\ &= \sum_{k=1}^{q} v(a - \zeta^k a'); \ \zeta \text{ a primitive } (q+1)^{st} \text{ root of unity} \\ &= \frac{1}{q-1} \cdot \sum_{n \geq 0} \mathrm{Card}\{\mathrm{Iso}_{W/\mu^n W}(\varphi, \varphi')\} \text{ as claimed.} \end{aligned}$$

□

4. A lifting theorem

The principal result of this section is a lifting theorem that will enable us to translate information regarding endomorphisms between two reduced elliptic modules in characteristic p back to the generic characteristic setting. The notation continues from the previous sections.

Consider the pair (φ_0, α_0) where φ_0 is an elliptic module defined over $W/\mu^n W$ and α_0 is a $W/\mu^n W$ endomorphism of φ_0. The main result of this section, Theorem 4.2, gives criteria telling exactly when (φ_0, α_0) can be lifted to a pair (φ, α) where φ is an elliptic module over W and α is a W endomorphism of φ.

Assume the subring $A[\alpha_0] \subseteq \mathrm{End}_{W/\mu^n W}(\varphi_0)$ has rank 2 as an A-module and is integrally closed in its quotient field. An alternate way of expressing this is to associate to α_0 its trace $t = \alpha_0 + \alpha_0^\vee$ and norm $n = \alpha_0 \alpha_0^\vee$ which are viewed as

multiplication by fixed elements in $\mathrm{End}_{W/\mu^n W}(\varphi_0)$. Then the assumption is that $d = t^2 - 4n$ is a fundamental imaginary discriminant.

On the tangent space $\mathrm{Lie}(\varphi_0)$, α_0 induces multiplication by an element w_0 which satisfies the integral quadratic equation $x^2 - tx + n = 0$. Thus, a necessary condition for lifting (φ_0, α_0) to W is the existence of an element $w \in W$ satisfying

$$\begin{cases} w \equiv w_0 \,(\mathrm{mod}\, \mu^n) \\ w^2 - tw + n = 0 \end{cases} \tag{4.1}$$

since the induced action of the lifted endomorphism on $\mathrm{Lie}(\varphi_0)$ will give rise to such an element. This condition is sufficient.

THEOREM 4.2. *Suppose there exists an element w satisfying* (4.1). *Then there is an elliptic A-module φ defined over W and an endomorphism α of φ such that*

(a) $(\varphi, \alpha) \equiv (\varphi_0, \alpha_0) \,(\mathrm{mod}\, \mu^n)$
(b) α *induces multiplication by w on* $\mathrm{Lie}(\varphi)$.

Moreover, if (φ', α') is any other lifting there is a commutative diagram

$$\begin{array}{ccc} \varphi & \overrightarrow{\alpha} & \varphi \\ \downarrow\wr & & \downarrow\wr \\ \varphi' & \overrightarrow{\alpha'} & \varphi' \end{array}$$

of morphisms over W.

Proof. Let $\mathfrak{p}$ be the characteristic of φ modulo μW and let $\mathbb{F}_q(T)_{\mathfrak{p}}$ and $A_{\mathfrak{p}}$ denote the localizations of $\mathbb{F}_q(T)$ and A at $\mathfrak{p}$. Drinfeld's [3] deformation theory shows it suffices to construct a lifting $\hat{\varphi}$ to W of the $\mathfrak{p}$-divisible group $\hat{\varphi}_0$ of φ_0 and an endomorphism lifting $\hat{\alpha}_0$. Gross [5] showed how this lifting can be accomplished.

In the ordinary case take $\hat{\varphi} \cong \hat{H} \times (\mathbb{F}_q(T)_{\mathfrak{p}}/A_{\mathfrak{p}})$ where $\hat{H}$ is the lifting of the unique formal $A_{\mathfrak{p}}$-module of height 1 and $\mathbb{F}_q(T)_{\mathfrak{p}}/A_{\mathfrak{p}}$ is the unique étale $A_{\mathfrak{p}}$-module of height 1.

In the supersingular case $\mathrm{End}_{W/\mu W}(\varphi_0) \cong R_{\mathfrak{p}}$ a maximal order in the definite quaternion algebra ramified at $\mathfrak{p}$ and ∞. Using Lubin–Tate theory Gross showed that there exists a canonical lifting of $\hat{\varphi}_0$ to a Lubin–Tate formal $A_{\mathfrak{p}}[\alpha_0]$-module of height 2 over W with endomorphism $\alpha[x] = wx + \cdots$. This lifting is unique up to W isomorphism. □

5. Factorization of singular moduli in function fields

Fix an element $u \in \mathbb{F}_q^*$ which is not a square. Then

$$H = \mathbb{F}_q(T, \sqrt{u}) = \mathbb{F}_{q^2}(T)$$

is the constant field extension of $\mathbb{F}_q(T)$. It is well known that H has class number 1, or equivalently H is its own Hilbert class field. Let $\mathcal{O}_H = \mathbb{F}_{q^2}[T]$. Let d be a fundamental negative discriminant such that $\mathbb{F}_q(T, \sqrt{d}) \neq H$. We now consider the factorization of $j(\tau)$ when $\operatorname{disc}(\tau) = d$. Fix a finite prime v of H having characteristic $\mathfrak{p}$ and denote by $B = B_v$ the completion of the maximal, unramified, extension of the ring of v integers in H. Let $W = W_v = B[s]$ where s is a fixed element which satisfies an integral quadratic equation of discriminant d. Let e be the ramification index of W/B and μ a uniformizer for W. Consider the norm of $j(\tau)$, namely the algebraic integer

$$J(d) = \prod_{\substack{[\tau] \\ \operatorname{disc}(\tau) = d}} j(\tau). \tag{5.1}$$

The product is taken over representative classes modulo $\mathrm{GL}_2(A)$. This integer lies in A and our goal is to compute $\operatorname{ord}_{\mathfrak{p}}(\alpha)$ for every non-zero prime ideal $\mathfrak{p}$ of A. To accomplish this we introduce the auxiliary elliptic A-module

$$\rho: T + F^2. \tag{5.2}$$

Up to isomorphism this is the unique elliptic A-module defined over W with complex multiplication by $\mathcal{O}_H$ and invariant $j(\rho) = 0$. It is clear that ρ has good reduction and by theorems of Drinfeld [3] and Takahashi [8] ρ is unique up to W isomorphism since the residue field is algebraically closed. Similarly, for each τ of discriminant d let φ denote the elliptic module defined over W having complex multiplication by $B[s]$ and invariant $j(\varphi) = j(\tau)$.

Since the j-invariant associated with ρ equals 0, (5.1) is nothing other than the algebraic integer

$$J(d) = \prod_{\substack{[\tau] \\ \operatorname{disc}(\tau) = d}} (j(\tau) - 0). \tag{5.3}$$

Consequently, by Theorem 3.5 it follows that

$$\operatorname{ord}_v J(d) = \frac{1}{e(q-1)} \sum_{\operatorname{disc}(\tau) = d} \sum_{n \geq 1} \operatorname{Card}\{\operatorname{Iso}_{W/\mu^n W}(\rho, \varphi)\}.$$

Thus, the problem is reduced to counting isomorphisms $\omega: \rho \tilde{\to} \varphi \pmod{\mu^n}$. Such an isomorphism gives rise to an endomorphism $s_\omega = \omega^{-1} \circ s \circ \omega$ of $\rho \pmod{\mu^n}$ belonging to the set

$$S_{n,v} = \begin{Bmatrix} \alpha_0 \in \mathrm{End}_{W/\mu^n W}(\rho)\colon \mathrm{Tr}(\alpha_0) = \mathrm{Tr}(s),\ \mathbb{N}(\alpha_0) = \mathbb{N}(s), \\ \alpha_0 \text{ induces multiplication by } s \text{ on } \mathrm{Lie}(\rho). \end{Bmatrix}. \tag{5.4}$$

Notice that s_ω is the same as $s_{\zeta\omega}$ for any $\zeta \in \mathbb{F}_q^*$ since A is in the center of the endomorphism ring of ρ. Thus the map from $\mathrm{Iso}_{W/\mu^n W}(\rho, \varphi)$ to $S_{n,v}$ is a $q-1$ to 1.

By Theorem 4.2 every element α_0 of $S_{n,v}$ is of the form s_α for some isomorphism $\alpha: \rho \to \varphi \pmod{\mu^n}$ to an elliptic module φ with complex multiplication by $B[s]$. This can be seen since the pair (ρ, α_0) can be lifted to (ψ, α) over W and since ψ has complex multiplication by $B[\alpha] = B[s]$ it is isomorphic to one of the elliptic modules φ by a map $\beta: \psi \tilde{\to} \varphi$ with $\alpha = \beta^{-1} \circ s \circ \beta$. Reducing this map (mod μ^n) shows that $\alpha_0 = s_\alpha$. Theorem 4.2 also shows the uniqueness of φ over W as well as the uniqueness of u up to W isomorphism. Thus,

$$\mathrm{ord}_v J(d) = \frac{1}{e} \sum_{n \geqslant 1} \mathrm{Card}\, S_{n,v}. \tag{5.5}$$

Our task then is to determine $S_{n,v}$. Since H/k is an unramified extension the only concern is with primes $\mathfrak{p}$ that either split or remain inert in H. This first case is handled by

PROPOSITION 5.6. *Suppose* $\mathfrak{p}$ *splits in* H. *Then* $\mathrm{ord}_v J(d) = 0$.

Proof. The elliptic A-module ρ has ordinary reduction (mod μ) in this situation. Thus $\mathrm{End}_{W/\mu^n}(\rho) = \mathcal{O}_H$ for all $n \geqslant 1$ Drinfeld [3]. Since $\mathcal{O}_H$ has no elements of discriminant d, Card $S_{n,v} = 0$ for all $n \geqslant 1$. □

From now on suppose that $\mathfrak{p}$ is inert in H. Then ρ has supersingular reduction modulo μ and $\mathrm{End}_{W/\mu W}(\rho)$ is isomorphic to a maximal order in the definite quaternion algebra $\mathbb{D}$ over k which is ramified at $\mathfrak{p}$ and ∞ [4, 179].

We give an explicit description of this quaternion algebra $\mathbb{D}$ and its unique maximal order containing $\mathcal{O}_H$. Since $\mathfrak{p}$ is inert in H it follows that its degree is odd. Let $\mathfrak{p} = (\pi)$ where π is any generator of the ideal $\mathfrak{p}$. The idele character $\chi = \Pi \chi_v$ associated with the extension H/k is unramified everywhere and consequently each of the χ_v is trivial on units. Thus the product formula gives $\chi_\infty(\pi)\chi_\mathfrak{p}(\pi) = 1$ since π is a unit at all places other than $\mathfrak{p}$ and ∞. Moreover $\chi_\infty(\pi) = (-1)^{\deg(\pi)} = -1$ as $\deg(\pi)$ is odd. It follows that $\chi_\mathfrak{p}(\pi) = -1$. Thus, the quaternion algebra $\mathbb{D}$ is given by two generators i and j where $i^2 = u$ and $j^2 = \pi$.

$\mathbb{D}$ can be realized as a matrix algebra with the description

$$\mathbb{D} = \left\{[\alpha, \beta] = \begin{bmatrix} \alpha & \beta \\ \pi\bar{\beta} & \bar{\alpha} \end{bmatrix}; \alpha, \beta \in H\right\}.$$

Here $^-$ is complex conjugation. Since the class number of H is 1 there is only 1 maximal order in $\mathbb{D}$ in which $\mathcal{O}_H$ embeds optimally namely,

$$R = R_1 = \{[\alpha, \beta] \in \mathbb{D} : \alpha, \beta \in \mathcal{O}_H\}.$$

R admits a filtration

$$R_n = \{[\alpha, \beta] \in R : \beta \equiv 0 \,(\mathrm{mod}\, \mathfrak{p}^{n-1})\}. \tag{5.7}$$

LEMMA 5.8. *Assume* $\mathfrak{p} \nmid d$. *Then* $e = 1$ *and*

1. $\mathrm{End}_{W/\mu^n W}(\varphi_T) = R_n$,
2. *Suppose that* $[\alpha, \beta] \in R_n$ *has trace* $\mathrm{Tr}(s)$ *and norm* $\mathbb{N}(s)$. *Then there exists an integral polynomial* m *and an element* $\gamma \in \mathcal{O}_H$ *solving the Diophantine equation*

$$um^2 + 4\pi^{2n-1}\mathbb{N}\gamma = d.$$

Conversely, suppose we have a solution (m, γ) *to the above equation with* $m \in A$ *and* γ *an element of* $\mathcal{O}_H$. *Then we obtain an element* $[\alpha, \beta] \in R_n$ *with trace* $= \mathrm{Tr}(s)$ *and norm* $= \mathbb{N}(s)$.

Proof. The first statement follows from Drinfeld [3] and Gross [5]. Considering the second claim suppose $[\alpha, \beta] \in R_n$ has trace $= \mathrm{Tr}(s)$ and norm $= \mathbb{N}(s)$. Write $\alpha = x + y\sqrt{u}$. Since trace $[\alpha, \beta] = \mathrm{Tr}(s)$ it follows that $x = \frac{1}{2}\mathrm{Tr}(s)$ so we write $\alpha = \frac{1}{2}\mathrm{Tr}(s) + y\sqrt{u}$. Write $\beta = \pi^{n-1}\gamma$ with $\gamma \in \mathcal{O}_H$. The norm condition implies $\frac{1}{4}\mathrm{Tr}(s)^2 - y^2u - \pi^{2n-1}\mathbb{N}\gamma = \mathbb{N}(s)$. Now s satisfies an integral quadratic equation of discriminant d so a bit of algebra yields

$$-4y^2u - 4\pi^{2n-1}\mathbb{N}\gamma = 4\mathbb{N}(s) - \mathrm{Tr}(s)^2 = -d. \tag{5.9}$$

Set $m = 2y$ and multiply through by -1 to get

$$um^2 + 4\pi^{2n-1}\mathbb{N}\gamma = d. \tag{5.10}$$

Conversely, suppose that we have a solution (m, γ) to (5.10) subject to the hypotheses. Then by reversing the above definitions one obtains an element in R_n having the stated trace and norm proving our claim. □

It is crucial to observe that (5.10) has only finitely many solutions since $\deg(um^2)$ and $\deg(\mathbb{N}\gamma)$ are bounded. To see this first notice that $\mathbb{N}\gamma$ is of even degree since it is a norm from $\mathbb{F}_{q^2}(T)$ so that $\deg(4\pi^{2n-1}\mathbb{N}\gamma)$ is odd. Now if $\deg(d)$ is odd, then $\deg(um^2) < \frac{1}{2}\deg(d)$ so $\deg(um^2)$ is bounded. In addition, $\deg(4\pi^{2n-1}\mathbb{N}\gamma) = \deg(ud)$ so $\deg(\mathbb{N}\gamma)$ is bounded. If, on the other hand, $\deg(d)$ is even then $\deg(um^2)$ is fixed since it must equal $\deg(d)$, and $\deg(4\pi^{2n-1}\mathbb{N}\gamma) < \deg(d)$ and so $\deg(\mathbb{N}\gamma)$ is bounded.

The determination of the cardinality of $S_{n,v}$ can be made by counting certain pairs $(m, \mathfrak{b})$ where $m \in A$ and $\mathfrak{b}$ is an integral $\mathcal{O}_H$ ideal. Notice that a solution to (5.10) is the same as stating that $\mathbb{N}\gamma$ equals $(d-um^2)/\pi^{2n-1}$ as elements of $\mathbb{F}_q(T)$. Now set $\mathfrak{b} = (\gamma)$. Then, $\mathbb{N}\mathfrak{b}$ is the ideal of $\mathbb{F}_q(T)$ generated by $(d-um^2)/\pi^{2n-1}$.

Thus a necessary condition for the existence of γ is that the ideal $\langle (d-um^2)/\pi^{2n-1}\rangle$ be the norm of some ideal $\mathfrak{b}=(\gamma)$. Notice that the ideal is necessarily principal since $\mathbb{F}_{q^2}(T)$ has class number 1. Using Hilbert's Theorem 90 one can easily show the norm map $\mathbb{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}: \mathbb{F}_{q^2}^* \twoheadrightarrow \mathbb{F}_q^*$ is surjective. Thus, for a given ideal $\mathfrak{b}$ there are $q+1$ generators of $\mathfrak{b}$ with norm equal to $\mathbb{N}\gamma$, namely $\varepsilon\gamma$ where $\varepsilon \in \mathbb{F}_{q^2}^*$ with $\mathbb{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}\varepsilon = 1$.

Having made these observations the sum (5.4) can be determined provided that an endomorphism $[\alpha, \beta]$ arising from a pair $(m, \mathfrak{b})$ induces multiplication by s on $\mathrm{Lie}(E)$. Assume $[\alpha, \beta]$ has this property. Since $e = 1$ the dual endomorphism $[\alpha, \beta]^\vee = [\bar{\alpha}, -\beta]$ induces multiplication by $\bar{s} \not\equiv s \pmod{\mu}$. Consequently, exactly half of the endomorphisms arising from a single solution to (5.10) contribute to this sum.

Thus, we have proved the following proposition

PROPOSITION 5.11. *The cardinality of $S_{n,v}$ is equal to $\frac{1}{2}(q+1)$ times the number of pairs $(m, \mathfrak{b})$ where $m \in A$ and $\mathfrak{b}$ is an integral ideal of $\mathcal{O}$ such that there is equality of ideals $\mathbb{N}\mathfrak{b} = \langle (d-um^2)/\pi^{2n-1}\rangle$.*

Next consider the case $\mathfrak{p} \mid d$. Let v, W, and B be as above. In this situation $[W: B] = 2$ and $e = 2$. Moreover $\mu \mid \mathfrak{p}$ and $\mu^2 = g\mathfrak{p}$ where g is a unit in B.

As before, ρ has supersingular reduction mod μ so for the fixed v there exists an integral ideal $\mathfrak{a}$ of $\mathcal{O}_H$ so that

$$\mathrm{End}_{B/\mathfrak{p}^n B}(\rho) = R_n$$

where R_n is given by (5.7). However, we must describe $\mathrm{End}_{W/\mathfrak{p}^n}(\rho)$. Since ρ acquires no new endomorphisms over W the ring $\mathrm{End}_{B/\mathfrak{p}^n}(\rho)$ accounts for all of the endomorphisms of ρ. Thus

$$\mathrm{End}_{W/\mu^n W}(\rho) = \mathrm{End}_{B/(\mu^n W \cap B)}(\rho).$$

Since $\mu^2 = g\mathfrak{p}$ it follows that

$$\mathrm{End}_{W/\mu^{2n-1}W}(\rho) = \mathrm{End}_{W/\mu^{2n}W}(\rho) \ (n = 1, 2, 3),$$

So

$$\mathrm{End}_{W/\mu^n W}(\rho) = \{[\alpha, \beta] \in \mathbb{D} : \alpha \in \mathcal{O}_H, \beta \in \mathfrak{p}^{r-1}\}$$

where $r = [(n+1)/2]$ the greatest integer in $(n+1)/2$.

As in the case above, an element $\alpha_0 = [\alpha, \beta] \in \mathrm{End}_{W/\mu^n W}(\rho)$ having trace $= \mathrm{Tr}(s)$ and norm $= \mathbb{N}(s)$ gives rise to a pair (m, γ) with $um \in A$ and γ an element of $\mathcal{O}_H$ solving

$$um^2 + 4\pi^{2r-1}\mathbb{N}\gamma = d.$$

Since $\mathfrak{p} \mid d$ this equation can only hold when $m = 1$, thus $n \leqslant 2$. Now α_0 induces multiplication by an element of W/μ on $\mathrm{Lie}(\rho)$. However, the reduction of s (mod μ^2) is in the residue field so $S_{n,1}$ is empty for $n \geqslant 2$. Consequently, the problem is reduced to computing the cardinality of S_1. Thus we are concerned with the equation

$$um^2 + 4\pi\mathbb{N}\gamma = d. \tag{5.12}$$

As before we can transfer the count to one of ideals by determining the number of $\mathcal{O}_H$ ideals $\mathfrak{b}$ satisfying the property that

$$\mathbb{N}\mathfrak{b} = \langle (d - um^2)/\pi \rangle.$$

Now let $(m, \mathfrak{b})$ be a solution to (5.10) with $m \in A$ and $\mathfrak{b}$ an integral $\mathcal{O}_H$ ideal. Then arguing as above it is easy to see that this solution leads to $2(q+1)$ endomorphisms in the case $m \neq 0$ and $q+1$ solutions when $m = 0$.

To see when an endomorphism $[\alpha, \beta]$ induces multiplication by s on $\mathrm{Lie}(E)$ recall that $[W : A] = 2$ and $e = 2$. So $[\alpha, \beta]^\vee = [\bar{\alpha}, -\beta]$ induces multiplication by $\bar{s} \equiv s$ (mod μ) on $\mathrm{Lie}(E)$. Thus we count all of the endomorphisms arising from a single solution rather than only half as in case 1.

Let N_1 be the number of pairs $(m, \mathfrak{b})$ with $m \in A$ and $\mathfrak{b}$ an integral ideal of $\mathcal{O}_H$ such that $um^2 + 4\pi\mathbb{N}\mathfrak{b} = d$ holds and let N_2 be the number of pairs $(0, \mathfrak{b})$ such that $4\pi\mathbb{N}\mathfrak{b} = d$ holds. We have proved

THEOREM 5.13. *Let v, W, and B be as above and assume $\mathfrak{p} \mid d$. Then $e = 2$ and S_n is empty for $n \geqslant 2$. The cardinality of S_1 is equal to $(q+1)(2N_1 + N_2)$.* □

The above results can now be nicely synthesized into one coherent formula given by the final theorem.

Let $\mathfrak{a}$ be an ideal of A having factorization

$$\mathfrak{a} = \prod_i \mathfrak{p}_i^{m_i} \prod_j \mathfrak{q}_j^{n_j}$$

with $\mathfrak{p}_i$ split and $\mathfrak{q}_j$ inert in $\mathbb{F}_{q^2}(T)$.

Define $R(\mathfrak{a})$ to be the number of principal ideals of $\mathbb{F}_{q^2}(T)$ having norm $\mathfrak{a}$. This number is given by the formula

$$R(\mathfrak{a}) = \begin{cases} \Pi(m_i+1) & \text{if all the } n_j \text{ are even} \\ 0 & \text{otherwise.} \end{cases} \tag{5.14}$$

THEOREM 5.15. *Let* $\mathfrak{p}$ *be a prime of* K *and let* π *be a generator for* $\mathfrak{p}$. *Then*

$$\operatorname{ord}_{\mathfrak{p}} J(d) = \frac{q+1}{2} \sum_{m \in A} \sum_{n \geqslant 1} R\left(\frac{d - um^2}{\pi^{2n-1}}\right).$$

By the discussion immediately following Lemma 5.8 we obtain the corollary

COROLLARY 5.16. *If* $\pi \mid J(d)$, *then* degree $\pi \leqslant$ degree d. □

6. Some computational examples

The formula given in Theorem 5.15 is quite practical. Hayes has provided us with a number of useful examples on which this formula can easily be verified by hand computation. In all cases we list the prime power q, the non-square unit u, and the discriminant d. Then, for each $m \in A$ the factors of $ud - m^2$ give all of the possible primes entering into $\operatorname{ord}_{\mathfrak{p}}(J(d))$. Then, after dividing $ud - m^2$ by the appropriate factor it is an easy matter to compute $R(\langle (ud-m^2)/u\pi^{2n-1} \rangle)$ using (5.14).

EXAMPLE 6.1. We begin with the general case of the discriminant $d = T$ a first degree polynomial. Let $q = p^s$, $p > 2$. Then the integers, $\mathcal{O}$, in the extension $K = k(\sqrt{T})$ have the form $\mathcal{O} = \mathbb{F}_q[y]$ where $y^2 = T$ and have class number equal to 1. Let u be a fixed non-square unit in $\mathbb{F}_q$.

m	m^2	$d - um^2$
0	0	T
$\pm a$	a^2	$T - ua^2$

From the last column we see the only possible factors of $J(d)$ are T and $T - ua^2$.

Suppose $\pi = T$. The only occurrence of π is when $m = 0$ so we see

$$\operatorname{ord}_T J(d) = (q+1) \cdot \tfrac{1}{2} \cdot R(1) = (q+1) \cdot \tfrac{1}{2} \cdot 1 = (q+1) \cdot \tfrac{1}{2}.$$

Now suppose $\pi = T - ua^2$. The only occurrence of π is when $m = \pm a$. Thus,

$$\operatorname{ord}_{T-ua^2} J(d) = (q+1)\cdot 2 \cdot \tfrac{1}{2}R(1) = (q+1).$$

The 2 in the above expression arises from counting $\pm a$. Consequently, up to a unit we see

$$\begin{aligned} J(d) = J(T) &= T^{(q+1)/2} \cdot \Bigg(\prod_{\text{squares}} (T - ua^2) \Bigg)^{q+1} \\ &= T^{(q+1)/2}(T^{(q-1)/2} + 1)^{q+1}. \end{aligned} \tag{6.2}$$

Suppose $y^2 = T$. The elliptic A-module of discriminant $d = T$ is given by

$$\begin{aligned} \varphi_T &= T + (y + y^q)F + F^2 \\ &= TX + (y + y^q)X^q + X^{q^2}. \end{aligned}$$

Using (2.4) it is immediate that

$$\begin{aligned} J(d) = J(T) &= (y + y^q)^{q+1} \\ &= T^{(q+1)/2}(T^{(q-1)/2} + 1)^{q+1}, \end{aligned} \tag{6.3}$$

which verifies the above computation up to a unit.

REMARK. The fact that (6.2) is determined only up to a unit in $\mathbb{F}_q^*$ implies that the quotient of (6.2) and (6.3) determines a unit in $\mathbb{F}_q^*$. This phenomenon, namely, that the quotient of the computed factorization of $J(d)$ by the one arising from the associated elliptic A-module determines a unit in $\mathbb{F}_q^*$ is repeated in the subsequent examples. Our calculations in all cases show this unit to be 1, however we cannot at this time prove this.

In the remaining examples we always take $q = 3$ *and* $u = -1$.

EXAMPLE 6.4. Let the discriminant be $d = T^3 - T - 1$ so $d = T^3 - T - 1$.

m	m^2	$d - um^2$
0	0	$(T^3 - T - 1)$
± 1	1	$T(T-1)(T+1)$
$\pm T$	T^2	$(T+1)^2(T-1)$
$\pm(T+1)$	$T^2 - T + 1$	$T(T-1)^2$
$\pm(T-1)$	$T^2 + T + 1$	$T^2(T+1)$

The last column in the table shows the only possible primes occurring in the factorization of $J(d)$ are T^3-T-1, T, $T-1$, and $T+1$.

Suppose $\pi = T^3-T-1$. The only occurrence of π is when $m = 0$ thus

$$\mathrm{ord}_{T^3-T-1}J(d) = (q+1)/e \cdot R(1) = 2 \cdot 1 = 2.$$

Suppose $\pi = T$. The possibilities for m are ± 1, $\pm(T+1)$ and $\pm(T-1)$. Consequently,

$$\begin{aligned}\mathrm{ord}_T J(d) &= 2((q+1)\cdot\tfrac{1}{2}(R((T-1)(T+1)) + R((T-1)^2) + R(T(T+1))))\\ &= 2\cdot 2(0+1+0) = 4.\end{aligned}$$

The values in the above equation are explained as follows. The initial 2 comes from the counting of both the plus and minus signs on m. The first and the third values of the R function are 0 since the arguments in both cases are products of inert primes to odd powers. Finally the value of the second R function is 1 since the argument is an inert prime to an even power.

Now suppose $\pi = T-1$. Then

$$\begin{aligned}\mathrm{ord}_{T-1}J(d) &= 2((q+1)\cdot\tfrac{1}{2}(R(T(T+1)) + R((T+1)^2) + R(T(T-1))))\\ &= 2\cdot 2(0+1+0) = 4.\end{aligned}$$

The reasoning follows the same lines as when $\pi = T$.

Finally suppose $\pi = T+1$. Then

$$\begin{aligned}\mathrm{ord}_{T+1}J(d) &= 2((q+1)\cdot\tfrac{1}{2}(R(T(T-1)) + R((T-1)(T+1)) + R(T^2)))\\ &= 2\cdot 2(0+0+1) = 4.\end{aligned}$$

Again the analysis is similar to the above, and we conclude that up to a unit

$$J(d) = J(T^3-T-1) = (T^3-T-1)^2[T(T-1)(T+1)]^4.$$

To verify this by direct computation set $y^2 = T^3-T-1$ then the elliptic module over A is given by $\varphi_T\colon T + y(T^3-T)X^3 + X^9$. Again using (2.4) the j-invariant can be calculated directly by hand and gives

$$j(\varphi_T) = (y(T^3-T))^4 = (T^3-T-1)^2[T(T-1)(T+1)]^4.$$

The true power of Theorem 5.15 comes when the class number is greater than 1. In the next two cases the class number is 2. The following example is

particularly nice since it illustrates all of the possible phenomenon that can occur.

EXAMPLE 6.5. Let $d = T(T^2 - T - 1)$.

m	m^2	$d - um^2$
0	0	$T(T^2 - T - 1)$
± 1	1	$(T-1)^2(T+1)$
$\pm T$	T^2	$T(T+1)(T-1)$
$\pm(T+1)$	$T^2 - T + 1$	$(T-1)(T^2+T-1)$
$\pm(T-1)$	$T^2 + T + 1$	$(T+1)^3$

From the last column we see the only possible primes entering into the factorization are T, T^2-T-1, $T-1$, $T+1$, and T^2+T-1.

First suppose $\pi = T$. Then

$$\begin{aligned}\operatorname{ord}_T J(d) &= (q+1)\cdot\tfrac{1}{2}(R(T^2-T-1) + 2\cdot R((T-1)(T+1)))\\ &= 2(2+2\cdot 0) = 4.\end{aligned}$$

$R(T^2-T-1)=2$ since T^2-T-1 is a split prime and $R((T-1)(T+1)) = 0$ since the argument is the product of two inert primes to odd degree. The 2 preceding that R value comes from both signs on the $m = \pm T$.

Now suppose $\pi = T^2 - T - 1$. Then

$$\operatorname{ord}_{T^2-T-1} J(d) = (q+1)\cdot\tfrac{1}{2}R(T) = 2\cdot 0 = 0$$

where $R(T) = 0$ since T is inert in H.

Next, suppose $\pi = T - 1$. Then

$$\begin{aligned}\operatorname{ord}_T J(d) &= 2((q+1)\cdot\tfrac{1}{2}(R((T-1)(T+1)) + R(T(T+1)) + R(T^2+T-1)))\\ &= 2\cdot 2(0+0+2) = 8.\end{aligned}$$

Where the first two R values equal 0 since the arguments are products of inert primes to odd degree, and last R value is 2 since T^2+T-1 is split in H.

Now suppose $\pi = T + 1$. Then

$$\begin{aligned}\operatorname{ord}_{T+1} J(d) &= 2((q+1)\cdot\tfrac{1}{2}(R((T-1)^2) + R(T(T-1)) + R((T+1)^2) + R(1)))\\ &= 2\cdot 2(1+0+1+1) = 12.\end{aligned}$$

This is the most interesting case so we will explain it in detail. $R((T-1)^2)=1$ since the argument is an inert prime to an even degree. $R(T(T-1))=0$ since the argument is the product of two inert primes to odd degree. The last two R's occur when $m=\pm(T-1)$. Recall we are looking to compute

$$\mathbb{N}\gamma=(d-um^2)/\pi^{2n-1}=(T+1)^3/(T+1)^{2n-1}.$$

This is possible for $n=1$ and 2. The case $n=1$ accounts for $R((T+1)^2)=1$ since $T+1$ occurs to even power, and the case $n=2$ accounts for $R(1)=1$.

Finally, suppose $\pi=T^2+T-1$. Since π is a split prime in H we know a priori by Proposition 5.5 that $\mathrm{ord}_{T^2+T-1}J(d)=0$. Nevertheless, our formula still holds since

$$\begin{aligned}\mathrm{ord}_{T^2+T-1}J(d)&=2(q+1)\cdot\tfrac{1}{2}R(T-1)\\&=2\cdot 2\cdot 0=0.\end{aligned}$$

Where $R(T-1)=0$ because $T-1$ is inert in H. Thus, up to a unit, it follows that

$$J(d)=T^4(T-1)^8(T+1)^{12}.$$

Direct verification is now more difficult since the class number is two. Let $y^2=T(T^2-T-1)$. Then the ring of integers in the Hilbert class field of $K=k(\sqrt{y})$ is $\mathbb{F}_3[T,w,z]$, where $w^2=T^2-T-1$, $z^2=T$, and $wz=y$. A fundamental unit is given by $\eta=1+T+w$ and $\eta\bar{\eta}=-1$. The associated elliptic A-module is given by

$$\begin{aligned}\varphi_T&=T+\eta z(1+\eta^{-4}T)F+F^2\\&=TX+\eta z(1+\eta^{-4}T)X^3+X^9.\end{aligned}$$

Thus, $j(d)=\eta^4T^2(1+\eta^{-4}T)^4$.

Taking norms yields

$$J(d)=T^4\mathbb{N}(1+\eta^{-4}T)^4,$$

and a hand computation gives

$$J(d)=T^4(T-1)^8(T+1)^{12}$$

as predicted.

Our final example is

EXAMPLE 6.6. Let $d = T - T^2$

m	m^2	$d - um^2$
0	0	$T(1-T)$
± 1	1	$(T^2 - T - 1)$
$\pm T$	T^2	T
$\pm(T+1)$	$T^2 - T + 1$	1
$\pm(T-1)$	$T^2 + T + 1$	$(1-T)$

From the last column we see the only possible primes contributing to the factorization are T, $1-T$, and T^2-T-1. Without further adieu we dismiss T^2-T-1 since it is a split prime in $\mathbb{F}_{q^2}(T)$.

Suppose $\pi = T$. Then

$$\begin{aligned}\operatorname{ord}_T J(d) &= (q+1)\cdot\tfrac{1}{2}(R(1-T) + 2\cdot R(1)) \\ &= 2(0 + 2\cdot 1) = 4.\end{aligned}$$

Where $R(1-T)=0$ since $1-T$ is inert and appears to odd power.

Suppose $\pi = 1 - T$. Then

$$\begin{aligned}\operatorname{ord}_{1-T} J(d) &= (q+1)\cdot\tfrac{1}{2}(R(T) + 2\cdot R(1)) \\ &= 2(0 + 2\cdot 1) = 4.\end{aligned}$$

Where $R(T)=0$ since T is inert and appears to odd power.

Let $y^2 = T - T^2$. The elliptic module over A is defined by

$$\varphi_T = T + y\eta F + \bar{\eta}F^2 = TX + y\eta X^3 + \bar{\eta}X^9,$$

where $\eta = 1 + T + iy$, $i^2 = -1$, and $\eta\bar{\eta} = 1$. Then

$$j = (y\eta)^4/\bar{\eta} = \eta^5(T - T^2)^2.$$

Taking norms gives

$$J(d) = T^4(1 - T)^4$$

as expected.

7. Acknowledgements

I would like to express my gratitude to the Department of Mathematics at Harvard University for my visits during summers and during the academic year 1989–1990. Much of the research for this paper was conducted during these stimulating visits.

I am delighted to thank D.S. Dummit, E.-U. Gekeler, D. Goss, B. Mazur, F.O. McGuinness, and D. Thakur for many useful discussions and suggestions. I would especially like to acknowledge and thank B. Gross and D. Hayes for their help and encouragement during the course of this study. Finally I am grateful to the referee for making thoughtful recommendations concerning style and content.

Remark added in proof

Hayes has informed me that he can now prove that the unit occurring in the above examples is always equal to 1.

References

1. P. Deligne and D. Husemöller, Survey of Drinfeld Modules, *Current Trends in Arithmetical Algebraic Geometry* (ed. K. Ribet) *Contemporary Mathematics* 67 (1986) American Math. Soc., Providence, Rhode Island.
2. D. R. Dorman, Special values of the elliptic modular function and factorization formulae, *J. reine und ang. Math.* 383 (1988), 207–220.
3. V. Drinfeld, Elliptic Modules (Russian) *Math. Sbornik* 94 (1974) 594–627, English translation: *Math. USSR-Sbornik* 23 (1976) 561–592.
4. E.-U. Gekeler, Zur Arithmetic von Drinfeld-Moduln, *Math. Ann.* 262 (1983) 167–182.
5. B. H. Gross, On canonical and quasi-canonical liftings, *Invent. Math.* 84 (1986) 321–326.
6. B.H. Gross and D.B. Zagier, On singular moduli, *J. reine und ang. Math.* 355 (1985), 191–220.
7. David R. Hayes, Explicit class field theory in global function fields, in (ed. G. Rota) *Studies in Algebra and Number Theory, Advances in Mathematical Supplementary Studies* 16 (1979) 173–217, Academic Press.
8. Toyofumi Takahashi, Good reduction of elliptic modules, *J. Math. Soc. Japan* 34(2) (1982) 475–487.