MATHEMATICS OF COMPUTATION
VOLUME 62, NUMBER 206
APRIL 1994, PAGES 875–883

RANK-ONE DRINFELD MODULES ON ELLIPTIC CURVES

D. S. DUMMIT AND DAVID HAYES

ABSTRACT. The sgn-normalized rank-one Drinfeld modules ϕ associated with all elliptic curves E over $\mathbb{F}_q$ for $4 \leq q \leq 13$ are computed in explicit form. (Such ϕ for $q < 4$ were computed previously.) These computations verify a conjecture of Dorman on the norm of $j(\phi) = a^{q+1}$ and also suggest some interesting new properties of ϕ. We prove Dorman's conjecture in the ramified case. We also prove the formula $\deg N(a) = q(h_k - 1 + q)$, where $N(a)$ is the norm of a and h_k is the class number of $k = \mathbb{F}_q(E)$. We describe a remarkable conjectural property of the trace of a in even characteristic that holds in all the examples.

In his recent paper [1] on the factorization of norms of j-invariants of rank-two Drinfeld modules with complex multiplications, D. Dorman conjectured that such norms are monic elements of $\mathbb{F}_q[x]$. Dorman computed the j-invariants in several examples and found his conjecture valid in all of them. For this purpose, he used the rank-one examples from [6]. The first extensive computational test of the conjecture was carried out by one of us, Dummit, who computed the rank-one Drinfeld modules associated with all elliptic curves over $\mathbb{F}_q$ with $q \leq 13$ (see §3 below). The results of these computations may be found on the microfiche card included at the end of this issue. Inspired by these computations, one of us, Hayes, proved Dorman's conjecture when the infinite place is ramified (see §2 below). In §3, we describe an algorithm for computing the rank-one Drinfeld modules associated with any hyperelliptic curve over $\mathbb{F}_q$, and we prove some basic attributes of the algorithm. In §4, we prove formulas for the degrees of the norm and trace of the j-invariants of Drinfeld modules associated with elliptic curves. These formulas were first observed computationally. They suggest a number of interesting questions for elliptic curves with complex multiplications in characteristic zero. In §5, we state some conjectures about the remarkable form of the trace term in characteristic two. These conjectures are supported by all our computations.

1. NOTATIONS

Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial of *odd* degree $n \geq 3$, and let $k/\mathbb{F}_q(x)$ be the hyperelliptic extension obtained by adjoining a root of

$$y^2 = f(x) \tag{1.1}$$

Received by the editor September 10, 1992.
1991 *Mathematics Subject Classification.* Primary 11G15, 11G20, 11R58.
The first author was supported in part by NSA and NSF grants, and the second author by NSF grant DMS-8702716.

©1994 American Mathematical Society
0025-5718/94 $1.00 + $.25 per page

if q is odd, or

$$y^2 + a_1xy + a_3y = f(x) \qquad (a_1, a_3 \in \mathbb{F}_q, \text{ not both zero}) \tag{1.2}$$

if q is even, to the field of rational functions $\mathbb{F}_q(x)$. If q is odd, we require that $f(x)$ be squarefree, which means that the affine plane curve defined by (1.1) has no singular points. For q even, we restrict $f(x)$ and a_1, a_3 also by requiring that the affine curve defined by (1.2) be nonsingular. In either case, the affine coordinate ring $\mathbf{A} = \mathbb{F}_q[x, y]$ is integrally closed in k.

Since n is odd, the infinite place of $\mathbb{F}_q(x)$ ramifies in $k/\mathbb{F}_q(x)$. Let ∞ denote its unique extension to k, and let k_∞ be the completion of k at ∞. It is clear from either (1.1) or (1.2) that $\pi_\infty = x^{(n-1)/2}/y$ is a uniformizer in k_∞ and therefore determines a unique sign function $\operatorname{sgn}: k_\infty \to \mathbb{F}_q$ such that $\operatorname{sgn}(\pi_\infty) = 1$. Since π_∞^2/x is a 1-unit at ∞, we conclude that $\operatorname{sgn}(x) = 1$, and so also $\operatorname{sgn}(y) = 1$.

The ring $\mathbf{A}$ is the ring of functions in k which are holomorphic away from ∞. Let ϕ be a sgn-normalized rank-one Drinfeld $\mathbf{A}$-module defined over the algebraic closure of k. Then ϕ is determined by its values

$$\phi_x = x + a\mathbf{F} + \mathbf{F}^2, \tag{1.3}$$

$$\phi_y = y + c_1\mathbf{F} + c_2\mathbf{F}^2 + \cdots + c_{n-1}\mathbf{F}^{n-1} + c_n\mathbf{F}^n, \tag{1.4}$$

where $c_n = \operatorname{sgn}(y) = 1$, the coefficients $a, c_1, c_2, \ldots, c_{n-1}$ are elements of the Hilbert class field H of $\mathbf{A}$, and $\mathbf{F}$ is the Frobenius endomorphism satisfying $\mathbf{F}c = c^q\mathbf{F}$ for any c in the algebraic closure of k. Since ∞ is of degree one, the degree $h_k = [H : k]$ is the class number of the function field k as well as the class number of the Dedekind domain $\mathbf{A}$. Let $\mathbf{B}$ be the integral closure of $\mathbf{A}$ in H. One knows that the coefficients of ϕ_x and ϕ_y actually belong to $\mathbf{B}$. In fact, a generates H over k, and the coefficients of ϕ_x and ϕ_y generate $\mathbf{B}$ over $\mathbf{A}$. For the theory of rank-one Drinfeld modules, the reader may consult [10] or Chapter IV of [3].

Equation (1.3) defines a rank-two Drinfeld $\mathbb{F}_q[x]$-module, and we may understand (1.4) to mean that this rank-two module allows "complex multiplications" by $\mathbf{A}$. The isomorphism invariant $j(\phi) = a^{q+1}$ (cf. [4]) is the Drinfeld analogue for the j-invariants of elliptic curves in characteristic zero which admit complex multiplications by the full ring of integers of an imaginary quadratic number field. The results in [1] provide an explicit formula for the ideal factorization of the norm

$$J(\phi) = \operatorname{Norm}_{H \to \mathbb{F}_q(x)}(j(\phi))$$

in $\mathbb{F}_q[x]$ for odd q, the Drinfeld analogue of the remarkable results of Gross and Zagier [5]. Dorman conjectured that $J(\phi)$ is monic (or "positive" with respect to the sign function sgn), which implies that his explicit formula actually computes $J(\phi)$ as a polynomial in x.

2. Proof of Dorman's conjecture

We shall show that a is *totally positive* for the sign function sgn. This means that $\operatorname{sgn}(\mathbf{e}(a)) = 1$ for every embedding $\mathbf{e}: H \to k_\infty$. As a corollary, we see that $\operatorname{Norm}_{H \to k}(a)$ is sgn-positive, and hence that $J(\phi)$ is a positive (or monic) polynomial in x. Our main tool is

Theorem 1. *Let $K_x = H(\Lambda_x)$, where Λ_x is the $\mathbb{F}_q$-vector space of x-torsion points for the* **A***-module ϕ. In fact, K_x is the splitting field of*

$$\phi_x(t) = xt + at^q + t^{q^2} \tag{2.1}$$

over H. Then K_x/k is abelian, and the inertia group G_∞ at ∞ in $\mathrm{Gal}(K_x/k)$ is isomorphic to $\mathbb{F}_q^\times$. The "real subfield" K_x^+ of K_x is the fixed field of G_∞. The k-place ∞ splits completely in K_x^+/k, and the group of norms from $K_x^\times$ down to $(K_x^+)^\times$ consists of totally positive elements of K_x^+.

This theorem follows from the results in §4 of [8]. The field K_x is a "cyclotomic function field" over k, and the last statement of the theorem is the analogue of the fact that norms from any cyclotomic extension of $\mathbb{Q}$ into its real subfield are totally positive.

Let $\lambda \in \Lambda_x$ generate the x-torsion over $\mathbf{A}$, and put $Y = -\lambda^{q-1}$. By Theorem 4.17 of [8], Y is a norm from K_x and is therefore a totally positive element of K_x^+. Now by (2.1), $x - aY + Y^{q+1} = 0$, which implies that

$$a = xY^{-1} + Y^q. \tag{2.2}$$

Let $\mathbf{v}_\infty$ be the normalized valuation induced on K_x^+ by some fixed embedding $\mathbf{e}$ of K_x^+ into k_∞. Since $\mathrm{sgn}(x) = 1$ by choice of sgn, a is a sum of two positive elements in the embedding $\mathbf{e}$. Therefore, a will also be positive in $\mathbf{e}$ if these two elements have different valuations in k_∞, i.e., if

$$\mathbf{v}_\infty(Y^q) = \mathbf{v}_\infty(xY^{-1}) = -2 - \mathbf{v}_\infty(Y)$$

is false. But this equality implies that $\mathbf{v}_\infty(Y) = -2/(q+1)$, which is impossible as ∞ is unramified in K_x^+/k.

3. The algorithm

Let R be any k-algebra. Since x and y generate the ring $\mathbf{A}$ as an $\mathbb{F}_q$-algebra, producing a sgn-normalized rank-one Drinfeld $\mathbf{A}$-module over R is equivalent to producing two polynomials ϕ_x and ϕ_y with coefficients in R as in equations (1.3) and (1.4), so that the map defined by $x \mapsto \phi_x$, $y \mapsto \phi_y$ is a homomorphism of $\mathbf{A}$ into the noncommutative ring of twisted polynomials in the Frobenius endomorphism $\mathbf{F}$ with left-coefficients in R. A necessary condition for such a map to be a homomorphism is that $\phi_x\phi_y = \phi_y\phi_x$, and the key to the explicit computation of such modules is the observation in [9] that this necessary commutativity relation is also sufficient. One quick proof of this fact (due to M. Rosen) goes as follows. Suppose $G(x, y) = 0$ for some polynomial $G(X, Y) \in \mathbb{F}_q[X, Y]$. Since the constant term of the twisted polynomial $G(\phi_x, \phi_y)$ is $G(x, y) = 0$, the lowest-order term of $G(\phi_x, \phi_y)$ is of the form $d_m\mathbf{F}^m$ for some $m \geq 1$. Since ϕ_x and ϕ_y commute by assumption, $\phi_x G(\phi_x, \phi_y) = G(\phi_x, \phi_y)\phi_x$, and comparing coefficients of the lowest-order terms gives $xd_m = d_m x^{q^m}$, and so $d_m = 0$. Hence, $G(\phi_x, \phi_y) = 0$, showing that the homomorphism from the polynomial ring $\mathbb{F}_q[X, Y]$ to the twisted polynomial ring in $\mathbf{F}$ with left-coefficients in R defined by $X \mapsto \phi_x$, $Y \mapsto \phi_y$ factors through $\mathbf{A}$.

This reduces the computation of Drinfeld $\mathbf{A}$-modules over R to the determination of two twisted polynomials as in (1.3) and (1.4) that commute. Comparing coefficients of $\mathbf{F}^i$, $i = 0, 1, \ldots, n+1$, in the relation $\phi_x\phi_y = \phi_y\phi_x$

gives $n+2$ equations in the coefficients $a, c_1, c_2, \ldots, c_{n-1}$. The first of these equations is trivially satisfied, and the next $n-1$ equations recursively define $c_1, c_2, \ldots, c_{n-1}$ in terms of x, y, and a. Substituting these expressions for the c_i into the last two equations, one obtains two equations in a with coefficients in k. Clearing the denominators gives two polynomials $P(a)$ and $Q(a)$ with coefficients in $\mathbf{A}$ that a must satisfy, so that a must be a zero of the greatest common divisor $\Upsilon(a)$ of these two polynomials. Conversely, any zero a of $\Upsilon(a)$ in R (with corresponding c_i) defines two commuting twisted polynomials, hence defines a rank-one Drinfeld module. Hence, the explicit determination of the Drinfeld $\mathbf{A}$-modules over R is reduced to the computation of the greatest common divisor of $P(a)$ and $Q(a)$.

In the case $n = 3$, k is the function field of an elliptic curve, and the equations arising from the relation $\phi_x\phi_y = \phi_y\phi_x$ are

$$\begin{aligned} xy &= yx, \\ xc_1 + ay^q &= ay + c_1x^q, \\ xc_2 + ac_1^q + y^{q^2} &= y + c_1a^q + c_2x^{q^2}, \\ x + ac_2^q + c_1^{q^2} &= c_1 + c_2a^{q^2} + x^{q^3}, \\ a + c_2^{q^2} &= c_2 + a^{q^3}. \end{aligned} \tag{3.1}$$

As mentioned, the first of these equations is trivial, and the next two can be used to solve recursively for c_1, c_2 in terms of x, y, a:

$$c_1 = \frac{1}{x^q - x}a(y^q - y), \qquad c_2 = \frac{1}{x^{q^2} - x}(y^{q^2} - y + ac_1^q - c_1a^q). \tag{3.2}$$

When these expressions for c_1 and c_2 are substituted into the last two equations in (3.1) and the denominators cleared, we obtain two polynomials $P(a)$ (of degree q^2+q+1) and $Q(a)$ (of degree q^3+q^2) in a with coefficients in $\mathbf{A}$.

Theorem 2. (1) *The polynomial $\Upsilon(a)$ is integral with respect to $\mathbf{A}$ and is separable and irreducible of degree h_k, the class number of the field k.*

(2) ("*purity*") *If q is even, the coefficients of $\Upsilon(a)$ are elements of $\mathbb{F}_q[x]$. Suppose a specialized to a zero of $\Upsilon(a)$ in H. Then $\mathbb{F}_q(x, a)$ is an extension of $\mathbb{F}_q(x)$ of degree h_k; i.e., $\mathrm{Gal}(H/\mathbb{F}_q(x, a))$ splits the extension of $\mathrm{Gal}(H/\mathbb{F}_q(x))$ by $\mathrm{Gal}(H/k)$. If q is odd, the coefficient of a^{h-i} in $\Upsilon(a)$ is an element of $\mathbb{F}_q[x]$ if i is even, and an element of $y \cdot \mathbb{F}_q[x]$ if i is odd. Further, $\mathbb{F}_q(x, a^2)$ is an extension of $\mathbb{F}_q(x)$ of degree h_k; i.e., $\mathrm{Gal}(H/\mathbb{F}_q(x, a^2))$ splits the extension of $\mathrm{Gal}(H/\mathbb{F}_q(x))$ by $\mathrm{Gal}(H/k)$.*

Proof. The fact that $\Upsilon(a)$ is integral with respect to $\mathbf{A}$ is immediate from the fact that a is an integral element over $\mathbf{A}$. Since the zeros of $\Upsilon(a)$ in H define all of the sgn-normalized rank-one Drinfeld $\mathbf{A}$-modules, these zeros are all conjugate under the Galois group of H over k, so $\Upsilon(a)$ is a power of the minimal polynomial for a over k. The separability of $\Upsilon(a)$ is a consequence of the fact that over $\mathbf{B}$ the Drinfeld module defined by (1.3) and (1.4) is a universal rank-one Drinfeld $\mathbf{A}$-module (cf. Theorem 1 of [9]), as follows. Suppose $\Upsilon(a) = p(a)^e$ for some polynomial $p(a) \in \mathbf{A}[a]$ and some integer $e \geq 1$. Then there exists a Drinfeld $\mathbf{A}$-module over the k-algebra $R = k[z]/p(z)^e$. By the universality of ϕ, there exists a homomorphism from $\mathbf{B}$ to R extending the

inclusion map of $\mathbf{A}$ into k and mapping a to $z \in R$ that carries the Drinfeld module on $\mathbf{B}$ to the Drinfeld module on R. Since this map carries $p(a)$ $(a \in \mathbf{B})$ onto $p(z) \in R$, $p(a) = 0$ implies $p(z) = 0$ in R, and so $e = 1$ and $p(z)$ must be separable.

To prove (2), let $\mathrm{Gal}(k/\mathbb{F}_q(x)) = \{1, \tau\}$, $\tau^2 = 1$, and let τ be extended in some way to an automorphism of $H/\mathbb{F}_q(x)$. Let $\mathscr{D}$ be the set of sgn-normalized Drinfeld $\mathbf{A}$-modules, and let $\mathscr{D}_* = \tau \circ \mathscr{D} \circ \tau$. The elements of $\mathscr{D}_*$ are also normalized $\mathbf{A}$-modules. If q is even, then $\mathscr{D}_* = \mathscr{D}$, whereas if q is odd, then $\mathscr{D}_*$ consists of the sgn_*-normalized $\mathbf{A}$-modules, where $\mathrm{sgn}_*(x/y) = -1$.

Assume first that q is odd, and choose ξ such that $\xi^{1-q} = -1$. Then $\xi\phi\xi^{-1} \in \mathscr{D}_*$ and so $\xi\phi\xi^{-1} = \tau \circ (\sigma\phi) \circ \tau$ for some $\sigma \in \mathrm{Gal}(H/k)$. We see that

$$\xi\phi_x\xi^{-1} = x - a\mathbf{F} + \mathbf{F}^2 = x + a^{\sigma\tau}\mathbf{F} + \mathbf{F}^2,$$

which implies (replacing τ by $\sigma\tau$) that $a^\tau = -a$, so that $\tau^2 = 1$ on H. The subgroup of order 2 generated by τ splits the extension of $\mathrm{Gal}(H/\mathbb{F}_q(x))$ by $\mathrm{Gal}(H/k)$. Since a^2 is fixed by τ and a is obviously quadratic over the field generated by a^2, this implies that a^2 generates an extension over $\mathbb{F}_q(x)$ of degree h_k. The statements regarding the coefficients of $\Upsilon(a)$ are equivalent to $a^\tau = -a$.

If q is even, $\mathscr{D}_* = \mathscr{D}$, and the same argument shows that we can assume τ chosen so that $a^\tau = a$. Now a itself generates an extension over $\mathbb{F}_q(x)$ splitting the extension of $H/\mathbb{F}_q(x)$ by H/k. □

Remark. When $n = 3$, the results of Theorem 2 can also be proved directly from the explicit form of the relations in (3.1), as follows. If $\Upsilon(a)$ were not separable as a polynomial in a, then $P(a)$, $Q(a)$, $\partial P(a)/\partial a$, and $\partial Q(a)/\partial a$ would all have a zero in common. The second and third equations in (3.1) give

$$\frac{\partial c_1}{\partial a} = \frac{y^q - y}{x^q - x} = c_1/a, \qquad (x^{q^2} - x)\frac{\partial c_2}{\partial a} = c_1^q - a^q\frac{\partial c_1}{\partial a}.$$

From $\partial Q(a)/\partial a = 0$ we obtain $\partial c_2/\partial a = 1$. The second equation above together with (3.2) then gives

$$x^{q^2} - x = a^q\frac{y^{q^2} - y^q}{x^{q^2} - x^q} - a^q\frac{y^q - y}{x^q - x},$$

which implies that a generates a purely inseparable extension of k, contradicting the fact that a generates H.

For (2), observe first that the "purity" assertions regarding the coefficients of $\Upsilon(a)$ are valid for the polynomials $P(a)$ and $Q(a)$. Now if the coefficients of two polynomials α and β are "pure", then it is easy to see that in any polynomial division of α by β the coefficients of the remainder are also "pure". It follows that the coefficients of the greatest common divisor $\Upsilon(a)$ of $P(a)$ and $Q(a)$ have "pure" coefficients. The remaining statements in (2) follow easily from the purity.

The polynomials $\Upsilon(a)$ for all elliptic curves with $q \leq 13$ have been computed and for $4 \leq q \leq 13$ appear in the microfiche supplement (the cases $q = 2, 3$ can be found in [9]). See [2] for some examples of $\Upsilon(a)$ for genus-two curves. Even for relatively small q, the direct computation of the greatest

common divisor of the polynomials $P(a)$ and $Q(a)$ exceeds both patience and memory capacity. Instead, the computations were performed modulo primes $\pi(x)$ in $\mathbb{F}_q[x]$ (generally of degree 5) that are inert in the field k. For odd q the prime $\pi(x) \in \mathbb{F}_q[x]$ of degree N is inert in k if $f(x)^{(q^N-1)/2} \equiv -1 \bmod \pi(x)$, and since $q^N - 1 = (q-1)(1 + q + \cdots + q^{N-1})$, this power of $f(x)$ can be rapidly computed using the Frobenius map. For even q a slight variant of this test is used. Computing modulo $\pi(x)$ keeps the degrees of the coefficients of the polynomials in a manageable (of degree at most $N-1$ in x and 1 in y if $\pi(x)$ has degree N). The Euclidean algorithm was then applied to the polynomials $P(a)$ and $Q(a)$ in $(k[x, y]/(\pi(x)))[a]$, keeping the remainder monic at each step by multiplying by a suitable element of $\mathbf{A}$. (This avoids the need for working with rational functions in the succeeding divisions). The Chinese Remainder Theorem was then used to reconstruct $\Upsilon(a)$ from the computed polynomials $\Upsilon(a) \bmod \pi(x)$. For the most part, the computations were performed using the Mathematica software system. For the cases $q = 4$, 8, and 9, Mathematica was also used as a front-end to handle the symbolic computations (computing the relations $P(a)$ and $Q(a)$ modulo $\pi(x)$, for example), passing many of the operations on polynomials with coefficients in finite fields to the PARI GP calculator. (This produced a performance factor increase of nearly 1000 on some computations.) As checks on the computations, the degree of $\Upsilon(a)$ was computed independently (being the class number of k, it is just the number of $\mathbb{F}_q$-rational points on the given elliptic curve), and the constant term was checked against the prime-ideal factorization given by Dorman's Theorem [1].

4. Degrees of the trace and norm terms

Throughout this section we assume that $n = 3$, so that k is the function field of an elliptic curve, and therefore has genus $g = 1$. It follows that the set $\mathscr{P}$ of prime ideals of degree one in $\mathbf{A}$ is a set of representatives for the $h_k - 1$ nontrivial ideal classes in the class group $\mathrm{Pic}(\mathbf{A})$ of $\mathbf{A}$. Let $\mathfrak{e} = \mathbf{A}$ denote the unit ideal.

Assuming the notation of §2, we fix an embedding $\mathbf{e}: K_x^+ \to k_\infty$. Let $\mathbf{C}$ be the completion of the algebraic closure of k_∞. The embedding $\mathbf{e}$ extends (noncanonically) to an embedding, also called $\mathbf{e}$, of K_x into $\mathbf{C}$. The image $\mathbf{e}(x\mathbf{A})$ of the principal ideal $x\mathbf{A}$ in this embedding is a lattice in $\mathbf{C}$. Therefore, there is an invariant $\xi(x\mathbf{A}) \in \mathbf{C}$ such that the rank-one Drinfeld module $\phi = \phi^\Gamma$ determined by the homothetic lattice $\Gamma = \xi(x\mathbf{A}) \cdot xA$ is sgn-normalized (see [7]). A generator λ of Λ_x for this ϕ may be constructed analytically in $\mathbf{C}$ as follows:

$$\lambda = \xi(x\mathbf{A}) \prod_{\gamma \in x\mathbf{A} - \{0\}} \left(1 - \frac{1}{\gamma}\right). \tag{4.1}$$

One knows (see Theorems 4.12 and 5.1 of [8]) that if the fractional ideal $\mathfrak{a}$ of $\mathbf{A}$ is prime to x, then

$$\lambda^{\sigma_\mathfrak{a}} = \xi(x\mathfrak{a}^{-1}) \prod_{\gamma \in x\mathfrak{a}^{-1} - \{0\}} \left(1 - \frac{1}{\gamma}\right), \tag{4.2}$$

where $\sigma_\mathfrak{a}$ is the Artin isomorphism of K_x/k associated with $\mathfrak{a}$. If $\mathbf{v}_\infty$ is

the normalized valuation on K_x^+ induced by the embedding $\mathbf{e}$, then we write $\deg z = -\mathrm{v}_\infty(z)$ for every $z \in K_x^+$.

Theorem 3. *Let*

$$T(a) = \mathrm{Trace}_{H\to k}(a) \quad \textit{and} \quad N(a) = \mathrm{Norm}_{H\to k}(a)$$

be the trace and norm terms of the polynomial $\Upsilon(a)$. *Then* $\deg T(a) = q^2$ *and* $\deg N(a) = q(h_k - 1 + q)$.

Proof. For $\mathfrak{p} \in \mathscr{P}$ and $0 \neq \gamma \in x\mathfrak{p}^{-1}$, we have $\deg\gamma \geq \deg x\mathfrak{p}^{-1} = 1$, as $\deg x = 2$ and $\deg\mathfrak{p} = 1$. It follows then from (4.1) and (4.2) with $\mathfrak{a} = \mathfrak{p}$ that

$$\deg\lambda = \deg\xi(x\mathbf{A}) \quad \text{and} \quad \deg\lambda^{\sigma_\mathfrak{p}} = \deg\xi(x\mathfrak{p}^{-1})$$

for all $\mathfrak{p} \in \mathscr{P}$ which are prime to x. Now by equation (4.2) of [7], with $g = 1$, for any fractional ideal $\mathfrak{a}$ of $\mathbf{A}$, we have

$$\deg\xi(\mathfrak{a}) + \deg\mathfrak{a} = \#F_1(\mathfrak{a}) - q\left(\frac{q-2}{q-1}\right),$$

where

$$F_1(\mathfrak{a}) = \{\gamma \in \mathfrak{a} : \deg\gamma = 1 + \deg\mathfrak{a}\}.$$

It is easy to check that $F_1(\mathfrak{a})$ is invariant on the ideal classes in $\mathrm{Pic}(\mathbf{A})$. Therefore, when $\mathfrak{p} \in \mathscr{P}$ is prime to x,

$$\deg\lambda^{\sigma_\mathfrak{p}} + 1 = \#F_1(\mathfrak{p}^{-1}) - q\left(\frac{q-2}{q-1}\right),$$

which implies that

$$\deg Y^{\sigma_\mathfrak{p}} = (q-1)\cdot\#F_1(\mathfrak{p}^{-1}) + 1 + q - q^2, \tag{4.3}$$

where $Y = -\lambda^{q-1}$. A similar computation yields

$$\deg Y = (q-1)\cdot\#F_1(\mathfrak{e}) + 2 - q^2. \tag{4.4}$$

In order to compute $\#F_1(\mathfrak{e})$ and $\#F_1(\mathfrak{p}^{-1})$, for any fractional ideal $\mathfrak{a}$, we define

$$T_1(\mathfrak{a}) = L(\mathfrak{a}^{-1}\infty^{\deg\mathfrak{a}+1}) = \{\gamma \in \mathfrak{a} : \deg\gamma \leq \deg\mathfrak{a} + 1\}.$$

Since $\deg(\mathfrak{a}^{-1}\infty^{\deg\mathfrak{a}+1}) = 1 > 2g - 2$,

$$\#T_1(\mathfrak{a}) = q$$

by the Riemann-Roch Theorem. For $\mathfrak{p} \in \mathscr{P}$, we have $T_1(\mathfrak{p}^{-1}) = F_1(\mathfrak{p}^{-1}) \cup \{0\}$, since otherwise $\mathfrak{p}$ would be a principal ideal. It follows that $\#F_1(\mathfrak{p}^{-1}) = q - 1$. Further, $\mathfrak{e}$ contains $\mathbb{F}_q$, and so $T_1(\mathfrak{e}) = \mathbb{F}_q$, which implies that $\#F_1(\mathfrak{e}) = 0$. We conclude from (4.3) and (4.4) that

$$\deg Y = 2 - q^2 \tag{4.5}$$

and that

$$\deg Y^{\sigma_\mathfrak{p}} = 2 - q$$

for every $\mathfrak{p} \in \mathscr{P}$ which is prime to x.

Assume first that x is inert in $k/\mathbb{F}_q(x)$, so that every $\mathfrak{p} \in \mathscr{P}$ is prime to x. Since $\deg Y \leq 0$ by (4.5), it follows from (2.2) that

$$\deg(a) = \deg(xY^{-1}) = 2 - (2 - q^2) = q^2. \tag{4.6}$$

Similarly, for every $\mathfrak{p} \in \mathscr{P}$,

$$\deg(a^{\sigma_{\mathfrak{p}}}) = \deg(xY^{-\sigma_{\mathfrak{p}}}) = 2 - (2 - q) = q. \tag{4.7}$$

The theorem follows easily from the evaluations (4.6) and (4.7).

Assume next that x splits or ramifies in $k/\mathbb{F}_q(x)$, and let $\mathfrak{p} \in \mathscr{P}$ divide x. By the weak approximation theorem, we may find an element $z \in k$ such that $\deg z = 0$ and $z\mathfrak{p}$ is prime to x. The calculations leading to (4.7) are valid with $\mathfrak{p}$ replaced by $z\mathfrak{p}$, and so the theorem follows in this case also. □

5. The trace term

The trace of a, $T(a) = \mathrm{Trace}_{H\to k}(a)$, exhibits some interesting behavior in all the computed examples, particularly in the case of even characteristic. When q is even, the elliptic curve in (1.2) can be taken to be in one of the following two forms [11, Appendix A]:

$$\begin{aligned} y^2 + xy &= x^3 + a_4x^2 + a_6, \\ y^2 + a_3y &= x^3 + a_4x + a_6, \qquad a_3 \neq 0. \end{aligned} \tag{5.1}$$

The hyperelliptic involution $y \mapsto y + x$ (respectively, $y \mapsto y + a_3$) has precisely two (respectively, one) fixed point, so the class number h_k for the first form above is always even, for the second form always odd. For all elliptic curves for $q = 2, 4, 8$, and for some additional examples with $q = 16$, the trace term of $\Upsilon(a)$ is

$$x + x^2 + x^4 + x^8 + \cdots + x^{q^2/2}, \quad \text{for } h_k \text{ even},$$

and

$$x^{q/2} + x^{q^2/2} = (x + x^q)^{q/2}, \quad \text{for } h_k \text{ odd}.$$

Remark. When q is odd, the situation is more complicated, but in all computed examples the trace term is a product of y with a polynomial in x (by Theorem 3 of degree $(q^2-3)/2$ as a polynomial in x) all of whose factors in $\mathbb{F}_q[x]$ have degree at most q. Note that by Dorman's formula, the norm term has factors of degree at most $n = 3$.

Bibliography

1. D. Dorman, *On singular moduli for rank 2 Drinfeld modules*, Compositio Math. **80** (1991), 235–256.
2. D. Dummit, *Genus two hyperelliptic Drinfeld modules over* $\mathbb{F}_2$, The Arithmetic of Function Fields, Proc. Workshop at Ohio State University, June 17–26, 1991, de Gruyter, Berlin and New York, 1992, pp. 117–129.
3. E.-U. Gekeler, *Drinfeld modular curves*, Lecture Notes in Math., vol. 1231, Springer-Verlag, Berlin, 1986.
4. ———, *Zur Arithmetik von Drinfeld-Moduln*, Math. Ann. **262** (1983), 167–182.
5. B. Gross and D. Zagier, *On singular moduli*, J. Reine Angew. Math. **355** (1985), 191–220.
6. D. Hayes, *Explicit class field theory in global function fields*, Studies in Algebra and Number Theory, Adv. Math. Suppl. Stud., vol. 6, Academic Press, New York, 1979, pp. 173–217.
7. ———, *Analytic class number formulas in global function fields*, Invent. Math. **65** (1981), 49–69.
8. ———, *Stickelberger elements in function fields*, Compositio Math. **55** (1985), 209–239.

9. ———, *On the reduction of rank-one Drinfeld modules*, Math. Comp. **57** (1991), 339–349.
10. ———, *A brief introduction to Drinfeld modules*, The Arithmetic of Function Fields, Proc. Workshop at Ohio State University, June 17–26, 1991, de Gruyter, Berlin and New York, 1992, pp. 1–32.
11. J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., No. 106, Springer-Verlag, Berlin, 1986.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF VERMONT, BURLINGTON, VERMONT 05401-1455
E-mail address: dummit@griffin.emba.uvm.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MASSACHUSETTS 01003
E-mail address: dhayes@math.umass.edu