MATHEMATICS OF COMPUTATION
VOLUME 57, NUMBER 195
JULY 1991, PAGES 339–349

ON THE REDUCTION OF RANK-ONE DRINFELD MODULES

DAVID R. HAYES

ABSTRACT. The Drinfeld modules of rank one associated to all elliptic curves over the finite fields $\mathbb{F}_2$ and $\mathbb{F}_3$ are computed in explicit form. These examples illustrate the theory of the j-invariant of such modules as developed by Gekeler and Dorman.

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

$$y^2 = f(x) \tag{1}$$

if q is odd, or

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

if q is even, to the field of rational functions $\mathbb{F}_q(x)$. If q is odd, we require that $f(x)$ be square-free, which means that the affine plane curve defined by (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 (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 ∞. Fix $\sqrt{x} \in k_\infty$, and let sgn: $k_\infty \to \mathbb{F}_q$ be the unique sign-function for which $\operatorname{sgn}(1/\sqrt{x}) = 1$. We choose y so that $\operatorname{sgn}(y) = 1$.

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

$$\rho_x = x + a\varphi + \varphi^2,$$
$$\rho_y = y + c_1\varphi + c_2\varphi^2 + \cdots + c_{n-1}\varphi^{n-1} + c_n\varphi^n,$$

where $c_n = \operatorname{sgn}(y) = 1$ and the coefficients $a, c_1, c_2, \ldots, c_{n-1}$ are elements of the Hilbert Class Field H of $\mathbf{A}$. The degree $h_k = [H : k]$ is the class number of k. Let $\mathbf{B}$ be the integral closure of $\mathbf{A}$ in H. One knows that the coefficients

Received July 25, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11G15, 11G20, 11R58.
Partially supported by NSF grant DMS-8702716.

0025-5718/91 $1.00 + $.25 per page

of ρ_x and ρ_y actually belong to $\mathbf{B}$. In fact, because $\deg(\infty) = 1$, we have

Theorem 1. *The* $\mathbf{A}$*-module* ρ *is a universal* sgn*-normalized Drinfeld* $\mathbf{A}$*-module of rank one. This means that if* γ: $\mathbf{A} \to K$ *is any* $\mathbb{F}_q$*-algebra morphism from* $\mathbf{A}$ *into a field* K *and if* τ *is a* sgn*-normalized rank-one Drinfeld* $\mathbf{A}$*-module over* K, $\mathbf{A}$ *acting through* γ, *then* γ *extends to* $\mathbf{B}$ *in such a way that* $\tau = \gamma \circ \rho$. *Further, the coefficients* $a, c_1, \ldots, c_{n-1}$ *generate* $\mathbf{B}$ *as an* $\mathbf{A}$*-algebra.*

For the theory of rank-one Drinfeld modules, the reader may consult [6] or Chapter IV of [4].

Let $\mathfrak{P}_0$ be a prime ideal of $\mathbf{B}$, and let $\mathfrak{p}_0 = \mathfrak{P}_0 \cap \mathbf{A}$. Let P_0 be the monic irreducible polynomial which generates the ideal $\mathfrak{p}_0 \cap \mathbb{F}_q[x]$, and put $d = \deg(P_0)$. The results in §1 below impose conditions on the ideals $\mathfrak{P}_0$ which divide the coefficient a of φ in ρ_x. At such a $\mathfrak{P}_0$, the reduction $\overline{\rho}$ of ρ over $\mathbf{B}/\mathfrak{P}_0$ has the form

$$\overline{\rho}_x = \overline{x} + \varphi^2,$$

$$\overline{\rho}_y = \overline{y} + \overline{c}_1\varphi + \overline{c}_2\varphi^2 + \cdots + \overline{c}_{n-1}\varphi^{n-1} + \varphi^n,$$

where for any $t \in \mathbf{B}$, $\overline{t}$ denotes the reduction of t modulo $\mathfrak{P}_0$. For odd q, Dorman [2] has found the full prime ideal decomposition in $\mathbf{A}$ of the norm of $j(a) = a^{q+1}$ from H down to k. His work is based upon the theory of j-invariants introduced by Gekeler in [5]. The results in §1 overlap those of Dorman to some extent; however, our point of view is computational, and the methods of proof are therefore more elementary.

In §2 below, we compute the Drinfeld $\mathbf{A}$-modules of rank 1 associated with elliptic curves ($n = 3$) over $\mathbb{F}_2$ and $\mathbb{F}_3$. These examples serve to illustrate and illuminate the theory. It is a pleasure to thank D. Dummit for checking the most complicated of these examples via *Mathematica.*

1. Some restrictions on the divisors of a

Let v_0 be the normalized valuation at $\mathfrak{p}_0$. Since ρ is a rank-one $\mathbf{A}$-module, its reduction modulo $\mathfrak{P}_0$ will have height one. This means that if $\mathrm{ht}_{\overline{\rho}}(z)$ is the smallest exponent s such that φ^s appears in $\overline{\rho}_z$ with nonzero coefficient, then

$$\mathrm{ht}_{\overline{\rho}}(z) = v_0(z) \cdot \deg(\mathfrak{p}_0) \tag{3}$$

for all $z \neq 0$ in $\mathbf{A}$.

Proposition 1. *Suppose* $P_0 = x + \alpha$ *has degree* $d = 1$. *Then* $\mathfrak{P}_0$ *divides* a *if and only if* P_0 *is inert or ramified in* $k/\mathbb{F}_q(x)$.

Proof. Since $\rho_{x+\alpha} = (x+\alpha)+a\varphi+\varphi^2$, $\mathfrak{P}_0$ divides a precisely if $\mathrm{ht}_{\overline{\rho}}(x+\alpha) = 2$, which in turn is equivalent to $v_0(x+\alpha) \cdot \deg(\mathfrak{p}_0) = 2$. Thus, $\mathfrak{P}_0$ divides a exactly when one of $\deg(\mathfrak{p}_0)$ and $v_0(x+\alpha)$ equals two and the other equals one. □

Proposition 2. *If* $\mathfrak{P}_0$ *divides a, then* $\deg(P_0) = d$ *is odd and* $d \leq n$. *Further,* $\bar{c}_r = 0$ *for all odd* r *such that* $1 \leq r < d$,

$$(\bar{x}^{q^2} - \bar{x})\bar{c}_2 = (\bar{y}^{q^2} - \bar{y}), \tag{4}$$

and

$$(\bar{x}^{q^r} - \bar{x})\bar{c}_r = (\bar{c}_{r-2}^{q^2} - \bar{c}_{r-2}) \tag{5}$$

for all even r *with* $2 < r < n$.

Proof. Let l be the unique odd integer such that $\bar{c}_l \neq 0$ but $\bar{c}_r = 0$ for all odd r, $1 \leq r < l$. Since $\bar{c}_n = 1$, l exists and $l \leq n$. By comparing coefficients of φ^l in the identity

$$(\bar{x} + \varphi^2) \cdot \bar{\rho}_y = \bar{\rho}_y \cdot (\bar{x} + \varphi^2), \tag{6}$$

we see that $(\bar{x}^{q^l} - \bar{x})\bar{c}_l = 0$. As $\bar{c}_l \neq 0$, $\mathbb{F}_q[x]/(P_0 \cdot \mathbb{F}_q[x])$ is isomorphic to a subfield of the field of q^l elements. Therefore, d divides l. The stated relations on the $\bar{c}_r$ for even r follow readily from (6). □

Lemma 1. *Let* τ *be the rank-two* $\mathbb{F}_q[x]$*-module determined by* $x \mapsto x + \varphi^2$, *and let* $\bar{\tau}$ *denote its reduction modulo* P_0. *Then the height of* $\bar{\tau}$ *equals one when* $\deg(P_0)$ *is even, and equals two when* $\deg(P_0)$ *is odd.*

Proof. Put $\psi = \varphi^2$, and let τ also denote the rank-one $\mathbb{F}_{q^2}[x]$-module determined by $x \mapsto x + \psi$. This abuse of language is justified by the fact that this new module restricts to the given one on $\mathbb{F}_q[x]$. Let Q_0 be a monic irreducible in $\mathbb{F}_{q^2}[x]$ which divides P_0, and let $\bar{\tau}$ also denote the reduction of τ modulo Q_0. Since $\bar{\tau}$ has height one as an $\mathbb{F}_{q^2}[x]$-module, (3) implies that

$$\mathrm{ht}_{\bar{\tau}}(Q_0) = \deg(Q_0). \tag{7}$$

If d is odd, then $Q_0 = P_0$. In this case, $\bar{\tau}_{P_0} = \psi^d = \varphi^{2d}$, so that $\bar{\tau}$ has height two as an $\mathbb{F}_q[x]$-module. If d is even, then $P_0 = Q_0 \cdot Q_0^{\mathrm{Frob}}$ in $\mathbb{F}_{q^2}[x]$. From (7), we see that $\bar{\tau}_{Q_0} = \psi^r = \varphi^d$, where $r = \deg(Q_0) = d/2$. Therefore,

$$\bar{\tau}_{P_0} = \varphi^d \cdot (\overline{Q_0^{\mathrm{Frob}}} + \text{higher-order terms in } \psi),$$

which proves that $\bar{\tau}$ has height one as an $\mathbb{F}_q[x]$-module. □

Proposition 3. *Suppose* $\mathfrak{P}_0$ *divides a. Then* P_0 *is inert or ramified in* $k/\mathbb{F}_q(x)$.

Proof. Let τ be the restriction of ρ to $\mathbb{F}_q[x]$. Then $\bar{\tau}$ is the rank-two $\mathbb{F}_q[x]$-module determined by $x \mapsto x + \varphi^2$. Since $\deg(P_0)$ is odd by Proposition 2, $\bar{\tau}$ has height two by Lemma 1. Therefore, $\mathrm{ht}_{\bar{\rho}}(P_0) = 2\deg(P_0)$, which together with (3) shows that $v_0(P_0) \cdot \deg(\mathfrak{p}_0) = 2\deg(P_0)$. □

Proposition 4. *Assume that q is odd and that $P_0 = f(x) - \alpha$, where $\alpha \in \mathbb{F}_q$ is either zero or a nonsquare. Then a is divisible by at least one prime ideal of* **B** *lying over P_0.*

Proof. Note first that $y^2 \equiv f(x) \equiv \alpha \pmod{\mathfrak{p}_0}$. By our hypothesis on α, either $\overline{y} = 0$ or else $y^2 - \alpha$ is irreducible modulo P_0. In any case, $\overline{y}^q + \overline{y} = 0$ because $z \mapsto z + z^q$ is the trace map from $\mathbb{F}_{q^2}$ down to $\mathbb{F}_q$. Therefore,

$$\overline{y}^{q^n} = (-1)^n \overline{y} = -\overline{y}$$

as n is odd. Let τ be the rank-two $\mathbb{F}_q[x]$-module determined by $x \mapsto x + \varphi^2$. Then $\overline{\tau}_{f(x)} = \overline{\tau}_{P_0+\alpha} = \alpha + \varphi^{2n}$ by Lemma 1. If we put $\overline{\tau}_y = \overline{y} + \varphi^n$, then

$$(\overline{\tau}_y)^2 = \overline{y}^2 + (\overline{y}^{q^n} + \overline{y})\varphi^n + \varphi^{2n} = \overline{y}^2 + \varphi^{2n} = \alpha + \varphi^{2n}.$$

Thus, $\overline{\tau}$ extends to a rank-one **A**-module defined over $\mathbf{A}/\mathfrak{p}_0$. By Theorem 1, $\overline{\tau}$ is a reduction of ρ. Since the kernel of this reduction sits over $\mathfrak{p}_0$, it must be a conjugate of $\mathfrak{P}_0$. □

2. Examples

The identity $\rho_x \cdot \rho_y = \rho_y \cdot \rho_x$ provides an algorithm for computing the coefficients $a, c_1, c_2, \ldots, c_{n-1}$ when q and $f(x)$ are assigned specific values. By comparing the coefficients of like powers of φ on both sides of this identity, one can solve recursively for the coefficients $c_1, c_2, \ldots, c_{n-1}$ in terms of a. The equality of the coefficients of φ^n and φ^{n+1} then yields two polynomial identities for a with coefficients in **A**. Let $\Upsilon(a) \in k[a]$ be the monic greatest common divisor of these two polynomials. Any root of $\Upsilon(a)$ determines a sgn-normalized rank-one **A**-module in the algebraic closure of k. By Theorem 1, this root lies in **B** and generates H. Therefore, $\Upsilon(a)$ is a power of the minimal polynomial over k of any one of its roots. Since these roots all lie in the integral closure **B** of **A**, $\Upsilon(a) \in \mathbf{A}[a]$. One can find the minimal polynomial itself by computing greatest common divisors with derivatives in the standard way. Since the minimal polynomial has degree h_k in a, this procedure provides an algorithm for computing the class number of k.

For the case of elliptic curves $(n = 3)$, we find

$$c_1 = a \cdot \frac{y^q - y}{x^q - x}, \tag{8}$$

$$c_2 = \frac{y^{q^2} - y + ac_1^q - c_1 a^q}{x^{q^2} - x}, \tag{9}$$

$$c_1^{q^2} - c_1 = c_2 a^{q^2} - ac_2^q + x^{q^3} - x, \tag{10}$$

$$c_2^{q^2} - c_2 = a^{q^3} - a. \tag{11}$$

Suppose that $n = 3$ and $\mathfrak{P}_0$ divides a. By the results in §1, $\mathfrak{P}_0$ lies over an irreducible P_0 of degree one or three, which is ramified or inert in $k/\mathbb{F}_q(x)$.

Proposition 1 completely characterizes the divisors of a which lie over a linear P_0. The following proposition provides a useful characterization of the cubic irreducibles P_0 which lie under a divisor of a when q is odd.

Proposition 5. *For q odd, assume $n = d = 3$, and let $f(x) = x^3 + \alpha x^2 + \beta x + \gamma$. Let δ be the coefficient of x^2 in P_0. Put*

$$t = \frac{y^{q^2} - y}{x^{q^2} - x} \in k.$$

Then a is divisible by at least one prime ideal of **B** *lying over P_0 if and only if P_0 is inert or ramified in $k/\mathbb{F}_q(x)$ and either $\alpha = \delta$ and $\bar{t} = 0$, or else $\alpha - \delta$ is a nonsquare in $\mathbb{F}_q^\times$ and $\bar{t}^2 = \alpha - \delta$.*

Proof. Assume that a is divisible by $\mathfrak{P}_0$. Then P_0 is inert or ramified in $k/\mathbb{F}_q(x)$ by Proposition 3. By (8) and (9), we have

$$\bar{\rho}_x = \bar{x} + \varphi^2, \qquad \bar{\rho}_y = \bar{y} + \bar{t}\varphi^2 + \varphi^3.$$

Since $\bar{x}^{q^3} = \bar{x}$ and $\bar{x} + \bar{x}^q + \bar{x}^{q^2} = -\delta$, we find after some computation that

$$\bar{\rho}_{f(x)} = f(\bar{x}) + (\beta + \alpha(\bar{x} + \bar{x}^{q^2}) + \bar{x}^2 + \bar{x}^{1+q^2} + \bar{x}^{2q^2})\varphi^2 + (\alpha - \delta)\varphi^4 + \varphi^6,$$
$$(\bar{\rho}_y)^2 = \bar{y}^2 + \bar{t}(\bar{y} + \bar{y}^{q^2})\varphi^2 + (\bar{y} + \bar{y}^{q^3})\varphi^3 + \bar{t}^{1+q^2}\varphi^4 + (\bar{t} + \bar{t}^{q^3})\varphi^5 + \varphi^6.$$

Since the coefficients of φ^4 must be equal, we see that $\bar{t}^{1+q^2} = \alpha - \delta$. Therefore, either $\bar{t} = \alpha - \delta = 0$ or else $\bar{t}^{q^2} = (\alpha - \delta)\bar{t}^{-1}$, which implies $\bar{t}^{q^4} = \bar{t}$. Since $\deg(P_0) = 3$, $\mathbf{A}/\mathfrak{p}_0$ does not contain a field of degree four over $\mathbb{F}_q$. Therefore, we infer that $\bar{t}^{q^2} = \bar{t}$, which shows that $\bar{t}^2 = \alpha - \delta$. Since the coefficients of φ^5 in the above pair of equations must be equal, $\bar{t}^{q^3} = -\bar{t}$, which implies that $\bar{t} \notin \mathbb{F}_q$. Therefore, $\alpha - \delta$ is a nonsquare.

For the converse, let P_0 be inert or ramified in $k/\mathbb{F}_q(x)$. Assume first that $\bar{t} = \alpha - \delta = 0$. Then $\bar{y}^{q^2} = \bar{y}$, which shows that $f(\bar{x}) \in \mathbb{F}_q$. Appealing to Proposition 4, we see that a must be divisible by a prime ideal of **B** lying over P_0. Assume next that $\alpha - \delta$ is a nonsquare in $\mathbb{F}_q^\times$ and that $\bar{t}^2 = \alpha - \delta$. Let τ be the rank-two $\mathbb{F}_q[x]$-module determined by $x \mapsto x + \varphi^2$, and define $\bar{\tau}_y = \bar{y} + \bar{t}\varphi^2 + \varphi^3$. Computing as above, we find that

$$\bar{\tau}_{f(x)} = f(\bar{x}) + (\beta + \alpha(\bar{x} + \bar{x}^{q^2}) + \bar{x}^2 + \bar{x}^{1+q^2} + \bar{x}^{2q^2})\varphi^2 + (\alpha - \delta)\varphi^4 + \varphi^6,$$
$$(\bar{\tau}_y)^2 = \bar{y}^2 + \bar{t}(\bar{y} + \bar{y}^{q^2})\varphi^2 + (\bar{y} + \bar{y}^{q^3})\varphi^3 + \bar{t}^{1+q^2}\varphi^4 + (\bar{t} + \bar{t}^{q^3})\varphi^5 + \varphi^6.$$

Now $\bar{y}^{q^3} = -\bar{y}$ because either $\bar{y} = 0$ or else $\bar{y}^2$ is a nonsquare in $\mathbf{A}/\mathfrak{p}_0$, and

this implies that

$$\bar{t}^{q^3} = \left(\frac{\bar{y}^{q^2} - \bar{y}}{\bar{x}^{q^2} - \bar{x}}\right)^{q^3} = \frac{\bar{y} - \bar{y}^{q^2}}{\bar{x}^{q^2} - \bar{x}} = -\bar{t}.$$

Therefore, $(\bar{\tau}_y)^2 = \bar{\tau}_{f(x)}$ except possibly for the coefficients of φ^2. We find, however, that

$$\begin{aligned}\bar{t}(\bar{y} + \bar{y}^{q^2}) &= \frac{\bar{y}^{2q^2} - \bar{y}^2}{\bar{x}^{q^2} - \bar{x}} = \frac{f(\bar{x})^{q^2} - f(\bar{x})}{\bar{x}^{q^2} - \bar{x}} \\ &= \frac{u^3 - \bar{x}^3 + \alpha(u^2 - \bar{x}^2) + \beta(u - \bar{x})}{u - \bar{x}},\end{aligned}$$

where $u = \bar{x}^{q^2}$. Thus,

$$\bar{t}(\bar{y} + \bar{y}^{q^2}) = \beta + \alpha(u + \bar{x}) + u^2 + u\bar{x} + \bar{x}^2,$$

which shows that the coefficients of φ^2 are also equal. Thus, $\bar{\tau}$ extends to a rank-one $\mathbf{A}$-module defined over $\mathbf{A}/\mathfrak{p}_0$. By Theorem 1, $\bar{\tau}$ is a reduction of ρ; and the kernel of this reduction must be one of the conjugates of $\mathfrak{P}_0$. □

The examples presented in the remainder of the paper provide a complete list (up to isomorphism) of universal sgn-normalized rank-one Drinfeld modules for the case $n = 3$ over $\mathbb{F}_2$ and $\mathbb{F}_3$. This list includes some of the examples given in §11 of [6]. They were computed by the method described above with the help of computer programs written in APL. In practice, one solves (8) and (9) above for c_1 and c_2 modulo a prime $P \in \mathbb{F}_q[x]$ which is inert in $k/\mathbb{F}_q(x)$, and then finds the greatest common divisor $\Upsilon_P(a)$ of (10) and (11) modulo P. If $\deg P$ is large enough, $\Upsilon_P(a) = \Upsilon(a)$; and one can verify this equality by checking (8)–(11) without reducing modulo P. If this check fails, one chooses another inert P and repeats the calculation. A candidate for $\Upsilon(a)$ which reduces to $\Upsilon_P(a)$ modulo all the primes of reduction can be found via the Chinese Remainder Theorem.

Of course, the monic irreducibles dividing the constant term of $\Upsilon(a)$ are the polynomials P_0 lying under divisors $\mathfrak{P}_0$ of a.

2.1. Elliptic curves over $\mathbb{F}_2$. In the set of eight cubic polynomials over $\mathbb{F}_2$, $\{x^3 + x + 1, x^3, x^3 + 1, x^3 + x\}$ is a subset of representatives for the orbits under the action of the translations $\{x \mapsto x, x \mapsto x + 1\}$. In Examples 1, 3, 4, and 6 below, we take $f(x)$ from this subset with $a_1 = 0$ and $a_3 = 1$ in (2). In Examples 2 and 5, we take $f(x) = x^3 + x^2 + 1$ and $f(x) = x^3 + 1$ with $a_1 = 1$ and $a_3 = 0$ in (2). These six curves represent all isomorphism classes of elliptic curves over $\mathbb{F}_2$ (see §4 of [3]). Example 1 is the only one of our examples which occurs in the known finite list of curves with class number one. Of course, one can easily compute the class number in any one of the examples presented here or in §2.2 below by counting the number of rational points on the elliptic curve.

Example 1. Consider $y^2 + y = x^3 + x + 1$. For this curve, we compute

$$\Upsilon(a) = a + (x^2 + x).$$

Therefore, $h_k = 1$. We find that

$$\rho_x = x + (x^2 + x)\varphi + \varphi^2,$$
$$\rho_y = y + (y^2 + y)\varphi + x(y^2 + y)\varphi^2 + \varphi^3.$$

In this example, $P_0 = x$ and $x+1$ are inert, and $P_0 = x^3+x+1$ and x^3+x^2+1 both split.

Example 2. Consider $y^2 + xy = x^3 + x^2 + 1$. For this curve, we compute

$$\Upsilon(a) = a^2 + (x^2 + x)a + (x^3 + x).$$

Therefore, $h_k = 2$. We have $\mathbf{B} = \mathbf{A}[z]$ with $z^2 + z = 1 + x$, and we find that

$$\rho_x = x + a\varphi + \varphi^2, \qquad \rho_y = y + c_1\varphi + c_2\varphi^2 + \varphi^3,$$

with

$$a = (x + 1)(xz + y + 1),$$
$$c_1 = (z + 1)(x^3 + x^2 + 1) + y(x^2 + xz + z),$$
$$c_2 = y(x^3 + x + 1) + z(x^4 + x^2 + x + 1).$$

In this example, $P_0 = x$ ramifies and $P_0 = x + 1$ is inert while $P_0 = x^3 + x + 1$ and $P_0 = x^3 + x^2 + 1$ both split.

Example 3. Consider $y^2 + y = x^3$. For this curve, we compute

$$\Upsilon(a) = a^3 + (x^2 + x)a^2 + (x + 1)^2 a + (x + 1)^4.$$

Therefore, $h_k = 3$. We have $a = (x + 1)b$, where

$$b^3 + xb^2 + b + (x + 1) = 0,$$

and we find that

$$\rho_x = x + (x + 1)b\varphi + \varphi^2, \qquad \rho_y = y + c_1\varphi + c_2\varphi^2 + \varphi^3,$$

with $c_1 = x^2 b$ and $c_2 = x^2 b^2 + xb + x$. Therefore, $\mathbf{B} = \mathbf{A}[b]$. By a computation of the norm, we observe that c_2 is divisible by a place over $x^3 + x + 1$. In this example, $P_0 = x$ splits, $P_0 = x + 1$ is inert, $P_0 = x^3 + x^2 + 1$ splits, and $P_0 = x^3 + x + 1$ is inert.

Example 4. Consider $y^2 + y = x^3 + 1$. For this curve, we compute

$$\Upsilon(a) = a^3 + (x^2 + x)a^2 + x^2 a + x^4.$$

Therefore, $h_k = 3$. We have $a = xb$, where

$$b^3 + (x + 1)b^2 + b + x = 0,$$

and we find that

$$\rho_x = x + xb\varphi + \varphi^2, \qquad \rho_y = y + c_1\varphi + c_2\varphi^2 + \varphi^3,$$

with $c_1 = (x^2+x+1)b$ and $c_2 = (x+1)^2b^2+(x+1)b+x$. Therefore, $\mathbf{B} = \mathbf{A}[b]$. By a computation of the norm, we observe that c_2 is divisible by a place over x^6+x^3+1. In this example, $P_0 = x$ is inert, $P_0 = x+1$ splits, $P_0 = x^3+x+1$ splits, and $P_0 = x^3+x^2+1$ is inert.

Example 5. Consider $y^2 + xy = x^3 + 1$. For this curve, we compute

$$\Upsilon(a) = a^4 + (x^2+x)a^3 + (x^3+x)a^2 + (x^4+x^3+x^2)a + x^2(x^3+x^2+1).$$

Therefore, $h_k = 4$. We find that

$$\rho_x = x + a\varphi + \varphi^2, \qquad \rho_y = y + c_1\varphi + c_2\varphi^2 + \varphi^3,$$

with $c_1 = a(x+1+(1+y)/x)$ and $c_2 = x^2+x+(a^3+xy+x)/x^2$. We have found no convenient generators for $\mathbf{B}$ over $\mathbf{A}$ for this example. Here, $P_0 = x$ ramifies and $P_0 = x+1$ splits while both $P_0 = x^3+x+1$ and $P_0 = x^3+x^2+1$ are inert.

Example 6. Consider $y^2 + y = x^3 + x$. For this curve, we compute

$$\Upsilon(a) = a^5 + (x^2+x)a^4 + a^3 + a^2 + (x^4+x+1)a + (x^3+x+1)(x^3+x^2+1).$$

Therefore, $h_k = 5$. We find that

$$\rho_k = x + a\varphi + \varphi^2, \qquad \rho_y = y + a(x+1)\varphi + (x^2+z)\varphi^2 + \varphi^3,$$

where $z = (a^3-1)/(x^2+x+1)$. Therefore, $\mathbf{B} = \mathbf{A}[a, z]$. By computing the norm, we observe that c_2 is divisible by a place over x^3+x+1 and a place over x^9+x^4+1. In this example, $P_0 = x$ and $x+1$ both split whereas $P_0 = x^3+x+1$ and x^3+x^2+1 are inert.

2.2. Elliptic curves over $\mathbb{F}_3$. In the set of eighteen monic, square-free cubic polynomials over $\mathbb{F}_3$,

$$\{x^3-x-1,\ x^3-x^2-x,\ x^3+x^2-1,\ x^3-x,\ x^3+x,\ x^3-x^2+1,\ x^3+x^2-x,\ x^3-x+1\}$$

is a subset of representatives for the orbits under the action of the translations $\{x \mapsto x,\ x \mapsto x+1,\ x \mapsto x-1\}$. The polynomials x^3-x, x^3-x+1, and x^3-x-1 are fixed points for this action. Any cubic in this subset with a nonzero constant term is irreducible. Our examples take $f(x)$ from this subset. Example 7 is the only one of these which occurs in the known finite list of curves with class number one. The tables of class numbers in §23 of [1] provide a convenient check on the computations.

In Examples 7, 8, and 10 below, we solve explicitly for the coefficients c_1 and c_2. In the remaining examples, we give only c_1, since the expression for c_2 is rather complicated.

Example 7. Consider $y^2 = x^3 - x - 1$. For this curve, we compute

$$\Upsilon(a) = a - y(x^3 - x).$$

Therefore, $h_k = 1$. We find that $a = y(x^3 - x)$, $c_1 = y^4 - y^2$, and $c_2 = (y^3 - y)(y^3 - y - 1)(y^3 - y + 1)$.

Example 8. Consider $y^2 = x^3 - x^2 - x$. For this curve, $a = (x^2 - 1)b$, where

$$b^2 - y(x - 1)b + x(x + 1) = 0.$$

Therefore, $h_k = 2$. Solving the quadratic equation for b, we obtain

$$b = z(x^2 + 1) - y(x - 1),$$

where $z^2 = x$. Let $u = y/z$. Then as one checks, $\mathbf{B} = \mathbf{A}[u, z]$. We compute $c_1 = u(y^2 - 1)b/z = u(y^2 - 1)((x^2 + 1) - u(x - 1))$ and $c_2 = z(R - Su)$ with $R = x^{13} - 1$ and

$$S = x^{12} - x^{11} - x^{10} - x^9 + x^8 + x^7 - x^6 + x^5 + x^4 + x^3 - x^2 - x + 1.$$

Example 9. Consider $y^2 = x^3 + x^2 - 1$. For this curve, $a = x(x + 1)b$, where

$$b^3 - xyb^2 - (x + 1)^2 b - y = 0.$$

Therefore, $h_k = 3$. For this example, $c_1 = y(x^2 - x - 1)b$. As observed in [6], $\mathbf{B} = \mathbf{A}[z]$, where $z^3 - z - y = 0$. We have in fact

$$b = -xy(z + 1)^2 - (x^3 + x^2 - x + 1)(z + 1) - y(x^2 + 1).$$

Example 10. Consider $y^2 = x^3 - x$. For this curve, $a = yb$, where

$$b^4 - (x^3 - x + 1)b^3 - b^2 + b + (x^3 - x + 1) = 0.$$

Since the polynomial defining b has only trivial common factors with its derivative, $h_k = 4$. We find $c_1 = b(y^2 - 1)$ and $c_2 = b(y^2 - 1)(z + yb^2)$, where $z = (b^2 + b - 1)/y$ is a unit in $\mathbf{B}$ satisfying $z^4 - y^3 z^3 + 1 = 0$. Since

$$b = (x^3 - x + 1) + (x^3 - x)yz + (x^6 + x^4 + x^2 - 1)z^2 - yz^3,$$

$\mathbf{B} = \mathbf{A}[z]$.

Example 11. Consider $y^2 = x^3 + x$. For this curve, $a = (x - 1)b$, where

$$b^4 - (x^2 + x - 1)yb^3 + x(x - 1)b^2 + xyb + x^2(x^3 + x^2 - x + 1).$$

Since the polynomial defining b has only trivial common factors with its derivative, $h_k = 4$. We compute $c_1 = (x^2 - x - 1)by/x$.

Example 12. Consider $y^2 = x^3 - x^2 + 1$. For this curve, $a = (x+1)b$, where

$$b^5 - (x^2 + x - 1)yb^4 + (x+1)(x^3 + x^2 - 1)b^3 - yb^2 + x(x^4 - x^3 + x^2 + x - 1)b - (x+1)(x^3 - x - 1)y = 0.$$

Therefore, $h_k = 5$. We find $c_1 = xyb$.

Example 13. Consider $y^2 = x^3 + x^2 - x$. For this curve,

$$\Upsilon(a) = a^6 + d_5a^5 + d_4a^4 + d_3a^3 + d_2a^2 + d_1a + d_0,$$

where

$$\begin{aligned}
d_0 &= x^3(x^3 + x^2 - x + 1)(x^3 - x^2 + x + 1)(x^3 - x^2 + 1),\\
d_1 &= x^2(x+1)(x^2 - x - 1)(x^4 - x^3 + x^2 - x + 1)y,\\
d_2 &= x^2(x^2 + 1)(x^5 - x^3 + x^2 + 1),\\
d_3 &= -x^3(x+1)^3y,\\
d_4 &= -x(x^2 + 1)(x^3 + x^2 + x - 1),\\
d_5 &= -(x^3 + x^2 - x + 1)y.
\end{aligned}$$

Therefore, $h_k = 6$. We compute $c_1 = (x+1)ay/x$.

Example 14. Consider $y^2 = x^3 - x + 1$. For this curve,

$$\Upsilon(a) = a^7 + d_6a^6 + d_5a^5 + d_4a^4 + d_3a^3 + d_2a^2 + d_1a + d_0,$$

where

$$\begin{aligned}
d_0 &= -(x^3 - x - 1)(x^3 + x^2 - 1)(x^3 + x^2 + x - 1)(x^3 + x^2 - x + 1)y,\\
d_1 &= x^6 + x^4 + x^3 + x^2 - x - 1,\\
d_2 &= -(x^6 + x^4 + x^3 + x^2 - x - 1)y,\\
d_3 &= -(x^9 + x^6 + x^4 + x^3 + x^2 + x + 1),\\
d_4 &= -(x^3 - x)y,\\
d_5 &= x^3 - x - 1,\\
d_6 &= -(x^3 - x - 1)y.
\end{aligned}$$

Therefore, $h_k = 7$. We compute $c_1 = ya$.

Bibliography

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen.* I, II, Math. Z. **19** (1924), 153–246.
2. D. R. Dorman, *On singular moduli for rank* 2 *Drinfeld modules*, preprint.
3. P. Deligne, *Courbes elliptiques*: *formulaire*, Modular Functions of One Variable, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin, 1975.

4. E.-U. Gekeler, *Drinfeld modular curves*, Lecture Notes in Math., vol. 1231, Springer-Verlag, Berlin, 1986.
5. ——, *Zur Arithmetik von Drinfeld-Moduln*, Math. Ann. **262** (1983), 167–182.
6. D. R. Hayes, *Explicit class field theory in global function fields*, Studies in Algebra and Number Theory, Adv. Math. Suppl. Stud., vol. 6, Academic Press, 1979, pp. 173–217.

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