CORRECTION TO “EXPLICIT POINTS ON THE LEGENDRE CURVE III”

DOUGLAS ULMER

In this note (added after publication) we correct an error in Section 5 of “Explicit points on the Legendre curve III”, and we discuss changes required in the p-adic exercises of Section 7. None of the main results of the paper are affected.

10.1. **Counterexample.** Let k be a finite field of characteristic p, let $W(k)$ be its ring of Witt vectors, and let $\sigma : W(k) \to W(k)$ be its Frobenius automorphism. Let $\mathcal{C}$ and $\mathcal{D}$ be smooth, projective curves over k.

Part (2) of Theorem 5.2 is incorrect as stated. For a counterexample, let $\mathcal{C} = \mathcal{D} = E$ where E is an ordinary elliptic curve over $k = \mathbb{F}_q$, and take $n = 1$. Using well-known properties of elliptic curves, one finds that

$$\left(\left(H^1(\mathcal{C}) \otimes_W H^1(\mathcal{D})\right)^{F=p}\right)/p \cong {\mathbb{F}_p}^2$$

and

$$\left(H^1(\mathcal{C})/p^n \otimes_W H^1(\mathcal{D})/p\right)^{F=V=p} \cong {\mathbb{F}_q}^2.$$

On the other hand, it is known (Milne, Inv. Math. **6**, 1968, p. 102) that the Brauer group of E^2 has order

$$[\mathrm{End}_{\mathbb{F}_q}(E) : \mathbb{Z}[\pi]]^2$$

where π is the Frobenius endomorphism of E. Since the discriminant of $\mathbb{Z}[\pi]$ is prime to p, so is the displayed index, and the p part of the Brauer group is thus trivial. This shows the sequence in Theorem 5.2 part (2) is not exact in general. The problem turns out to be that the middle term is not correct.

10.2. **Corrected Theorem.** We reformulate Theorem 5.2. Although part (1) is correct as stated, we give an equivalent formulation which is more parallel to the correct statement of part (2).

Let $W = W(k)$ and recall that A denotes the Dieudonné ring $W\{F, V\}$ where $FV = VF = p$, $F\alpha = \sigma(\alpha)F$, and $\alpha V = V\sigma(\alpha)$ for $\alpha \in W$. Recall also that $\mathrm{NS}'(\mathcal{C} \times_k \mathcal{D})$ denotes the orthogonal complement in the Néron-Severi group $\mathrm{NS}(\mathcal{C} \times_k \mathcal{D})$ of the classes of $P \times \mathcal{D}$ and $\mathcal{C} \times Q$ where P and Q are k-rational divisors of degree 1 on $\mathcal{C}$ and $\mathcal{D}$ respectively.

10.3. **Theorem** (Corrected Theorem 5.2)**.**

(1) *There is a functorial isomorphism*

$$\mathrm{NS}'(\mathcal{C} \times_k \mathcal{D}) \otimes \mathbb{Z}_p \tilde{\to} \mathrm{Hom}_A\left(H^1(\mathcal{D}), H^1(\mathcal{C})\right).$$

(2) *There is a functorial exact sequence*

$$0 \to \mathrm{Hom}_A\left(H^1(\mathcal{D}), H^1(\mathcal{C})\right)/p^n \to \mathrm{Hom}_A\left(H^1(\mathcal{D})/p^n, H^1(\mathcal{C})/p^n\right) \to \mathrm{Br}(\mathcal{C} \times_k \mathcal{D})_{p^n} \to 0.$$

Date: May 27, 2017.

Here Hom_A *denotes homomorphisms of* A*-modules, and "functorial" means that the displayed maps are equivariant for the action of* $\mathrm{Aut}(\mathcal{C}) \times \mathrm{Aut}(\mathcal{D})$.

The published proof of Theorem 5.2 minus the second half of the last sentence proves the statement above. The second half of the last sentence, written in an overzealous desire for symmetry, purports to go from the "Hom" formulation above to a "$\otimes$" formulation, and this introduces an error. Specifically, the last displayed equation of the proof is not correct. Omitting this last translation yields the correct statement and proof.

10.4. **More on Frobenius.** Before explaining the changes needed to the p-adic exercises of Section 7, we add one detail on the action of Frobenius on the crystalline cohomology group discussed in Section 6.

We use the notations of that section. In particular, $\mathcal{C}$ is the smooth projective model of the affine curve $z^d = x^2 - 1$, $H^1_{crys}(\mathcal{C}/\mathbb{Z}_p)$ is its first crystalline cohomology group, and e_i ($0 < i < d$, $i \neq d/2$) is the basis of $H^1_{crys}(\mathcal{C}/\mathbb{Z}_p)$ appearing in Proposition 6.4. (Here and below, we read the indices modulo d.) We showed that the action of Frobenius on $H^1_{crys}(\mathcal{C}/\mathbb{Z}_p)$ is given by $F(e_i) = c_i e_{pi}$, where $c_i \in \mathbb{Z}_p$ satisfies

$$\mathrm{ord}(c_i) = \begin{cases} 0 & \text{if } i > d/2 \\ 1 & \text{if } i < d/2. \end{cases}$$

10.4.1. **Lemma.**

$$c_i c_{-i} = \begin{cases} p & \textit{if } i < d/2 \textit{ and } pi < d/2 \\ p & \textit{if } i > d/2 \textit{ and } pi > d/2 \\ -p & \textit{if } i < d/2 \textit{ and } pi > d/2 \\ -p & \textit{if } i > d/2 \textit{ and } pi < d/2 \end{cases}$$

Proof. Let $f \in H^2(\mathcal{C}/\mathbb{Z}_p)$ be the cup product $e_1 \cup e_{-1}$. The content of part (1) of Proposition 6.4 is that

$$e_i \cup e_{-i} = \begin{cases} f & \text{if } i < d/2 \\ -f & \text{if } i > d/2. \end{cases}$$

If $i < d/2$, we have

$$pf = F(f) = F(e_i \cup e_{-i}) = c_i c_{-i} e_{pi} \cup e_{-pi},$$

and

$$e_{pi} \cup e_{-pi} = \begin{cases} f & \text{if } pi < d/2 \\ -f & \text{if } pi > d/2. \end{cases}$$

Comparing the last two displays yields the first and third cases of the lemma. For the second and fourth, we have $i > d/2$,

$$-pf = F(-f) = F(e_i \cup e_{-i}) = c_i c_{-i} e_{pi} \cup e_{-pi},$$

and

$$e_{pi} \cup e_{-pi} = \begin{cases} f & \text{if } pi < d/2 \\ -f & \text{if } pi > d/2. \end{cases}$$

Comparing the last two displays yields the remaining two cases of the lemma. □

Define

$$d_i := c_i/p^{\mathrm{ord}_p(c_i)}.$$

We record two useful facts about the d_i: First, the d_i are p-adic units, and by the lemma we have

$$d_i d_{-i} = \pm 1 \tag{10.4.1}$$

where the sign is $+1$ if i and pi lie in the same half of the interval $[0, d]$ and -1 if they lie in opposite halves.

Second, by Proposition 6.4(4-5), if o is an orbit of Frobenius on $\mathbb{Z}/d\mathbb{Z}$ with $\gcd(d, o) < d/2$ and p is balanced modulo $d/\gcd(d, o)$, then

$$\prod_{i \in o} d_i^2 = 1. \tag{10.4.2}$$

10.5. **Modified p-adic exercises.** We now explain the changes needed in Sections 7.1, 7.2, and 7.4 when we replace Theorem 5.2 with Theorem 10.3.

We use the same notations as in Section 7.1: Write W for the Witt vectors $W(\mathbb{F}_q)$, W_n for W/p^n, $H^1(\mathcal{C})$ for $H^1_{crys}(\mathcal{C}/W)$, and $H^1(\mathcal{D})$ for $H^1_{crys}(\mathcal{D}/W)$ where $\mathcal{C} = \mathcal{D}$ is the curve over $\mathbb{F}_q$ studied in Section 6. The product $\mathcal{C} \times_{\mathbb{F}_q} \mathcal{D}$ carries an action of $\Delta = \mu_2 \times \mu_d$ acting “anti-diagonally” as well as an action of $G = \mu_d \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acting on the factor $\mathcal{C}$.

Our goal is to compute

$$H' := \mathrm{Hom}_A \left(H^1(\mathcal{C}), H^1(\mathcal{D})\right)^{\Delta}$$

and

$$H'_n := \mathrm{Hom}_A \left(H^1(\mathcal{C})/p^n, H^1(\mathcal{D})/p^n\right)^{\Delta}.$$

For an orbit $o \in O_{d,p}$, we write H'^o and H'^o_n for the o parts of the corresponding groups, i.e., for the images of the projector π_o of Section 2.8 on H' or H'_n.

Since

$$\mathrm{Hom}_A \left(H^1(\mathcal{C}), H^1(\mathcal{D})\right)^{\Delta} \subset \mathrm{Hom}_W \left(H^1(\mathcal{C}), H^1(\mathcal{D})\right)^{\Delta}$$

and

$$\begin{aligned} \mathrm{Hom}_A \left(H^1(\mathcal{C})/p^n, H^1(\mathcal{D})/p^n\right)^{\Delta} &\subset \mathrm{Hom}_W \left(H^1(\mathcal{C})/p^n, H^1(\mathcal{D})/p^n\right)^{\Delta} \\ &= \left(\mathrm{Hom}_W \left(H^1(\mathcal{C}), H^1(\mathcal{D})\right)^{\Delta}\right)/p^n \end{aligned}$$

we first consider

$$M' := \mathrm{Hom}_W(H^1(\mathcal{C}), H^1(\mathcal{D}))^{\Delta}.$$

Recall the W-basis e_i ($0 < i < d$, $i \neq d/2$) of $H^1(\mathcal{C}) = H^1(\mathcal{D})$ from Proposition 6.4. For $0 < i, j < d$, $i, j \neq d/2$, let $\varphi_{ij} \in \mathrm{Hom}_W(H^1(\mathcal{C}), H^1(\mathcal{D}))$ be the element with

$$\varphi_{ij}(e_\ell) = \begin{cases} e_i & \text{if } \ell = j \\ 0 & \text{if } \ell \neq j. \end{cases}$$

Then the φ_{ij} form a W-basis of $\mathrm{Hom}_W(H^1(\mathcal{C}), H^1(\mathcal{D}))$. The submodule commuting with the anti-diagonal action of Δ, i.e., M', is spanned by the $\varphi_{i,-i}$ with $0 < i < d$, $i \neq d/2$.

Now we fix an orbit $o \in O_{d,p}$ and assume that $\gcd(o,d) < d/2$ and that p is balanced modulo $d/\gcd(o,d)$. Let $i \in o$ be the standard base point, and for $j = 0, \dots, |o| - 1$ define

$$f_{ip^j} = \left(\prod_{\ell=0}^{j-1} d_{ip^\ell}^2\right) \varphi_{ip^j,-ip^j}.$$

The f_{ip^j} form a new basis of M'^o, the part of M' cut out by the projector π_o.

It follows from equation (10.4.2) that f_{ip^j} only depends on the class of ip^j modulo d, i.e., we may read the index j modulo $|o|$ without any ambiguity.

We now turn to computing H'^o and $H_n'^o$. Consider a typical element

$$c = \sum_{j=0}^{|o|-1} \alpha_j f_{ip^j}$$

where $\alpha_j \in W$ or W_n and we read the index j modulo $|o|$.

Applying $F \circ c$ and $c \circ F$ to e_{-ip^j} for $j = 0, \dots, |o| - 1$, we see that $F \circ c = c \circ F$ if and only if

$$\sigma(\alpha_j) c_{ip^j} = \alpha_{j+1} d_{ip^j}^2 c_{-ip^j} \tag{10.5.1}$$

for all j. A similar calculation shows that $V \circ c = c \circ V$ if and only if

$$\sigma(\alpha_j)\left(\frac{p}{c_{-ip^j}}\right) = \alpha_{j+1} d_{ip^j}^2 \left(\frac{p}{c_{ip^j}}\right),$$

and Proposition 6.4(4) and Lemma 10.4.1 show that this equation is equivalent to (10.5.1).

We now simplify equation (10.5.1), separating into four cases depending on the positions of ip^j and ip^{j+1} in $[0,d]$. More precisely, recall the word $w = w_1 \cdots w_{|o|}$ attached to o: the letter w_j is l if the least positive residue of ip^{j-1} modulo d is $> d/2$ and it is u if the residue is $< d/2$. Using Proposition 6.4(4) and equation (10.4.1), we see that equation (10.5.1) is equivalent to the equations

$$\begin{aligned}
+\sigma(\alpha_j) &= p\alpha_{j+1} && \text{if } w_{j+1}w_{j+2} = ll\\
-\sigma(\alpha_j) &= p\alpha_{j+1} && \text{if } w_{j+1}w_{j+2} = lu\\
-p\sigma(\alpha_j) &= \alpha_{j+1} && \text{if } w_{j+1}w_{j+2} = ul\\
+p\sigma(\alpha_j) &= \alpha_{j+1} && \text{if } w_{j+1}w_{j+2} = uu.
\end{aligned}$$

Note that when $w_{j+1} = l$, α_{j+1} determines α_j, and when $w_{j+1} = u$, α_j determines α_{j+1}. Thus we may eliminate many of the variables α_j. More precisely, write the word w in exponential form: $w = u^{e_1} l^{e_2} \cdots l^{e_{2k}}$. Setting $\beta_0 = \alpha_0$ and

$$\beta_j = \alpha_{e_1+e_2+\cdots+e_{2j}}$$

for $1 \le j \le k$ (so that $\beta_k = \beta_0$), the class c is entirely determined by the β's. Indeed, for $\sum_{i=1}^{2j} e_i \le \ell < \sum_{i=1}^{2j+1} e_i$, we have

$$\alpha_\ell = (\sigma p)^{\ell - \sum_{i=1}^{2j} e_i} \beta_j$$

and for $\ell = \sum_{i=1}^{2j+1} e_i$, we have

$$\alpha_\ell = -(\sigma p)^{e_{2j+1}} \beta_j.$$

On the other hand, for $\sum_{i=1}^{2j+1} e_i \le \ell < \sum_{i=1}^{2j+2} e_i$, we have

$$\alpha_\ell = -(\sigma^{-1}p)^{\sum_{i=1}^{2j+2} e_i - \ell}\beta_{j+1}$$

and for $\ell = \sum_{i=1}^{2j+2} e_i$, we have

$$\alpha_\ell = \beta_{j+1}.$$

The conditions on the α's translated to the β's become

$$\begin{aligned}
(\sigma p)^{e_1}\beta_0 &= (\sigma^{-1}p)^{e_2}\beta_1\\
(\sigma p)^{e_3}\beta_1 &= (\sigma^{-1}p)^{e_4}\beta_2\\
&\vdots\\
(\sigma p)^{e_{2k-1}}\beta_{k-1} &= (\sigma^{-1}p)^{e_{2k}}\beta_k
\end{aligned} \tag{10.5.2}$$

These are exactly the “basic equations” (7.4.2) and the rest of the calculation of H'^o and H'^o_n proceeds exactly as in Sections 7.5 and 7.6.

10.6. **A few typos.** We take this opportunity to correct a few other typos.

In Proposition 6.4, part (2), “$\lfloor (d+1)/2 \rfloor$” should be “$\lceil (d+1)/2 \rceil$”.

In the penultimate display of Section 7.2, on the right hand side, “f_{pi}” should be “f_{pj}”.

In Section 7.4, all occurrences of “w_j” should be “w_{j+1}”.

In Proposition 7.5.1, “p is balanced modulo p” should be “p is balanced modulo $d/\gcd(o,d)$”.

The sixth displayed equation in Section 7.6 is missing several powers of σ. It should read

$$\begin{aligned}
0 = p^{ht(o)}\beta_k &= p^{e_{2\ell+2,2k}}\beta_k\\
&= \sigma^{e_{2k-1}+e_{2k}}p^{e_{2\ell+2,2k-2}}\beta_{k-1}\\
&\vdots\\
&= \sigma^{e_{2\ell+3}+\cdots+e_{2k}}p^{e_{2\ell+2}}\beta_{\ell+1}.
\end{aligned}$$

The key point, namely that $p^{e_{2\ell+2}}\beta_{\ell+1} = 0$, is unchanged.

School of Mathematics, Georgia Institute of Technology, Atlanta, GA 30332
E-mail address: ulmer@math.gatech.edu