

Appendix and erratum: ‘Massey products for elliptic curves of rank 1 ’

Jennifer S. Balakrishnan, Kiran S. Kedlaya, and Minhyong Kim

April 16, 2010

Keywords: elliptic curve, Selmer variety, Massey product
MSC: 11G05

The paper [6] contains a few errors in the basic assumptions as well as in the formula of corollary 0.2. First of all, it should have been made clear at the outset that the regular model \mathcal{E} for the elliptic curve E must be the minimal regular model, and \mathcal{X} the complement of the origin in the regular minimal model. Similarly, the tangential base-point b must be integral, in that it is a \mathbb{Z} -basis of the relative tangent space $e^*T_{\mathcal{E}/\mathbb{Z}}$. It could also be an integral two-torsion point for the arguments of the paper to hold verbatim.

The most significant error is in the contribution of the local terms at $l \neq p$, that is, Lemma 1.2. The problem is that a point that is integral on \mathcal{X} may not be integral on a smooth model over a field of good reduction. As it stands, the lemma will only apply to points that are integral in this stronger sense.

However, to get immediate examples, one can replace the lemma by

Lemma 1.2' *Suppose the Neron model of E has only one rational component for each prime. (Equivalently, the Tamagawa number is one at each prime.) Then the map*

$$\mathcal{X}(\mathbb{Z}_l) \rightarrow H^1(G_l, U_2)$$

is trivial for every $l \neq p$.

Therefore, for the function

$$\mathcal{X}(\mathbb{Z}_p) \xrightarrow{j_{2,loc}^{et}} H_f^1(G_p, U_2) \xrightarrow{\psi^p} H^2(G_p, \mathbb{Q}_p(1)) \simeq \mathbb{Q}_p,$$

constructed via the refined Massey product, we get

Theorem 0.1' *Suppose the Neron model of E has only one rational component for each prime. Then the map*

$$\psi^p \circ j_{2,loc}^{et}$$

vanishes on the global points $\mathcal{X}(\mathbb{Z}) \subset \mathcal{X}(\mathbb{Z}_p)$.

The assumption can be easily verified if the elliptic curve has square-free minimal discriminant, since the Neron model will then have only one geometric component in the special fiber. We point out that the integral j -invariant hypothesis is no longer necessary in this version.

Some carelessness with the Hodge theory also requires a modification of the explicit formula in Corollary (0.2). Recall the notation

$$D_2(x) = \int_b^x \alpha\beta$$

and

$$\log_\alpha(x) = \int_b^x \alpha$$

of the paper.

Corollary 0.2' *In addition to the assumptions of the theorem, suppose there is a point y of infinite order in $\mathcal{E}(\mathbb{Z})$. Then*

$$\mathcal{X}(\mathbb{Z}) \subset \mathcal{E}(\mathbb{Z}_p)$$

is in the zero set of

$$(\log_\alpha(y))^2 D_2(z) - (\log_\alpha(z))^2 D_2(y).$$

The proof of Theorem (0.1') is identical to that of Theorem (0.1), once we have replaced Lemma (1.2) by Lemma (1.2').

Proof of Lemma (1.2'). We follow essentially the argument in [6], supplemented in a few places by the methods of [7].

Let $I_l \subset G_l$ be the inertia subgroup. We have the exact sequence

$$0 \rightarrow H^1(G_l/I_l, (U_2)^I) \rightarrow H^1(G_l, U_2) \rightarrow H^1(I_l, U_l).$$

On the other hand, there is also the exact sequence

$$0 \rightarrow (U^3 \setminus U^2)^I \rightarrow (U_2)^I \rightarrow (U_1)^I,$$

and the Frobenius weights on the left and right terms are negative. Therefore,

$$H^1(G_l/I_l, (U_2)^I) = 0,$$

and it suffices to show that the map

$$\mathcal{X}(\mathbb{Z}_l) \rightarrow H^1(I_l, U_2)$$

is trivial.

For this, it suffices to show the triviality of the map

$$\mathcal{X}(\mathbb{Z}_l) \rightarrow H^1(I_l, \pi_2^p)$$

where

$$\pi_2^p := [\pi_1^{et,p}(\bar{X}, b), [\pi_1^{et,p}(\bar{X}, b), \pi_1^{et,p}(\bar{X}, b)]] \setminus \pi_1^{et,p}(\bar{X}, b)$$

is the quotient of the pro- p étale fundamental group of \bar{X} by the second level of its descending central series, that is, the group classifying the abelian-by-central pro- p covers of \bar{X} . Here, the terminology abelian-by-central refers to Galois covers with Galois groups D having the property that $[D, D]$ is central in D .

Denote by \mathcal{E}^0 the scheme whose special fibers are the connected components of the identity in the Néron model of E . Since $\mathcal{X}(\mathbb{Z}_l) = (\mathcal{E}^0 \setminus \{e\})(\mathbb{Z}_l)$, we may replace \mathcal{X} by $\mathcal{E}^0 \setminus \{e\}$ in the following discussion, which then has connected fibers. Also, for ease of notation in this purely local proof, we will now take the base field to be K , the maximal unramified extension of \mathbb{Q}_l in $\bar{\mathbb{Q}}_l$. Any abelian-by-central p -power covering of \bar{X} with a lift of the base-point is dominated by a covering of the form

$$\bar{Z} \longrightarrow \bar{Y} \longrightarrow \bar{X},$$

each map being actually defined over K , where

$$Y = E \setminus E[p^m] \longrightarrow X$$

is the map induced by the p^m map of E and $h : Z \rightarrow Y$ is a cyclic unramified p^n -covering (again, with a lift of the base-point). As in [7], it suffices to show that $Z(K)$ surjects onto $\mathcal{X}(\mathcal{O}_K) \subset X(K)$, for which it suffices to construct an étale model

$$\mathcal{Z} \longrightarrow \mathcal{X}$$

over \mathcal{O}_K that is surjective on the special fibers.

The map $Y \rightarrow X$ extends to an étale map

$$[p^m] : \mathcal{Y} = \mathcal{E}^0 \setminus \mathcal{E}^0[p^m] \longrightarrow \mathcal{E}^0 \setminus \{e\} = \mathcal{X}.$$

The map on special fibers

$$(\mathcal{E}^0 \setminus \mathcal{E}^0[p^m])_s \longrightarrow \mathcal{X}_s$$

is surjective, from which we see that any point in $\mathcal{X}(\mathcal{O}_K) \subset X(K)$ lifts to a point of $\mathcal{Y}(\mathcal{O}_K)$.

We go on to lift to Z . Since K contains all p -power roots of 1, we know that $Z \rightarrow Y$ is a composition of cyclic p -covers. Consider first the case where the base-point b' on Y is an integral point in $\mathcal{Y}(\mathcal{O}_K)$. By induction, it suffices to show the following:

Let \mathcal{Y} be a smooth irreducible curve over \mathcal{O}_K with generic fiber Y , connected special fiber \mathcal{Y}_s , and integral base-point $b' \in \mathcal{Y}(\mathcal{O}_K)$. Let $Z \rightarrow Y$ be a cyclic p -cover with a lift of the base-point b' to $b'' \in Z(K)$. Then there is a smooth \mathcal{O}_K -model \mathcal{Z} of Z with connected special fiber such that \mathcal{Z} is étale over \mathcal{Y} , $b'' \in \mathcal{Z}(\mathcal{O}_K)$, and the map $\mathcal{Z}_s \rightarrow \mathcal{Y}_s$ of special fibers is surjective. In particular, $\mathcal{Z}(\mathcal{O}_K) \rightarrow \mathcal{Y}(\mathcal{O}_K)$ is surjective.

To see this, note that

$$Z = \text{Spec}_Y(\oplus_{i=0}^{p-1} L^{-i})$$

for a line bundle L on Y with a trivialization

$$s : \mathcal{O}_Y \simeq L^p$$

that defines the algebra structure. Extend L to a line bundle \mathcal{L} on \mathcal{Y} . Then s extends to an isomorphism

$$s : \mathcal{O}_{\mathcal{Y}}(k\mathcal{Y}_s) \simeq \mathcal{L}^p$$

for some k , so that we have a trivialization

$$t = l^{-k}s : \mathcal{O}_{\mathcal{Y}} \simeq \mathcal{L}^p.$$

Let v be an \mathcal{O}_K -basis for $\mathcal{L}|_{b'}$. The points of Z above $b' \in Y(K)$ are the inverse image in the fiber $L|_{b'}$ of $s(b') \in (L|_{b'})^p$ under the p -power map

$$L|_{b'} \rightarrow (L|_{b'})^p.$$

Since b' lifts to a rational point of Z , if we write $s = cv^p$, the coefficient $c \in K$ must be a p -th power. On the other hand, since $t(b')$ is an \mathcal{O}_K -basis for $(L|_{b'})^p$, we know that $l^{-k}c$ must be a unit. Hence, we must have $p|k$. Therefore, the finite étale covering

$$\mathcal{Z} := \text{Spec}_{\mathcal{Y}}(\oplus_{i=0}^{p-1} (\mathcal{L})^{-i})$$

of \mathcal{Y} with the algebra structure defined by t is isomorphic to Z over the generic fiber, and $b'' \in \mathcal{Z}(\mathcal{O}_K)$. By removing the components of the special fiber except the one containing the specialization of b'' , we can assume that \mathcal{Z} has connected special fiber. Since the map of special fibers is still surjective, we see that $\mathcal{Z}(\mathcal{O}_K) \rightarrow \mathcal{Y}(\mathcal{O}_K)$ is surjective.

Now consider the situation where the base-point b' is tangential at $e \in E$. We let \mathcal{Y}' be the smooth partial compactification of \mathcal{Y} obtained by adding the point e , and Y' the generic fiber.

Once again, by induction, it suffices to show:

Let \mathcal{Y}' be a smooth irreducible curve over \mathcal{O}_K with connected special fiber. Let $e \in \mathcal{Y}'(\mathcal{O}_K)$ be a point in the smooth locus and $\mathcal{Y} = \mathcal{Y}' \setminus \{e\}$. Let $b' \in e^*(T_{\mathcal{Y}'/\mathcal{O}_K})$ be an \mathcal{O}_K -basis of the tangent space at e . Let $Z' \rightarrow Y'$ be a cyclic p -cover, unramified over the generic fiber Y of \mathcal{Y} , equipped with a lift b'' of the tangent vector b' to a tangent vector at a rational point $e' \in Z(K)$. Then there is a smooth \mathcal{O}_K -model \mathcal{Z}' for Z' with connected special fiber such that $e' \in \mathcal{Z}'(\mathcal{O}_K)$, b'' is a basis for $(e')^*(T_{\mathcal{Z}'/\mathcal{O}_K})$, $\mathcal{Z} := \mathcal{Z}' \setminus \mathcal{Z}'_e$ is finite étale over \mathcal{Y} , and the map $\mathcal{Z}_s \rightarrow \mathcal{Y}_s$ of special fibers is surjective.

This time as well,

$$Z' = \text{Spec}_{\mathcal{Y}'}(\oplus_{i=0}^{p-1} (L')^{-i}),$$

where we have

$$s : (L')^{-p} \simeq \mathcal{O}_{\mathcal{Y}'}(D)$$

with $D = 0$ or $D = -e$. If $D = 0$ then an identical argument to that above will yield a scheme \mathcal{Z}' and \mathcal{Z} with exactly the same properties as in the integral base-point case. Otherwise, $Z' \rightarrow Y'$ is totally ramified over e . Once again, we extend L' to \mathcal{L}' on \mathcal{Y}' and find a k such that $t := l^k s$ gives an isomorphism

$$(\mathcal{L}')^{-p} \simeq \mathcal{O}_{\mathcal{Y}'}(-e).$$

Written in terms of a local basis v for \mathcal{L}' , we have $t = zv^p$ where $(z) = e$, and $s = l^{-k}zv^p$. In terms of the dual $(b')^*$ to the tangential base-point b' , we must have $dz(e') = c(b')^*$ for some unit c . A local basis w for $(L')^{-1}$ can be regarded as a local uniformizer at e' on Z' , so that Z' is locally defined by $w^p = l^{-k}z$. The principal part map takes $w \mapsto l^{-k}w^p$ in the coordinates given by w on $T_{e'}Z'$ and z on T_eY' . We have $b' = c$ in these coordinates. Since b' is liftable to a K -rational b'' , we deduce that $l^k c$ must be a p -th power, so that $p|k$ again. Hence,

$$\mathcal{Z}' = \text{Spec}_{\mathcal{Y}'}(\oplus_{i=0}^{p-1} (\mathcal{L}')^{-i}),$$

with the algebra structure defined by t gives a covering of \mathcal{Y}' smooth over \mathcal{O}_K , whose generic fiber is isomorphic to Z' . If we define $\mathcal{L} = \mathcal{L}'|_{\mathcal{Y}}$, we see that

$$\mathcal{Z} = \text{Spec}_{\mathcal{Y}}(\oplus_{i=0}^{p-1} (\mathcal{L})^{-i})$$

is finite and étale over \mathcal{Y} . A local basis w for $(\mathcal{L}')^{-1}$ can be regarded as a local uniformizer at e' on Z' , so that \mathcal{Z} is locally defined by $w^p = z$. The coordinates on \mathcal{Z}' of the point e' is $w = 0, z = 0$, which is an integral point. The principal part map takes $w \mapsto w^p$ in the coordinates given by w on $T_{e'}Z'$ and z on $T_e\mathcal{Y}'$. We have $b' = c$ in these coordinates, so the base-point lift b'' is an \mathcal{O}_K -integral basis for $T_{e'}Z'$ at the smooth point $e' \in \mathcal{Z}'(\mathcal{O}_K)$. By removing from \mathcal{Z}'_s all components except that containing the specialization of e' , we can assume that \mathcal{Z}' , and hence, $\mathcal{Z} = \mathcal{Z}' \setminus \{e\}$, has connected special fiber. Clearly, $\mathcal{Z}_s \rightarrow \mathcal{Y}_s$ is still surjective. \square

Proof of Corollary (0.2') Two points require modification, the first having to do with the distinction between left and right cosets, and the second a small confusion between the Hodge filtrations on U^{DR} and its Lie algebra. That is, torsors for U^{DR} can be classified by U^{DR}/F^0 or $F^0 \backslash U^{DR}$. Now, in [6], section 3, we described $p^{cr} \in R_x$ as the power series

$$G(x) = \sum_w \int_b^x \alpha_w w,$$

which is actually an element of U^{DR} . However, this identification was achieved through a trivialization of the universal bundle with connection that is compatible with the Hodge structure, that is, an element p^H of $F^0\pi_1^{DR}(X_{\mathbb{Q}_p}; b, x)$. So the element $G(x)$ is the unique u that satisfies $p^{cr} = p^H u$, rather than $p^{cr}u = p^H$ as written there. With this normalization, the correct classifying space becomes

$$F^0 \backslash U^{DR}.$$

The computation of p_2^{cr} then becomes

$$\begin{aligned}
p_2^{cr} &= 1 + \int_b^x \alpha A + \int_b^x \beta B + \int_b^x \alpha \alpha A^2 + \int_b^x \beta \beta B^2 + \int_b^x \alpha \beta AB + \int_b^x \beta \alpha BA \\
&= 1 + \int_b^x \alpha A + \int_b^x \beta B + \left(\int_b^x \alpha \right)^2 A^2 / 2 + \left(\int_b^x \beta \right)^2 B^2 / 2 + \int_b^x \alpha \beta AB - \int_b^x \alpha \beta BA + \int_b^x \alpha \beta BA + \int_b^x \beta \alpha BA \\
&= 1 + \int_b^x \alpha A + \int_b^x \beta B + \left(\int_b^x \alpha \right)^2 A^2 / 2 + \left(\int_b^x \beta \right)^2 B^2 / 2 + \int_b^x \alpha \beta [A, B] + \int_b^x \beta \int_b^x \alpha BA \\
&= \left(1 + \int_b^x \beta B + \left(\int_b^x \beta \right)^2 B^2 / 2 \right) \left(1 + \int_b^x \alpha A + \left(\int_b^x \alpha \right)^2 A^2 / 2 \right) \left(1 + \int_b^x \alpha \beta [A, B] \right) \\
&= \exp\left(\int_b^x \beta B \right) \exp\left(\int_b^x \alpha A + \int_b^x \alpha \beta [A, B] \right).
\end{aligned}$$

Therefore,

$$j_2^{dr/cr}(x) = \int_b^x \alpha A + \int_b^x \alpha \beta [A, B],$$

and we see that the formula for the function in corollary 0.2 should be

$$(\log_\alpha y)^2 D_2(z) - (\log_\alpha z)^2 D_2(y).$$

(Fortunately, this is simpler than the one originally given.) In other words, the quantity

$$D_2(z) / (\log_\alpha z)^2$$

is the same for all integral points z of infinite order. \square

Finally, we remarked at the beginning that the vanishing of the function works also for an integral base-point of order 2. Such a possibility was explicitly included in Lemma (1.2'). However, since Corollary (0.2) was originally written just for a tangential base-point, it may be useful to see directly why it carries over to a base-point of order 2. For this, it is useful to note another proof of the explicit formula due to Gerd Faltings.

With either kind of base-point, the class

$$j_2(z) - \frac{\log_\alpha z}{\log_\alpha y} j_2(y)$$

lies in $H_f^1(G, \mathbb{Q}_p(1))$ and vanishes at all $l \neq p$. In particular, it must come from a number in \mathbb{Q}^* that is a local unit at all primes. But then, the number must be ± 1 , and hence, the class in $H_f^1(G, \mathbb{Q}_p(1))$ is zero. Going over to the De Rham side at p , the formula for $j_2^{dr/cr}$ shows that the difference in classes is captured by

$$\int_b^z \alpha \beta - \left(\frac{\log_\alpha z}{\log_\alpha y} \right)^2 \int_b^y \alpha \beta$$

as in section 3 of the paper, which therefore must vanish.

1 Some examples

The following computations were carried out using Sage [8]. Sage includes an implementation of single Coleman integration for hyperelliptic curves developed by Balakrishnan, Bradshaw, and Kedlaya [3]; the computations here rely on a generalization to multiple integrals suggested in op. cit. (cf. [2]). They also depend on Cremona's tables of elliptic curves [5], which are included in Sage. See [1] for the full Sage source code used in the computations, which will appear in a future release of Sage. An integral two-torsion base-point is used in each of the first three examples.

Example 1 Let E be the elliptic curve $y^2 = x^3 - 1323x + 3942$, with minimal model

$$\mathcal{E} : y^2 + xy = x^3 - x$$

(Cremona label '65a1'). Let $b = (3, 0), P = (39, 108), Q = (-33, -108), R = (147, 1728), S = (103, 980), T = (-6, -108)$ be points on E , which arise from points on \mathcal{E} in the following manner:

$$\begin{aligned} \mathcal{E} &\longrightarrow E \\ (0, 0) &\mapsto (3, 0) \\ (1, 0) &\mapsto (39, 108) \\ (-1, 0) &\mapsto (-33, -108) \\ (4, 6) &\mapsto (147, 1728) \\ \left(\frac{25}{9}, \frac{85}{27}\right) &\mapsto (103, 980) \\ \left(-\frac{1}{4}, -\frac{3}{8}\right) &\mapsto (-6, -108). \end{aligned}$$

Note that $p = 11$ is a prime of good reduction for E . We compute

$$\frac{D_2(P)}{(\log_\alpha(P))^2} = \frac{D_2(Q)}{(\log_\alpha(Q))^2} = \frac{D_2(R)}{(\log_\alpha(R))^2} = 3 \cdot 11^{-1} + 6 + 2 \cdot 11 + 10 \cdot 11^2 + 3 \cdot 11^3 + 5 \cdot 11^4 + O(11^5).$$

However,

$$\frac{D_2(S)}{(\log_\alpha(S))^2} = 3 \cdot 11^{-1} + 10 + 6 \cdot 11 + 9 \cdot 11^2 + 8 \cdot 11^3 + 6 \cdot 11^4 + O(11^5),$$

and

$$\frac{D_2(T)}{(\log_\alpha(T))^2} = 6 \cdot 11^{-1} + 1 + 4 \cdot 11 + 4 \cdot 11^2 + 11^3 + 7 \cdot 11^4 + O(11^5).$$

Example 2 Let E be the elliptic curve $y^2 = x^3 - 3483x + 74358$, with minimal model

$$\mathcal{E} : y^2 + xy + y = x^3 - x^2 - 3x + 2$$

(Cremona label '145a1'). Let $b = (27, 0), P = (63, 324), Q = (-9, 324), R = (-9, -324), S = (43, 64), T = (-54, 324)$ be points on E , which arise from points on \mathcal{E} in the following manner:

$$\begin{aligned} \mathcal{E} &\longrightarrow E \\ (1, -1) &\mapsto (27, 0) \\ (2, 0) &\mapsto (63, 324) \\ (0, 1) &\mapsto (-9, 324) \\ (0, -2) &\mapsto (-9, -324) \\ \left(\frac{13}{9}, -\frac{25}{27}\right) &\mapsto (43, 64) \\ \left(-\frac{5}{4}, \frac{13}{8}\right) &\mapsto (-54, 324). \end{aligned}$$

Note that $p = 7$ is a prime of good reduction for E . We compute

$$\frac{D_2(P)}{(\log_\alpha(P)\alpha)^2} = \frac{D_2(Q)}{(\log_\alpha(Q)\alpha)^2} = \frac{D_2(R)}{(\log_\alpha(R))^2} = 6 \cdot 7^{-2} + 7^{-1} + 5 + 7^2 + 2 \cdot 7^3 + 5 \cdot 7^4 + O(7^5).$$

However,

$$\frac{D_2(S)}{(\log_\alpha(S))^2} = 3 \cdot 7^{-3} + 3 \cdot 7^{-2} + 5 + 6 \cdot 7 + 2 \cdot 7^2 + 3 \cdot 7^3 + 6 \cdot 7^4 + O(7^5),$$

and

$$\frac{D_2(T)}{(\log_\alpha(T))^2} = 7^{-3} + 4 \cdot 7^{-2} + 2 \cdot 7 + 3 \cdot 7^2 + 3 \cdot 7^4 + O(7^5).$$

Example 3 Let E be the elliptic curve $y^2 = x^3 - 18171x + 940950$, with minimal model

$$\mathcal{E} : y^2 + xy = x^3 - 14x + 19$$

(Cremona label '689a1'). Let $b = (75, 0), P = (39, 540), Q = (111, -540), R = (39, -540), S = (-150, 540), T = (-150, -540)$ be points on E , which arise from points on \mathcal{E} in the following manner:

$$\begin{aligned} \mathcal{E} &\longrightarrow E \\ (2, -1) &\mapsto (75, 0) \\ (1, 2) &\mapsto (39, 540) \\ (3, -4) &\mapsto (111, -540) \\ (1, -3) &\mapsto (39, -540) \\ \left(-\frac{17}{4}, \frac{37}{8}\right) &\mapsto (-150, 540) \\ \left(-\frac{17}{4}, -\frac{3}{8}\right) &\mapsto (-150, -540). \end{aligned}$$

Note that $p = 17$ is a prime of good reduction for E . We compute

$$\frac{D_2(P)}{(\log_\alpha(P))^2} = \frac{D_2(Q)}{(\log_\alpha(Q))^2} = \frac{D_2(R)}{(\log_\alpha(R))^2} = 12 \cdot 17^{-1} + 13 + 3 \cdot 17 + 9 \cdot 17^2 + 9 \cdot 17^3 + 3 \cdot 17^4 + O(17^5).$$

However,

$$\frac{D_2(S)}{(\log_\alpha(S))^2} = \frac{D_2(T)}{(\log_\alpha(T))^2} = 11 \cdot 17^{-1} + 11 + 13 \cdot 17 + 5 \cdot 17^2 + 2 \cdot 17^3 + 11 \cdot 17^4 + O(17^5).$$

Together with the non-trivial examples, we have included above some comparison of points x and $-x$, for which the quotients are equal for purely local reasons. That is, equality occurs for these simply because

$$\int_b^{-x} \alpha = - \int_b^x \alpha$$

and

$$\int_b^{-x} \alpha\beta = \int_b^{-x} [-1]^*(\alpha)[-1]^*(\beta) = \int_b^x \alpha\beta.$$

We note that the denominator $(\int_b^x \alpha)^2$ is in any case quadratic as a function of x . However, the numerator is definitely not quadratic. If it were, we would get the same quotients even for rational points in this rank one situation, which the computations show not to be the case. In fact, as noted already in [6], for a fixed y , the equality

$$D_2(z) = (\log_\alpha(z))^2 \frac{D_2(y)}{(\log_\alpha(y))^2}$$

can hold only for finitely many points in $\mathcal{X}(\mathbb{Z}_p)$. That is to say, there is no local explanation for the constancy of the ratio on general pairs of integral points. It is unquestionably a *global* phenomenon, akin to a non-abelian reciprocity law.

Even though it is presently difficult to compute with a tangential base-point, it is possible to circumvent its direct use when we are given *two* integral points x and y of infinite order such that x is not of the form $\pm y + t$ where t is torsion.

This uses the co-product formula by viewing the path from the tangent vector b to y as the path from b to x followed by the path from x to y . That is,

$$\int_b^y \alpha\beta = \int_x^y \alpha\beta + \int_x^y \alpha \int_b^x \beta + \int_b^x \alpha\beta.$$

Since

$$\int_b^y \alpha\beta / (\int_b^y \alpha)^2 = \int_b^x \alpha\beta / (\int_b^x \alpha)^2,$$

we then get

$$\int_b^y \alpha\beta(1 - (\int_b^x \alpha)^2 / (\int_b^y \alpha)^2) = \int_x^y \alpha\beta + \int_x^y \alpha \int_b^x \beta,$$

or

$$\int_b^y \alpha\beta / (\int_b^y \alpha)^2 = (\int_x^y \alpha\beta + \int_x^y \alpha \int_b^x \beta) / ((\int_b^y \alpha)^2 - (\int_b^x \alpha)^2).$$

Since α is regular at e , the term $\int_b^y \alpha = \int_e^y \alpha$ and $\int_b^x \alpha = \int_e^x \alpha$. Furthermore,

$$\int_b^z \beta = (1/2) \int_{-z}^z \beta$$

for any z . To see this, note that

$$\begin{aligned} \int_{-z}^z \beta &= \int_{-z}^b \beta + \int_b^z \beta = - \int_b^{-z} \beta + \int_b^z \beta = \int_b^{-z} [-1]^*(\beta) + \int_b^z \beta \\ &= \int_{-b}^z \beta + \int_b^z \beta = \int_{-b}^b \beta + 2 \int_b^z \beta. \end{aligned}$$

The integral here between tangential base-points is zero: Recall briefly the definition of the fiber functor associated to a tangential base point. There is a functor

$$Res : \text{Un}(X) \rightarrow \text{Un}(D^*)$$

from unipotent bundles with connection on X to those on the punctured tangent space $D^* = T_e^0(E)$, which associates to (V, ∇) ,

$$(V_e \otimes \mathcal{O}_D, d - Ndz/z),$$

where N is the residue of the canonical logarithmic extension of (V, ∇) and z is any linear coordinate on the tangent space. For a tangent vector $b \in D^*$, we then have

$$F_b : (V, \nabla) \mapsto Res(V, \nabla) \mapsto (V_e \otimes \mathcal{O}_D^*)|_b \simeq V_e.$$

Therefore, if b and b' are two tangential base-points, then the Frobenius invariant path from b , b' is induced by the one coming from the category $\text{Un}(D^*)$. That is to say, Res induces a map

$$\pi_1^{DR}(D^*; b, b') \rightarrow \pi_1^{DR}(X; b, b')$$

and the Frobenius invariant path comes from the first space. Therefore, for any (V, ∇) , we get that $p_{bb'}$ is given by multiplication by

$$\exp(N \int_b^{b'} dz/z).$$

Now, since

$$\int_b^x dz/z$$

is a homomorphism in x for the group law where b is the origin, we get that

$$\int_b^{\zeta b} dz/z = 0$$

and hence, $p_{b(\zeta b)} = 1$ for any root ζ of 1.

To use this formula, note that for a third integral point z of infinite order, we have

$$\frac{(\int_x^y \alpha \beta + \int_x^y \alpha \int_b^x \beta)}{((\int_b^y \alpha)^2 - (\int_b^x \alpha)^2)} = \frac{(\int_x^z \alpha \beta + \int_x^z \alpha \int_b^x \beta)}{((\int_b^z \alpha)^2 - (\int_b^x \alpha)^2)}$$

as long as the denominator is non-zero. So if we had x and y in hand, we could search for such z in the zero set of the function

$$((\int_b^z \alpha)^2 - (\int_b^x \alpha)^2) \frac{(\int_x^y \alpha \beta + \int_x^y \alpha \int_b^x \beta)}{((\int_b^y \alpha)^2 - (\int_b^x \alpha)^2)} - (\int_x^z \alpha \beta + \int_x^z \alpha \int_b^x \beta)$$

of z , where everything can be computed without the direct use of the tangential base-point.

Furthermore, we can express the quotient $D_2(z)/(\log_\alpha(z))^2$ for an arbitrary point z using the two integral points x and y as follows. The coproduct formula again gives

$$\int_b^z \alpha \beta = \int_y^z \alpha \beta + \int_y^z \alpha \int_b^y \beta + \int_b^y \alpha \beta,$$

but we have already a formula for the last integral that eliminates the direct use of the tangential base-point. So

$$\int_b^z \alpha \beta = \int_y^z \alpha \beta + \int_y^z \alpha \int_b^y \beta + (\int_b^y \alpha)^2 \frac{(\int_x^y \alpha \beta + \int_x^y \alpha \int_b^x \beta)}{((\int_b^y \alpha)^2 - (\int_b^x \alpha)^2)}$$

and

$$\frac{D_2(z)}{(\log_\alpha(z))^2} = \frac{\int_y^z \alpha \beta}{(\log_\alpha(z))^2} + \frac{\int_y^z \alpha \int_b^y \beta}{(\log_\alpha(z))^2} + \frac{(\log_\alpha(y))^2}{(\log_\alpha(z))^2} \frac{(\int_x^y \alpha \beta + \int_x^y \alpha \int_b^x \beta)}{((\log_\alpha(y))^2 - (\log_\alpha(x))^2)}.$$

Example 4 We are now able to give an example without integral 2-torsion, using the tangential base-point implicitly. Consider the curve $E : y^2 = x^3 - 16x + 16$, with minimal model given by

$$\mathcal{E} : y^2 + y = x^3 - x$$

(Cremona label '37a1'). Let $P = (0, 4)$, $2P = (4, 4)$, $3P = (-4, -4)$, $4P = (8, -20)$, $6P = (24, 116)$ be points on E , which arise from points on \mathcal{E} in the following manner:

$$\begin{aligned} \mathcal{E} &\longrightarrow E \\ (0, 0) &\mapsto (0, 4) \\ (1, 0) &\mapsto (4, 4) \\ (-1, -1) &\mapsto (-4, -4) \\ (2, -3) &\mapsto (8, -20) \\ (6, 14) &\mapsto (24, 116). \end{aligned}$$

Note that $p = 7$ is a prime of good reduction. For each of the ten (unordered) pairs (x, y) , where $x \neq y, x, y \in \{P, 2P, 3P, 4P, 6P\}$, we see

$$\frac{\int_x^y \alpha \beta + \int_x^y \alpha \int_b^x \beta}{\left(\int_b^y \alpha\right)^2 - \left(\int_b^x \alpha\right)^2} = 7^{-1} + 1 + 3 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^4 + O(7^5).$$

This implies that

$$\begin{aligned} \frac{D_2(P)}{(\log_\alpha(P))^2} &= \frac{D_2(2P)}{(\log_\alpha(2P))^2} = \frac{D_2(3P)}{(\log_\alpha(3P))^2} = \frac{D_2(4P)}{(\log_\alpha(4P))^2} = \frac{D_2(6P)}{(\log_\alpha(6P))^2} \\ &= 7^{-1} + 1 + 3 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^4 + O(7^5). \end{aligned}$$

However, we also have the non-integral points with minimal coordinates

$$5P = \left(\frac{1}{4}, \frac{5}{8}\right), \quad 7P = \left(\frac{-5}{9}, \frac{8}{27}\right), \quad 8P = \left(\frac{21}{25}, \frac{-69}{125}\right), \quad 9P = \left(\frac{-20}{49}, \frac{-435}{343}\right), \quad 10P = \left(\frac{161}{16}, \frac{-2065}{64}\right)$$

with which one can compute

$$\frac{D_2(5P)}{(\log_\alpha(5P))^2} = 2 * 7^{-1} + 5 + 3 * 7 + 6 * 7^2 + 3 * 7^3 + 5 * 7^4 + 4 * 7^5 + 2 * 7^6 + O(7^7)$$

$$\frac{D_2(7P)}{(\log_\alpha(7P))^2} = 5 * 7^{-3} + 3 * 7^{-1} + 1 + 4 * 7 + 3 * 7^2 + 7^3 + 6 * 7^4 + O(7^5)$$

$$\frac{D_2(8P)}{(\log_\alpha(8P))^2} = 6 * 7^{-1} + 4 + 7 + 7^2 + 5 * 7^3 + 4 * 7^4 + 2 * 7^5 + 5 * 7^6 + O(7^7)$$

$$\frac{D_2(9P)}{(\log_\alpha(9P))^2} = 3 * 7^{-8} + 7^{-6} + O(7^{-5})$$

$$\frac{D_2(10P)}{(\log_\alpha(10P))^2} = 5 * 7^{-1} + 6 + 6 * 7 + 2 * 7^2 + 2 * 7^3 + 5 * 7^4 + 5 * 7^5 + 4 * 7^6 + O(7^7)$$

to see the values fluctuating over the non-integral points.

Acknowledgements: M.K. is extremely grateful to J.B. and K.K. for informing him of the initial computations that led to the discovery of the mistake and for agreeing to work together on the correction. The authors are grateful to Amod Agashe, Dino Lorenzini, Robert L. Miller, and William Stein for a number of helpful discussions leading to the examples.

References

- [1] Balakrishnan, J. S. Sage code available at <http://math.mit.edu/~kedlaya/papers/>.
- [2] Balakrishnan, J. S. Explicit iterated Coleman integration for hyperelliptic curves and the non-abelian Chabauty method, in preparation.
- [3] Balakrishnan, J.S.; Bradshaw, R.W.; and Kedlaya, K.S. Explicit Coleman integration for hyperelliptic curves, in ANTS 9, Lecture Notes in Computer Science, Springer-Verlag, to appear; preprint available at <http://math.mit.edu/~kedlaya/papers/>.
- [4] Bosch, Siegfried; Lütkebohmert, Werner; Raynaud, Michel Néron models. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21. Springer-Verlag, Berlin, 1990.
- [5] Cremona, J. E. Algorithms for modular elliptic curves. Second edition. Cambridge University Press, Cambridge, 1997. vi+376 pp.

- [6] Kim, Minhyong Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.* 23 (2010), 725-747.
- [7] Kim, Minhyong, and Tamagawa, Akio The l -component of the unipotent Albanese map. *Math. Ann.* 340 (2008), no. 1, 223–235.
- [8] Stein, W. et al. Sage mathematics software (version 4.3.5), 2010, <http://www.sagemath.org>.

J.B. and K.K.: Department of Mathematics, M.I.T., 77 Massachusetts Avenue, Cambridge, MA 02139-4307, U.S.A.
M.K.: Department of Mathematics, University College London, Gower Street, London, WC1E 6BT, United Kingdom
and The Korea Institute for Advanced Study, Hoegiro 87, Dongdaemun-gu, Seoul 130-722, Korea.