Two Longer Corrections to *Elliptic Curves* from Langlands

First Correction

Difficulty. The use of Proposition 5.5 to obtain Proposition 5.6 is inadequate if the reduction map r_p on the set of distinct points among $\{P, Q, PQ\}$ is not one-one. For example, if P, Q, and PQ are distinct and $r_p(P) = r_p(Q) = r_p(PQ)$, then Proposition 5.5 shows that the intersection multiplicity for $r_p(P)$ is ≥ 1, but it does not produce either a second or a third point on r_p of the line. Thus we cannot obtain the desired conclusion that $r_p(P)r_p(P) = r_p(P)$, i.e., that $r_p(P)$ has intersection multiplicity 3. What is needed is an improved version of Proposition 5.5 and then a little extra argument in Proposition 5.6 to show that all cases have been handled. The improved version below is actually more than is needed; only the cases $k \leq 2$ are needed with elliptic curves, and a page of matrix calculations are unncessary for such cases. However, the principle is a little clearer with the version of Proposition 5.5 given below.

Correction. Change Proposition 5.5, its proof, and the proof of Proposition 5.6 as follows.

Proposition 5.5. Suppose $F \in \mathbb{Q}[x, y, w]_m$ is a plane curve, $L \in \mathbb{Q}[x, y, w]_1$ is a line, and $P_0, P_1, \ldots, P_k$ are $k + 1 \geq 1$ distinct points on L having the same reductions modulo p. If F_p and L_p are reductions of F and L modulo p, then the intersection multiplicities satisfy

$$\min\big(m,\ i(P_0, L, F) + k\big) \leq i(r_p(P_0), L_p, F_p). \tag{5.6}$$

Proof. Without loss of generality, we may assume for $0 \leq i \leq k$ that (x_i, y_i, w_i) is a p-reduced representative of P_i. Scaling by a common denominator prime to p, we may assume for each $i \geq 0$ that x_i, y_i, w_i are all integers. The condition that $r_p(P_0) = r_p(P_i)$ means for each $i \geq 1$ that there is an integer a_i prime to p with $(x_0, y_0, w_0) \equiv a_i(x_i, y_i, w_i) \bmod p$. Changing notation, we may assume for $i \geq 0$ that (x_i, y_i, w_i) is a p-reduced representative of P_i with integer entries and that $(x_i, y_i, w_i) \equiv (x_0, y_0, w_0) \bmod p$ for $i \geq 1$.

Fix a point P' of L with $r_p(P') \neq r_p(P_0)$, and let (x', y', w') be a p-reduced representative of it with integer coordinates. In preparation for p reduction, we may assume that F has been scaled so that all its coefficients are integers and at least one of its coefficients is prime to p. Form the polynomial in $\mathbb{Z}[t]$ given by

$$\psi(t) = F(x_0 + tx', y_0 + ty', w_0 + tw') = t^r \widetilde{F}_r + \cdots + t^m \widetilde{F}_m$$

with $\widetilde{F}_r \neq 0$. By Proposition 2.9 the intersection multiplicity $i(P_0, L, F)$ equals r. Recomputing $\psi(t)$ modulo p (i.e., in $\mathbb{Z}_p[t]$) and applying Proposition 2.9 again, we see that we are done if $k = 0$ and that it is enough to show that p divides the integers $\widetilde{F}_r, \ldots, \widetilde{F}_{\min(m,\, r+k-1)}$ if $k \geq 1$. For the remainder of the proof, there is no loss of generality in assuming that $1 \leq k \leq m - r + 1$.

For $i \geq 1$ it follows from the facts that $P_i \neq P'$ and that P_i is on L that there exists a unique $t_i \in \mathbb{Q}$ such that $[(x_i, y_i, w_i)] = [(x_0 + t_i x', y_0 + t_i y', w_0 + t_i w')]$. Since $P_0, \ldots, P_k$ are distinct, the rationals $t_1, \ldots, t_k$ are distinct and nonzero. We shall derive some properties of the numbers t_i. Let us write

$$(x_i, y_i, w_i) = c(x_0 + t_i x', y_0 + t_i y', w_0 + t_i w')$$

for some nonzero $c \in \mathbb{Q}$. For each $i \geq 1$, the fact that $r_p(P_i) \neq r_p(P')$ implies that some 2-by-2 determinant from two of the coordinates of (x_i, y_i, w_i) and (x', y', w') is $\not\equiv 0 \bmod p$. Without loss of generality, suppose that these coordinates are the first two, so that $x_i y' - y_i x' \not\equiv 0 \bmod p$. Since $c \neq 0$, the equations $x_i = c(x_0 + t_i x')$ and $y_i = c(y_0 + t_i y')$ together imply that $x_i(y_0 + t_i y') = y_i(x_0 + t_i x')$, hence that

$$t_i = \frac{y_i x_0 - x_i y_0}{x_i y' - y_i x'}.$$

The fact that $x_i y' - y_i x' \not\equiv 0 \bmod p$ implies that t_i is a p-integral member of $\mathbb{Q}$, and the fact that $(x_i, y_i, w_i) \equiv (x_0, y_0, w_0) \bmod p$ implies that the numerator is divisible by p. In other words the p-adic norm satisfies $|t_i|_p < 1$.

Meanwhile each t_i with $i \geq 1$ satisfies

$$\begin{aligned} 0 &= F(x_i, y_i, w_i) = c^m F(x_0 + t_i x', y_0 + t_i y', w_0 + t_i w') \\ &= c^m (t_i^r \widetilde{F}_r + t_i^{r+1} \widetilde{F}_{r+1} + \cdots + t_i^m \widetilde{F}_m). \end{aligned}$$

Since c and all t_i are nonzero, we therefore obtain a system of k equations

$$\widetilde{F}_r + t_i \widetilde{F}_{r+1} + \cdots + t_i^{m-r} \widetilde{F}_m = 0 \qquad \text{for } 1 \leq i \leq k$$

in the $m - r + 1$ unknowns $\widetilde{F}_r, \ldots, \widetilde{F}_m$. In matrix form the system is

$$\begin{pmatrix} 1 & t_1 & t_1^2 & \cdots & t_1^{m-r} \\ & & \vdots & & \\ 1 & t_k & t_k^2 & \cdots & t_k^{m-r} \end{pmatrix} \begin{pmatrix} \widetilde{F}_r \\ \vdots \\ \widetilde{F}_m \end{pmatrix} = 0.$$

In the second paragraph of the proof, we saw that we may take $1 \leq k \leq m - r + 1$.

Suppose first that $k = m - r + 1$. Then the coefficient matrix is a Vandermonde matrix, up to transpose, and is invertible since the numbers t_i are distinct. We see in this case that $\widetilde{F}_r, \ldots, \widetilde{F}_m$ are all 0 and in particular that they are all divisible by p.

Now suppose that $1 \leq k < m - r + 1$. Let us write the matrix of coefficients in blocks as $(V(k) \;\; U(k))$, where

$$V(k) = \begin{pmatrix} 1 & t_1 & t_1^2 & \cdots & t_1^{k-1} \\ & & \vdots & & \\ 1 & t_k & t_k^2 & \cdots & t_k^{k-1} \end{pmatrix} \qquad \text{and} \qquad U(k) = \begin{pmatrix} t_1^k & \cdots & t_1^{m-r} \\ & & \vdots \\ t_k^k & \cdots & t_k^{m-r} \end{pmatrix}.$$

Here $V(k)$ and $U(k)$ have k rows, $V(k)$ has k columns, and $U(k)$ has $m - r + k + 1$ columns. Then our system of equations is

$$\begin{pmatrix} V(k) & U(k) \end{pmatrix} \begin{pmatrix} \widetilde{F}^* \\ \widetilde{F}^{**} \end{pmatrix} = 0,$$

where

$$\widetilde{F}^* = \begin{pmatrix} \widetilde{F}_r \\ \vdots \\ F_{r+k-1} \end{pmatrix} \qquad \text{and} \qquad \widetilde{F}^{**} = \begin{pmatrix} \widetilde{F}_{r+k} \\ \vdots \\ F_m \end{pmatrix}.$$

The matrix $V(k)$ is a Vandermonde matrix and is invertible; let $V(k)^{-1}$ be the inverse. If we multiply through on the left by $V(k)^{-1}$, then our system of equations becomes

$$F^* + V(k)^{-1}U(k)F^{**} = 0.$$

Let us introduce the diagonal matrix D with diagonal entries $t_1, \ldots, t_k$, the elementary symmetric functions

$$\sigma_1 = t_1 + \cdots + t_k, \ \ldots \ , \ \sigma_k = t_1 \cdots t_k$$

of $t_1, \ldots, t_n$, and the k-by-k matrix

$$W = \begin{pmatrix} 0 & 0 & \cdots & 0 & (-1)^{k+1}\,\sigma_k \\ 1 & 0 & \cdots & 0 & (-1)^{k}\,\sigma_{k-1} \\ 0 & 1 & \cdots & 0 & (-1)^{k-1}\,\sigma_{k-2} \\ & & \vdots & & \\ 0 & 0 & \cdots & 0 & -\sigma_2 \\ 0 & 0 & \cdots & 1 & \sigma_1 \end{pmatrix}.$$

A routine computation shows that $DV(k) = V(k)W$. Hence $V(k)^{-1}D = WV(k)^{-1}$. Meanwhile the columns of $U(k)$ are of the form

$$C_l = \begin{pmatrix} t_1^l \\ \vdots \\ t_k^l \end{pmatrix} \qquad \text{for } k \leq l \leq m,$$

and they satisfy $C_{l+1} = DC_l$ for $l \geq 0$. Therefore

$$V(k)^{-1}C_{l+1} = V(k)^{-1}DC_l = WV(k)^{-1}C_l,$$

and the result is a recursive formula for computing the columns of $V(k)^{-1}U(k)$. For $l = k-1$, C_l is the last column of $V(k)$, and $V(k)^{-1}C_{k-1}$ thus yields the last column e_k of the identity matrix. Consequently our recursive formula gives

$$V(k)^{-1}C_l = W^{l-k+1}e_k \qquad \text{for } l \geq k-1.$$

Examining W and its powers, we see inductively that the $(i,k)^{\text{th}}$ entry of W^{l-k+1} is a homogeneous polynomial in $t_1, \ldots, t_k$ of degree $l-i+1$. The columns of $U(k)$ come from columns C_l with $l \geq k$, and we conclude that each entry of $V(k)^{-1}U(k)$ is a homogeneous polynomial in $t_1, \ldots, t_k$ of some degree ≥ 1.

Applying the formula $F^* + V(k)^{-1}U(k)F^{**} = 0$, we obtain expressions of the form

$$\widetilde{F}_i = \sum_{j=k}^{m} P_{ij}(t_1, \ldots, t_k)\widetilde{F}_j$$

for $1 \leq i \leq k$; here each P_{ij} is a homogeneous polynomial of degree ≥ 1. Applying $|\cdot|_p$ to both sides and using that $|t_i|_p < 1$ for $1 \leq i \leq k$ and $|\widetilde{F}_j|_p \leq 1$ for all j, we obtain $|\widetilde{F}_i|_p < 1$ for $1 \leq i \leq k$. Hence $\widetilde{F}_i \equiv 0 \bmod p$ for $1 \leq i \leq k$, and the proof is complete.

(*The paragraph following the proof of Proposition 5.5 is unchanged, and so is the statement of Proposition 5.6.*)

PROOF. Since $r_p(0,1,0) = (0,1,0)$, r_p carries O to O_p. If L is a given line, suppose that we are given points P_j on L with $\sum_j i(P_j, L, E) = 3$ and with $i(P_j, L, E) \geq 1$ in each case. The heart of the proof is to show that if P and Q are points lying on L and E, then $r_p(PQ) = r_p(P) \cdot r_p(Q)$. Indeed, if this identity is always valid, then

$$\begin{aligned} r_p(P+Q) &= r_p(O \cdot PQ) = r_p(O) \cdot r_p(PQ) = r_p(O) \cdot (r_p(P) \cdot r_p(Q)) \\ &= O_p \cdot (r_p(P) \cdot r_p(Q)) = r_p(P) + r_p(Q), \end{aligned}$$

and r_p is a group homomorphism.

We now divide matters into cases. First, if r_p is one-one on the set $\{P_j\}$, then Proposition 5.5 gives $i(P_j, L, E) \leq i(r_p(P_j), L_p, E_p)$ for each j. Since the sum of intersection multiplicities over L_p is ≤ 3 (by nonsingularity of E_p), we conclude that $i(P_j, L, E) = i(r_p(P_j), L_p, E_p)$ for each j and that no other points besides the points $r_p(P_j)$ lie on L_p and E_p. It follows that $r_p(PQ) = r_p(P) \cdot r_p(Q)$, as asserted.

Second, suppose that $\{P_0, P_1, P_2\}$ are distinct on L and that $r_p(P_0) = r_p(P_1) \neq r_p(P_2)$. Applying Proposition 5.5 to $\{P_0, P_1\}$ and then to P_2, we obtain $i(r_p(P_0), L_p, E_p) \geq i(P_0, L, E) + 1 \geq 2$ and $i(r_p(P_2), L_p, E_p) \geq i(P_2, L, E) \geq 1$. Since $i(r_p(P_0), L_p, E_p) + i(r_p(P_2), L_p, E_p) \leq 3$, we conclude that $i(r_p(P_0), L_p, E_p) = 2$ and $i(r_p(P_2), L_p, E_p) = 1$. There can be no further points on L_p and E_p, and again our identity for $r_p(PQ)$ is established.

Third, suppose that $\{P_0, P_1, P_2\}$ are distinct on L and that $r_p(P_0) = r_p(P_1) = r_p(P_2)$. Proposition 5.5 shows that $i(r_p(P_0), L_p, E_p) \geq i(P_0, L, E) + 2 \geq 1 + 2 = 3$, and therefore $i(r_p(P_0), L_p, E_p) = 3$. There can be no further points on L_p and E_p, and again our identity for $r_p(PQ)$ is established.

Finally, suppose that $\{P_0, P_1\}$ are distinct on L, that $i(P_0, L, E) = 2$, and that $r_p(P_0) = r_p(P_1)$. Proposition 5.5 shows that $i(r_p(P_0), L_p, E_p) \geq i(P_0, L, E) + 1 \geq 2 + 1 = 3$, and therefore $i(r_p(P_0), L_p, E_p) = 3$. There can be no further points on L_p and E_p, and again our identity for $r_p(PQ)$ is established. All cases have been handled, and the proof is complete.

SECOND CORRECTION

DIFFICULTY. The proof on pages 299–300 of (10.21) that extends from the statement of (10.21) to the end of the paragraph has a gap. In effect it assumes that the numerator and denominator of (10.20) are relatively prime, and such an assertion requires proof.

CORRECTION. Replace the last 4 lines of page 299 and the first 8 lines of page 300 by the following.

up to a $\mathbb{Z}_p$ factor. Write $\dfrac{(Qx-P)^2}{BD} = \dfrac{R}{S}$ with R and S relatively prime in $\mathbb{Z}_p[x]$. Then (10.20) gives

$$RAC = S[(Px - aQ)^2 - 4bQ(Qx + P)] \tag{10.22a}$$

$$RBD = S(Qx-P)^2, \tag{10.22b}$$

and (10.19) gives

$$R(AD + BC) = 2S[PQx^2 + P^2x + axQ^2 + 2bQ^2 + aPQ]. \tag{10.22c}$$

Let F be a prime factor of S. Since $\mathrm{GCD}(R, S) = 1$, (10.22b) shows that $F \mid BD$. Without loss of generality, suppose $F \mid B$. Then $F \nmid A$ since $\mathrm{GCD}(A, B) = 1$. Since (10.22a) shows that $F \mid AC$, $F \mid C$. Thus $F \mid BC$. By (10.22c), $F \mid (AD + BC)$. So $F \mid AD$. Since $F \nmid A$, $F \mid D$. Then $F \mid C$ and $F \mid D$, in contradiction to $\mathrm{GCD}(C, D) = 1$. We conclude that S is a scalar. Now consider R. If G is a prime factor of R, then (10.22b) shows that $G \mid (Qx - P)$. The expressions in brackets on the right sides of (10.22a) and (10.22c) must therefore be divisible by G when we substitute Qx for P. On the other hand, G does not divide Q since otherwise it would divide $P = Qx - (Qx - P)$, in contradiction to the condition $\mathrm{GCD}(P, Q) = 1$. Thus the divisibility by G for the expressions in brackets implies that G divides both $U(x) = (x^2 - a)^2 - 8bx$ and $V(x) = x^3 + ax + b$. Consequently G divides $\mathrm{GCD}(U, V)$. A little computation shows that $\mathrm{GCD}(U, V) = 1$ unless $4a^3 + 27b^2 = 0$. Since $4a^3 + 27b^2$ is, up to sign, the discriminant of our cubic and is by assumption nonzero, we conclude that R has no prime factors and is scalar. This proves (10.21).

5/2/05