Intersecting algebraic plane curves with the Euclidean algorithm

Jan Hilmar and Chris Smyth

Fields Institute, 24 September 2009

arXiv:0907.0361[math]

$$A(x,y,z) = \sum_{i,j} a_{ij} x^i y^j z^{m-i-j}$$
$$B(x,y,z) = \sum_{i,j} b_{ij} x^i y^j z^{n-i-j}$$

$$\begin{aligned} i_{\mathbf{P}}(A,B) = & \text{ intersection multiplicity of } A \text{ and } B \\ & \text{at } \mathbf{P} \in \overline{K}\mathbb{P}^2, \\ = & \begin{cases} > 0 \text{ if } \mathbf{P} \text{ lies on both } A \text{ and } B, \\ = 0 \text{ otherwise.} \end{cases} \end{aligned}$$

Want formal sum $A \cdot B = \sum_{\mathbf{P}} i_{\mathbf{P}}(A,B)\mathbf{P}$, the *intersection cycle* of A and B, an object for recording the intersection of these curves.

Our algorithm does not need to use the definition of $i_{\mathbf{P}}(A,B)$, only standard properties of intersection cycles:

Proposition 1. *Let A, B and C be algebraic curves with*

$$\gcd(A, B) = \gcd(A, C) = 1.$$

Then

(a) $A \cdot B = B \cdot A$;

(b) $A \cdot (BC) = A \cdot B + A \cdot C$;

(c) $A \cdot (B + AC) = A \cdot B$ *if* $\partial B = \partial(AC)$;

(d) *If A and B are distinct lines, say $A(x, y, z) = a_1x + a_2y + a_3z$ and $B(x, y, z) = b_1x + b_2y + b_3z$, then their intersection cycle $A \cdot B$ is the single point $\mathbf{P}_\times$ given by*

$$\mathbf{P}_\times = \left(\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, \begin{vmatrix} a_3 & a_1 \\ b_3 & b_1 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \right).$$

Applying the Euclidean algorithm

$A, B \in K[x, y, z]$ be algebraic curves,
$\gcd(A, B) = 1$
$\partial_x A \geq \partial_x B \geq 1$.

By polynomial division we can find $q, r \in K(y, z)[x]$ with

$$A = qB + r$$

and $0 \leq \partial_x r < \partial_x B$ and $q, r \neq 0$.

Can multiply through by LCM $H \in K[y, z]$ of their denominators to get

$$HA = QB + R,$$

where $Q = qH, R = rH \in K[x, y, z]$ homogeneous, $\partial(QB) = \partial R$.

Suppose now that $G = \gcd(B, R)$. As $\gcd(A, B) = 1$, it is clear that also $\gcd(B, H) = G$, so we can divide through by G to get

$$H'A = QB' + R',$$

where $B = B'G$, $H = H'G$, $R = R'G$, and $\gcd(B', R') = \gcd(B', H') = 1$. Now

$$\begin{aligned}
A \cdot B &= A \cdot (B'G) \\
&= A \cdot B' + A \cdot G \\
&= (H'A) \cdot B' - H' \cdot B' + A \cdot G \\
&= (QB' + R') \cdot B' - H' \cdot B' + A \cdot G \\
&= R' \cdot B' - H' \cdot B' + A \cdot G
\end{aligned}$$

Intersecting curve with product of lines

Given $C \in K[x, y, z]$, $D \in K[y, z]$, can assume D irreducible $/K$.

$$D(y, z) = \prod_{\beta} (y - \beta z), \qquad (1)$$

where the β are roots in $\overline{K}$ of $D(y, 1)$. Thus $D =$ product of lines. Then since

$$C(x, y, z) = C(x, \beta z, z) + (y - \beta z)C''(x, y, z)$$

for some C'' in $K[x, y, z]$,

$$C \cdot (y - \beta z) = C(x, \beta z, z) \cdot (y - \beta z).$$

$$\begin{aligned} C \cdot D &= C(x, y, z) \cdot (\prod_{\beta} (y - \beta z)) \\ &= \sum_{\beta} C(x, \beta z, z) \cdot (y - \beta z). \end{aligned}$$

Next, factorize $C(x, \beta z, z)$ over $K(\beta)$. $C_2(x, z)$ = a typical factor, we have that over $\overline{K}$, we have

$$C_2(x, z) = \prod_{\gamma} (x - \gamma z),$$

where the γ are the roots in $\overline{K}$ of $C_2(x, 1)$, and

$$\begin{aligned} C_2 \cdot D &= \sum_{\beta} \sum_{\gamma} (x - \gamma z) \cdot (y - \beta z) \\ &= \sum_{\beta} \sum_{\gamma} (\gamma, \beta, 1). \end{aligned}$$

From our algorithm: intersection cycle $A \cdot B$ = sum or difference of simpler sums of the following types:

(1) The point $(1, 0, 0)$;

(2) A sum $\sum_\alpha (\alpha, 1, 0)$, over roots α of monic $f \in K[x]$ irreducible over K; denote this sum by $\mathcal{C}_0(f(x))$;

(3) A double sum $\sum_\beta \sum_\gamma (\gamma, \beta, 1)$, where $\sum_\beta$ over the roots β of monic polynomial $g \in K[y]$ irreducible over K, with $\sum_\gamma$ taken over the roots γ of some monic polynomial $h_\beta \in K(\beta)[x]$ irreducible over $K(\beta)$.

Then can write h_β as $h(x, \beta) \in K[x, y]$, where β-degree of $h <$ degree of g; denote double sum by $\mathcal{C}_1(h(x, y), g(y))$.

Example. Take

$$\begin{aligned} A(x,y,z) &= y^2z - x^3 \\ B(x,y,z) &= y^2z - x^2(x+z). \end{aligned}$$

Applying Euclid's algorithm to A and B as polynomials in x, we first have

$$A(x,y,z) = B(x,y,z) + x^2z,$$

so that

$$A \cdot B = A \cdot (x^2z) = 2(A \cdot x) + A \cdot z.$$

Then

$$A{\cdot}x = (y^2z){\cdot}x = 2(y{\cdot}x) + z{\cdot}x = 2(0,0,1) + (0,1,0)$$

while

$$A \cdot z = (x^3) \cdot z = 3(0,1,0).$$

So

$$A \cdot B = 4(0,0,1) + 5(0,1,0).$$

Example 2.

$$\begin{aligned} A(x,y,z) &= (y-z)x^5 + (y^2-yz)x^4 \\ &\quad +(y^3-y^2z)x^3 + (-y^2z^2+yz^3)x^2 \\ &\quad +(-y^3z^2+y^2z^3)x - y^4z^2 + y^3z^3 \\ B(x,y,z) &= (y^2-2z^2)x^2 + (y^3-2yz^2)x \\ &\quad +y^4 - y^2z^2 - 2z^4. \end{aligned}$$

Applying one step of Euclid's algorithm to A and B as polynomials in x, we get

$$A = \frac{(y-z)x(x^2-z^2)}{y^2-2z^2}B + z^2(y-z)(z^2x-y^3);$$

thus clearing the denominator y^2-2z^2 gives

$$\begin{aligned} (y^2-2z^2)A &= (y-z)x(x^2-z^2)B \\ &\quad + (y^2-2z^2)z^2(y-z)(z^2x-y^3). \end{aligned}$$

Get

$$\begin{aligned} A{\cdot}B &= 2(1,0,0) + 2\mathcal{C}_0(x^2+x+1) \\ &\quad + \mathcal{C}_1(x^2+x+2, y-1) + \mathcal{C}_1(x+y, y^2+1) \\ &\quad + \mathcal{C}_1(x-y^3, y^4+1) + \mathcal{C}_1(x^3-y, y^2-2) \\ &\quad + \mathcal{C}_1(x^2+yx+2, y^2-2). \end{aligned}$$

Once this final form has been obtained, the Galois cycles can be unpacked to write them explicitly as sums of points. For instance,

$$\mathcal{C}_0(x^2+x+1) = (\omega,1,0) + (\omega^2,1,0)$$

where $\omega = \frac{-1+\sqrt{-3}}{2}$,

$$\begin{aligned} \mathcal{C}_1(x^3-y, y^2-2) &= (\gamma,\gamma^3,1) + (\omega\gamma,\gamma^3,1) \\ &\quad + (\omega^2\gamma,\gamma^3,1) + (-\gamma,-\gamma^3,1) \\ &\quad + (-\omega\gamma,-\gamma^3,1) + (-\omega^2\gamma,-\gamma^3,1), \end{aligned}$$

where $\gamma = 2^{1/6}$.

Theorem 2 (Bézout's Theorem)**.** *Let $A, B \in K[x, y, z]$ be homogeneous of degrees m, n respectively, with no nonconstant common factor. Then in $\overline{K}\mathbb{P}^2$ the curves $A = 0$ and $B = 0$ intersect in exactly mn points, counting multiplicities.*

Proof of Bézout's Theorem

We need to show that $\#(A \cdot B) = \sum_{\mathbf{P}} i_{\mathbf{P}}(A, B) = mn$. We proceed by induction on the x-degree of B.

Base case. First suppose that B has x-degree 0. Then B factors over $\overline{K}$ into a product of n lines L, so that $A \cdot B$ is a sum of n intersection cycles $A \cdot L$. Each $A \cdot L = A' \cdot L$, where $A' =$ degree m polynomial in two variables , so a product of m lines. Hence $A \cdot L$ can be written as a sum of m intersections $L' \cdot L$, giving mn such intersections in total. Since, by Proposition , $L' \cdot L$ consists of a single point, we have $\#(A \cdot B) = mn$ in this case.

Induction step. Suppose now that B has x-degree $k > 0$ and that we know that the result holds for all B with $\partial_x B < k$ and for all A. Then

$$\begin{aligned}\#(A \cdot B) &= \#(R' \cdot B') - \#(H' \cdot B') \\ &\qquad + \#(A \cdot G) \\ &= (\partial R' - \partial H')\partial B' + \partial A \partial G,\end{aligned}$$

recalling that $\partial_x R' < \partial_x B = k$ and $\partial_x H' = \partial_x G = 0$.

By homogeneity, we have that $\partial R' - \partial H' = \partial A$. Finally, since $\partial B' + \partial G = \partial B$ from $B = B'G$, the result $\#(A \cdot B) = \partial A \, \partial B = mn$ follows for $\partial_x B = k$.

Define the *local ring of rational functions of degree* 0 at $\mathbf{P} \in \overline{K}\mathbb{P}^2$ to be

$$R_{\mathbf{P}} = \left\{ \frac{S}{T} : S, T \in \overline{K}[x, y, z], \partial S = \partial T, \right.$$
$$\left. T(\mathbf{P}) \neq 0 \right\},$$

$$(A, B)_{\mathbf{P}} = \left\{ \frac{S}{T} \in R_{\mathbf{P}} : S = MA + NB, \right.$$
$$\left. M, N, T \in \overline{K}[x, y, z], T(\mathbf{P}) \neq 0 \right\},$$

the ideal generated by A and B in $R_{\mathbf{P}}$.

Following e.g. Fulton, we can now define the intersection multiplicity $i_{\mathbf{P}}(A, B)$ of A and B to be the dimension of the $\overline{K}$-vector space $R_{\mathbf{P}}/(A, B)_{\mathbf{P}}$ (and so equal to 0 if $(A, B)_{\mathbf{P}} = R_{\mathbf{P}}$).

Lemma 3. *Let* $\mathbf{P} \in \overline{K}\mathbb{P}^2$ *and* $A, B, C \in K[x, y, z]$ *with* $\gcd(A, B) = \gcd(A, C) = 1$. *Then*

(a) $i_{\mathbf{P}}(A, B) > 0$ *if and only if* $\mathbf{P}$ *lies on both* A *and* B*;*

(b) $i_{\mathbf{P}}(A, B) = i_{\mathbf{P}}(B, A)$*;*

(c) $i_{\mathbf{P}}(A, BC) = i_{\mathbf{P}}(A, B) + i_{\mathbf{P}}(A, C)$*;*

(d) $i_{\mathbf{P}}(A, B+AC) = i_{\mathbf{P}}(A, B)$ *if* $\partial(AC) = \partial B$*;*

(e) *For distinct lines* L, L', *the only point on both lines is* $\mathbf{P}_\times$ *given by (1), and* $i_{\mathbf{P}_\times}(L, L') = 1$.

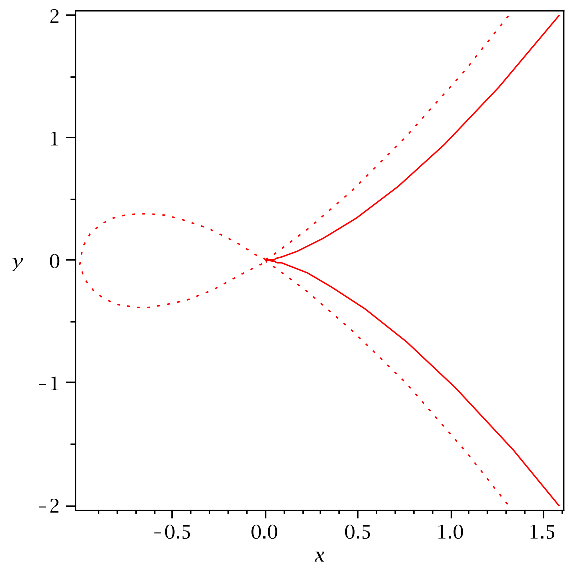

Figure 1: The 'slice' $z = 1$ of the cubic curves $y^2z - x^3$ (solid line) and $y^2z - x^2(x + z)$ (dotted line) near $(0, 0, 1)$, an intersection point of multiplicity 4. (These are the curves $y^2 = x^3$ and $y^2 = x^2(x + 1)$.)

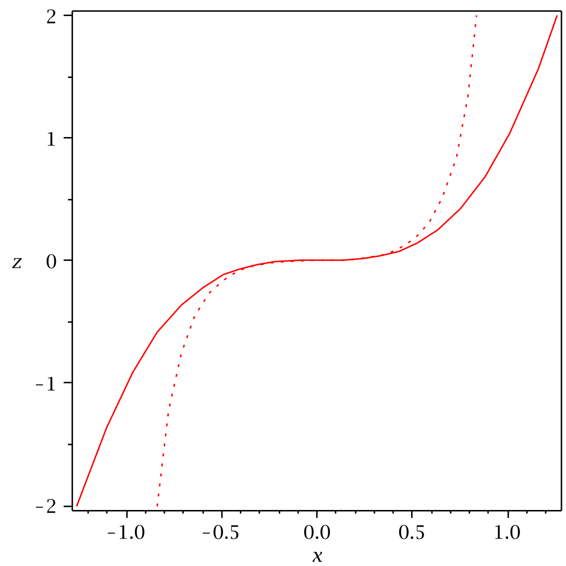

Figure 2: The 'slice' $y = 1$ of the same curves $y^2z - x^3$ (solid line) and $y^2z - x^2(x + z)$ (dotted line) near $(0, 1, 0)$, an intersection point of multiplicity 5. (These are the curves $z = x^3$ and $z = x^3/(1 - x^2)$.)