Curves in $\mathbb{P}^2$ and Bezout's Theorem

Peter Hawthorne

October 20, 2003

1 Introduction

In this paper we introduce projective geometry and one of its important theorems. We begin by defining projective space in terms of homogenous coordinates. Next, we define homgenous curves, and describe a few important properties they have. We then introduce Bezout's Theorem, which asserts that the number of intersection points of two homogenous curves is less than or equal to the product of their degrees. We conclude by proving the theorem, assuming several results about intersection multiplicities.

2 Projective Spaces

We begin by defining $\mathbb{P}^n$, the n-dimensional projective space. We define an equivalence relation $\sim$ on the non-zero points of $\mathbb{R}^{n+1}$ such that given $p_1 = [x_1, x_2, \ldots, x_{n+1}]$ and $p_2 = [x'_1, x'_2, \ldots, x'_{n+1}]$, $p_1 \sim p_2$ if and only if there exists $r \in \mathbb{R}$, $r \neq 0$, such that $p_1 = rp_2$. For each equivalence class, the coordinates of any one of the included points are said to be homogeneous coordinates. We can see that each of these equivalence classes corresponds to a line in $\mathbb{R}^{n+1}$, so there is a mapping from 1-dimensional subspaces in $\mathbb{R}^{n+1}$ to points of $\mathbb{P}^n$. Similarly, we may map planes in $\mathbb{R}^{n+1}$ to lines of $\mathbb{P}^n$.

An alternative way to look at $\mathbb{P}^2$ is as $\mathbb{A}^2 \cup \mathbb{P}^1$, where $\mathbb{P}^1$ is the set of equivalence classes of non-zero points in $\mathbb{A}^2$. We can think of these equivalence classes as corresponding to the "directions" in $\mathbb{A}^2$. This can be made more clear by noting that any lines with the same slope will all intersect at the same point at infinity.

It is straightforward to define curves in $\mathbb{P}^2$. We say that a C is a homogenous curve in $\mathbb{P}^2$ if it is the set of solutions of $F(X, Y, Z) = 0$, where F is a polynomial that satisfies $F(tX, tY, tZ) = t^d F(tX, tY, tZ)$ for some d.

Given any affine curve $f(x, y) = \sum_{i,j} a_{ij} x^i y^j$, we can extend it to a projective curve. Let $d = \deg(f)$. Then $F = \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}$. This ensures that our extended curve will be homogenous.

It is possible, using our description of $\mathbb{P}^2$ as $\mathbb{A}^2 \cup \mathbb{P}^1$, to define the affine part of a given curve. We let $f(x, y) = F(X, Y, 1)$ be this function. This includes all the points on the curve with non-zero Z-coordinates. The points on C with $Z = 0$ end up as points at infinity. We may think of this mapping as intersecting the lines in $\mathbb{R}^3$ with the plane $Z = 1$. Any horizontal line maps to a point at infinity, while the $X - Y$ plane is mapped to the line at infinity. It is of course possible to perform this intersection with any plane in $\mathbb{R}^3$ not passing through the origin, allowing us to map different parts of the projective curve to infinity. Easy cases are mapping onto $X = 1$ or $Z = 1$, but even the more complicated projections simply require us to use linear transformations of the projective coordinates. [2]

Given any projective curve $C : F(X, Y, Z) = 0$, we may write it as the product $F(X, Y, Z) = F_1(X, Y, Z) \cdots F_m(X, Y, Z)$, where each of the F_i is an irreducible projective polynomial. We call each of the F_i a component of C. We will be interested in pairs of curves C_1 and C_2 that have distinct sets of components; that is, such that if $f_i(x, y)$ is a component of C_1, it is not a component of C_2, and vice versa. We will say that such curves have no common component.

3 Intersections

The axiomatic description of $\mathbb{P}^n$ differs from the axiomatic description of $\mathbb{R}^n$ in one respect - there are no parallel lines: every pair of distinct lines shares an intersection point. A similar property holds when we look at curves of higher degree. Bezout's theorem, which will be presented in the next section, shows that the number of intersection points of two projective curves is related to the product of the degrees of the intersecting curves, a remarkable result with many interesting consequences. This section will introduce a few of the notions we will need to introduce and prove this theorem.

First of all, we will look only at curves that have no common components. It is easy to see that curves with a shared component have infinitely many intersection points. The converse of this statement is also true:

Proposition 3.1. *If C_1 and C_2 are projective curves with no common components, then $C_1 \cap C_2$ is a finite set.*

Proof. We need one result that will be assumed both here and below:

$$\#(C_1 \cap C_2 \cap \mathbb{A}^2) \leq n_1 n_2.$$

We choose some line l_1 that is not a component of C_1 or C_2, and map it to the line at infinity. By the assumed inequality, this means that $\#(C_1 \cap C_2 \cap l_1^C)$ is finite. Now choose another line l_2 also not a component of C_1 or C_2. Now $l_1 \cap l_2$ is a single point, and we have as before that $\#(C_1 \cap C_2 \cap l_2^C)$ is finite. So

$$\#(C_1 \cap C_2) \leq \#(C_1 \cap C_2 \cap l_1^C) + \#(C_1 \cap C_2 \cap l_2^C) + 1,$$

which is finite. □

For the rest of this discussion, let C_1 and C_2 be projective curves with no common components, with $C_1 : F_1(X, Y, Z) = 0$ and $C_2 : F_2(X, Y, Z) = 0$. We will also require that they are curves over k, where k is any algebraically closed field. If k is not algebraically closed, Bezout's Theorem will not hold. For example, consider the unit circle $x^2 + y^2 - 1 = 0$ and the line $x - 2 = 0$ in $\mathbb{R}^2$. It is clear that these do not intersect. We can homogenize each, giving $X^2 + Y^2 - Z^2 = 0$ and $X - 2Z = 0$. Substituting $X = 2Z$ into the first equation gives $3Z^2 + Y^2 = 0$, which has no non-zero real solutions. Therefore, these curves don't intersect in the real projective plane either. Viewed as curves in $\mathbb{C}^2$, however, they intersect at $(2, i\sqrt{3})$ and $(2, -i\sqrt{3})$.

Now, let us make a few necessary definitions:

Definition 3.2 (Local Ring). Let $P \in \mathbb{P}^2$ be a projective point. Then we define the local ring $\mathcal{O}_P$ of P to be the set of functions $\varphi \in k(x, y)$ which are defined at P. That is, $\mathcal{O}_P$ is the set of rational functions in x and y with a non-zero denominator at P. Note that $\mathcal{O}_P$ is a subring of $k(x, y)$.

Now, we will denote by $(f_1, f_2)_P$ the ideal $\mathcal{O}_P f_1 + \mathcal{O}_P f_2$, and by M_P the set $\{\phi \in \mathcal{O}_P : \phi(P) = 0\}$.

Definition 3.3 (Intersection Multiplicity in $\mathbb{A}_2$). Let C_1 and C_2 be curves in the affine plane with no common components. We define the intersection multiplicity at a point $P \in (C_1 \cap C_2)$ by:

$$I(P, C_1 \cap C_2) = \dim \left(\frac{\mathcal{O}_P}{(f_1, f_2)_P} \right)$$

We will now state a few facts about $I(P, C_1 \cap C_2)$.

Proposition 3.4. *If $P \notin C_1 \cap C_2$, then $I(P, C_1 \cap C_2) = 0$. If $P \in C_1 \cap C_2$, then $I(P, C_1 \cap C_2) = 1 + \dim \left(\frac{M_P}{(f_1, f_2)_P} \right)$.*

Proof. To prove the first part of the proposition, we need only show that $1 \in (f_1, f_2)_P$. By hypothesis, either f_1 or $f_2 \neq 0$ at P, say f_1. But this means that $f_1^{-1} \in \mathcal{O}_P$, so that $f_1 f_1^{-1} = 1 \in (f_1, f_2)_P$, as desired.

To prove the second statement, we must first note that $\mathcal{O}_P = k + M_P$. Moreover, given $P \in C_1 \cap C_2$, we have $(f_1, f_2)_P \subset M_P$. This follows immediately from the fact that $f_1(P) = f_2(P) = 0$. We now proceed:

$$\begin{aligned} I(P, C_1 \cap C_2) &= \dim \left(\frac{\mathcal{O}_P}{(f_1, f_2)_P} \right) \\ &= \dim \left(\frac{k + M_P}{(f_1, f_2)_P} \right) \\ &= \dim \left(\frac{k}{(f_1, f_2)_P} \right) + \dim \left(\frac{M_P}{(f_1, f_2)_P} \right). \end{aligned}$$

But, $\dim \left(\frac{k}{(f_1, f_2)_P} \right) = 1$, so we are done.

□

We can also define interesection multiplicity over homogeneous coordinates, although we will not do so explicitly here. This definition is equivalent to the given definition on the affine plane. Furthermore, it is invariant under projective transformations.[3][pp. 248–249]

4 Bezout's Theorem

Now that we have defined intersection multiplicities, we can give the full statement of Bezout's Theorem:

Theorem 4.1 (Bezout's Theorem). *Let C_1 and C_2 be projective curves with no common components, and $I(P, C_1 \cap C_2)$ the intersection mulitiplicity of point $P \in C_1 \cap C_2$. Then*

$$\sum_{P \in C_1 \cap C_2} I(P, C_1 \cap C_2) = (\deg C_1)(\deg C_2).$$

An elementary proof of this theorem is possible, but quite lengthy. The rest of this section will present an outline of the proof, and the details of several important steps. Our proof follows the outline presented in [3][pp. 242–251], filling in many of the details left as exercises there.

We have already mentioned in Section 3 how we can apply a projective transformation so that any finite set of points in $\mathbb{P}^2$ will lie in the affine plane. Combined with the facts that $C_1 \cap C_2$ is finite, and that intersection multiplicites are invariant under projective transformations, this means that we need only consider the case where all of the intersection points line in the affine plane.

Proof. The proof proceeds by first showing that

$$\#(C_1 \cap C_2 \cap \mathbb{A}^2) \leq \dim\left(\frac{R}{(f_1, f_2)}\right) \leq n_1 n_2.$$

In a complete proof, we would also show that $\dim\left(\frac{R}{(f_1,f_2)}\right) = n_1 n_2$ in the case that none of the elements of $C_1 \cap C_2$ lie at infinity. In this presentation, however, these steps of the proof will be taken as given, and we will only present the details of the rest of the proof.

We first wish to show that

$$\sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(P, C_1 \cap C_2) \leq \dim\left(\frac{R}{(f_1, f_2)_P}\right)$$

We then show that this is an equality, giving us Bezout's Theorem in the case where none of the intersection points lie at infinity. We then explain how to obtain the general result.

To begin, we claim $\dim(\frac{\mathcal{O}_P}{(f_1,f_2)_P}) \leq \dim(\frac{R}{(f_1,f_2)_P})$. First, we observe that given any set of functions $\phi_1, \phi_2, \ldots, \phi_m \in \mathcal{O}_P$, we can write each as $\frac{g_i}{h}$, that is, with a common denominator. Now, let $\frac{g_1}{h}, \frac{g_2}{h}, \ldots, \frac{g_m}{h} \in \mathcal{O}_P$ be a set of functions that are linearly independent modulo $(f_1, f_2)_P$. We claim that $g_1, g_2, \ldots, g_m$ are linearly independent modulo (f_1, f_2). If not, then there exist functions $\alpha_1, \alpha_2, \ldots, \alpha_m \neq 0$ such that

$$\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_m g_m = 0 \pmod{(f_1, f_2)},$$

with each of the $\alpha_i \in \mathcal{O}_P$. But then we have $\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_m g_m \in (f_1, f_2)$, so we can write $\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_m g_m = \beta_1 f_1 + \beta_2 f_2$.

Then, $\frac{\alpha_i g_i}{h} \in \mathcal{O}_P$, giving $\frac{\alpha_1 g_1}{h} + \cdots + \frac{\alpha_m g_m}{h} \in \mathcal{O}_P$. But this is just equal to

$$\frac{\alpha_1 g_1 + \cdots + \alpha_m g_m}{h} = \frac{\beta_1 f_1 + \beta_2 f_2}{h} = \frac{\beta_1}{h} f_1 + \frac{\beta_2}{h} f_2$$

Since $h \neq 0$ at P, we have $\frac{\beta_1}{h}, \frac{\beta_2}{h} \in \mathcal{O}_P$, so that $\frac{\alpha_1 g_1 + \cdots + \alpha_m g_m}{h} \in (f_1, f_2)_P$. But this imples that $\frac{\alpha_1 g_1 + \cdots + \alpha_m g_m}{h} = 0 \pmod{(f_1, f_2)_P}$, which contradicts our assumption that the $\frac{g_i}{h}$ were linearly independent. Therefore it must be the case that $g_1, \ldots, g_m$ are linearly independent modulo (f_1, f_2).

We continue by showing that given $P \in C_1 \cap C_2$, and $r \geq \dim\left(\frac{\mathcal{O}_P}{(f_1,f_2)}\right)$, $M_P^r \subset (f_1, f_2)_P$. Let $t_1, t_2, \ldots, t_r \in M_P$. Now, let $J_i \subset \mathcal{O}_P$ be a sequence of ideals with $J_i = t_1 t_2 \cdots t_i \mathcal{O}_P + (f_1, f_2)_P$ for $1 \leq i \leq r$, and $J_{r+1} = (f_1, f_2)$. Now, we note that for any i, $J_i \supset J_{i+1}$. Furthermore, for any i, we have $M_P \supset J_i \supset (f_1, f_2)_P$. Since $r \geq \dim\left(\frac{\mathcal{O}_P}{(f_1,f_2)}\right)$, we know that $J_i = J_{i+1}$ for some i. If this i equals r, then we have $t_1 \cdots t_r \in (f_1, f_2)_P$, as desired. If not, then for some i, we have $t_1 \cdots t_i \in J_{i+1}$. This gives

$$t_1 t_2 \cdots t_i = t_1 t_2 \cdots t_{i+1} \phi + \psi$$

where $\phi \in \mathcal{O}_P$, and $\psi \in (f_1, f_2)_P$. This gives $t_1 t_2 \cdots t_i (1 - t_{i+1}\phi) = \psi$. Note that $(1 - t_{i+1}\phi) = 1$, since $t_{i+1} \in M_P$. This means that $(1 - t_{i+1}\phi)^{-1} \in \mathcal{O}_P$, so we have $t_1 \cdots t_i = \psi(1 - t_{i+1}\phi)^{-1}$. Thus, we may rewrite:

$$t_1 \cdots t_r = t_{i+1} \cdots t_r \psi (1 - t_{i+1}\phi)^{-1}.$$

Since $\psi \in (f_1, f_2)_P$, and each of the $t_j \in \mathcal{O}_P$, this product is in $(f_1, f_2)_P$, as desired. This proves the second case.

Next, we show that given $P \in C_1 \cap C_2 \cap \mathbb{A}^2, \phi \in \mathcal{O}_P$, there exists $g \in R$ so that

$$g \equiv \phi \pmod{(f_1, f_2)_P} \quad \text{and}$$

$$g \equiv 0 \pmod{(f_1, f_2)_Q} \text{ for all } Q \neq P, Q \in C_1 \cap C_2 \cap \mathbb{A}^2.$$

To show this, we use the following fact: For any finite set of points $p_1, \ldots, p_n \in \mathbb{A}^2$, there exists a set of functions $g_1, g_2, \ldots, g_n$ such that each g_i has the property that $g_i(p_i) = 1$, and $g_i(p_j) = 0$ for $j \neq i$. The inequalitites we assumed at the beginning of the proof tell us that $C_1 \cap C_2 \cap \mathbb{A}^2$ is finite, so the fact applies. So take P as given. Then there exists a function $h \in R$ such that $h(P) = 1$, and $h(Q) = 0$ for $Q \neq P, Q \in C_1 \cap C_2 \cap \mathbb{A}^2$. Note that for any Q, we have $h \in M_Q$. By the previous result, there is some r such that for any Q, we have $h^r \in (f_1, f_2)_Q$. Furthermore, since $h(P) \neq 0, h^{-1} \in \mathcal{O}_P$, so that $\phi h^{-r} \in \mathcal{O}_P$. We showed above that $\mathcal{O}_P/(f_1, f_2)_P \cong R$, so there exists $f \in R$ such that $f \equiv \phi h^{-r} \pmod{(f_1, f_2)_P}$. Now consider $g = fh^r$. We have

$$g \equiv \phi h^r h^{-r} \equiv \phi \pmod{(f_1, f_2)_P}.$$

Finally, for any Q, we have $f \in (f_1, f_2)_Q$ and $h^r \in (f_1, f_2)_Q$, so that

$$g \equiv 0 \pmod{(f_1, f_2)_Q},$$

as desired.

Now, in order to prove the desired inequality, we must show that the map given by

$$R \to \prod_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} \frac{\mathcal{O}_P}{(f_1, f_2)_P}$$

$$f \mapsto (\cdots, f \pmod{(f_1, f_2)_P}, \cdots)_{P \in C_1 \cap C_2 \cap \mathbb{A}^2}$$

is surjective. This map sends a function $f \in R$ into a product space with dimension $\#(C_1 \cap C_2 \cap \mathbb{A}^2)$. Now, say that $(C_1 \cap C_2 \cap \mathbb{A}^2) = (P_1, \ldots, P_m)$, and let $(\phi_1, \ldots, \phi_m)$ be an element of the target space. Then the result just proven asserts that there exist $g_1, \ldots, g_m \in R$ such that $g_i \equiv \phi_i \pmod{(f_1, f_2)_{P_i}}$. Now consider the polynomial $g = \sum_{i=1}^m g_i$. The image of g under the map will be $(\phi_1, \ldots, \phi_m)$, as desired.

Let J be the kernel of this map. We can see that

$$\dim \frac{R}{J} = \sum_P \dim \left(\frac{\mathcal{O}_P}{(f_1, f_2)_P} \right) = \sum_P I(P, C_1 \cap C_2).$$

If we can show that $J = (f_1, f_2)$, then this will give us the desired equality. It is clear that $(f_1, f_2) \subset J$, and so we will prove the other direction.To that end, let $f \in J$. We will consider the set $L_f = \{g \in R : gf \in (f_1, f_2)\}$, showing that L_f is the unit ideal. It is clear that L_f is an ideal in R, and that $(f_1, f_2) \subset R$. We now claim that for every $P \in \mathbb{A}^2$, there exists $g \in L_f$ such that $g(P) \neq 0$. There are two cases to condsider. First, assume that $p \in C_1 \cap C_2 \cap \mathbb{A}^2$. The function f has the property that $f \in (f_1, f_2)_P$ for this P. Then $f = \alpha_1 f_1 + \alpha_2 f_2$, where $\alpha_1, \alpha_2 \in \mathcal{O}_P$. We can write α_1 and α_2 over a common denominator: $\alpha_1 = \beta_1/g, \alpha_2 = \beta_2/g$. Then

$$gf = \beta_1 f_1 + \beta_2 f_2, \quad \text{where } \beta_1, \beta_2 \in R \text{ and } g(P) \neq 0.$$

Therefore, we have g as desired. Now assume that $P \notin C_1 \cap C_2 \cap \mathbb{A}^2$. Then either $f_1(P) \neq 0$ or $f_2(P) \neq 0$. Let g be whichever is non-zero.

We now assume that L_f is not the unit ideal; that is, $1 \notin L_f$. Note that since $(f_1, f_2) \subset L_f$, we know that $\dim(R/L_f)$ is finite. Because of this, we know that it cannot be the case that all powers of $x \in R$ are linearly independent modulo L_f. Therefore there exist $c_i \in k$ and $n \in \mathbb{Z}$ such that $x^n + c_1 x^{n-1} + \cdots + c_n \in L$. Recall that k is algebraically closed. This means we can rewrite this sum as the product

$$\prod_{i=1}^n (x - a_i) \quad \text{for some } a_i \in k$$

Now, let us assume that $1 \in L + R(x - a_i)$ for all $1 \leq i \leq n$. Then for each i, we have $1 = g_i + r_i(x - a_i)$, with $g_i \in L_f$ and $r_i \in R$. So, we have

$$\left(\frac{1 - g_1}{r_1}\right)\left(\frac{1 - g_2}{r_2}\right)\cdots\left(\frac{1 - g_n}{r_n}\right) \in L_f.$$

Multiplying through by $r_1 r_2 \cdots r_n$ gives $(1 - g_1) \cdots (1 - g_n) \in L$. But this is equal to $1 + G$, where G is the sum of products of the g_i. We have $G \in L$, giving that $1 \in L$. But this contradicts our assumption that $1 \notin L$, so we conclude that there is an $a \in k$ such that $1 \notin L + R(x - a)$.

We can similarly prove the result that there exists $b \in k$ such that $1 \notin L + R(x - a) + R(y - b)$.

With the previous two results in hand, we let $P = (a, b)$, and show that $g(P) = 0$ for $g \in L$. Note that we may write $g(x, y)$ as $g(a+(x-a), b+(y-b))$. Since g is a polynomial, this is equivalent to

$$g(a, b) + g_1(x, y)(x - a) + g_2(x, y)(y - b)$$

for some $g_1, g_2 \in R$. But this lets us write

$$-g(a, b) = -g(x, y) + g_1(x, y)(x - a) + g_2(x, y)(y - b)$$

Note that the right-hand side is an element of $L + R(x - a) + R(y - b)$. Now, -g(a,b) is a constant, so $-g(a, b) \in k$. If $g(a, b) \neq 0$, we can divide through by $-g(a, b)$, and the right-hand side will still be in $L + R(x - a) + R(y - b)$. But the left-hand side will be 1, giving $1 \in L + R(x - a) + R(y - b)$, and contradicting the result just proven. This means that $g(a, b) = 0$, but this is another contradiction, since we had shown that for any P there must exist some $g \in L$ such that $g(P) \neq 0$.

We have therefore contradicted our hypothesis that $1 \notin L$, so we have $1 \in L$, as desired. This means that $J = (f_1, f_2)$. As we claimed, this shows that

$$\sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(P, C_1 \cap C_2) = \dim\left(\frac{R}{(f_1, f_2)}\right).$$

So long as all of the intersection points lie in the affine plane, we have proven Bezout's Theorem.

We now need the following result:

Proposition 4.2. *Given a finite set of points in $\mathbb{P}^2$, there is a line L not intersecting any of them.*

Proof. Say the proposition is not true. Then there exists a set $S = p_1, \ldots, p_n$ such that every line in $\mathbb{P}^2$ meets S. This means that one of the s_i is a solution to every equation $aX+bY+cZ+d = 0$ with $a, b, c, d \in k$. Now, given such an equation, say that $s_i = [X_i, Y_i, Z_i]$ is a root. Now, if we chose any other d', it must be the case that $aX_i+bY_i+cZ_i+d' \neq 0$. However, by assumption, there exists j such that s_j such that $aX_j + bY_j + cZ_j + d' = 0$. We can continue to choose $d'', \cdots, d^{(n-1)}$ in this manner. Now, if there were another $d^(n) \in k$ distinct from the chosen d's, we would contradict our assumption. So k must be finite. This contradicts the fact that an algebraically closed field is infinite. Therefore, there exists such L as claimed. □

However, as mentioned in Section 3, the number of intersection points of two homogenous curves is finite. This means we can find a line L not meeting $C_1 \cap C_2$. We can then find a projective transformation T that carries this line to the line at infinity. This will mean that each of $C_1 \cap C_2$ will lie in the affine plane. Since the intersection multiplicities are invariant under T, we can easily reduce the general case to the case just proved.

□

5 Some Consequences

This theorem has many important consequences, which is not surprising, given the nature of the result. It leads to many geometric and analytic results. On the geometric side, we have the following results: [1][These results and more may be found in Chap. 6]

Proposition 5.1. *If any two projective curves of degree m intersect in $m(m+3)/2$ or more points, they are the same curve.*

Theorem 5.2. *Let C_1 and C_2 be homogenous curves of degree n that meet in exactly n^2 points. When exactly mn of these points lie on an irreducible curve C' of degree m, then the remaining $n(n-m)$ interesection points line on a curve C'' of order $m-n$.*

This allows us to prove many other results, such as Pascal's theorem:

Theorem 5.3. *Let C be an irreducible quadratic curve in $\mathbb{P}^2$. If H is a hexagon inscribed inside C, then the intersection points of the three pairs of opposite sides are collinear.*

On the analytic side, Bezout's Theorem allows us to construct the group operation on elliptic curves. Let E be an elliptic curve, p_1, p_2 two points on

E, and l the line through p_1 and p_2. Then we define $p_1 + p_2$ as the third intersection of l with E. Such a point is guaranteed to exist by Bezout's Theorem.

References

[1] Egbert Brieskorn and Horst Knörrer, *Plane algebraic curves*, Birkhäuser Verlag, Basel, 1986, Translated from the German by John Stillwell. MR 88a:14001

[2] Patrick J. Ryan, *Euclidean and non-Euclidean geometry*, Cambridge University Press, Cambridge, 1986, An analytical approach. MR 87i:51001

[3] Joseph H. Silverman and John Tate, *Rational points on elliptic curves*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1992. MR 93g:11003