Appendix A

Projective Geometry

In this appendix we summarize the basic properties of the projective plane and projective curves that are used elsewhere in this book. For further reading about projective algebraic geometry, the reader might profitably consult Brieskorn–Knörrer [8], Fulton [16], Harris [18], or Reid [37]. More high-powered accounts of modern algebraic geometry are given in Hartshorne [20] and Griffiths–Harris [17].

A.1 Homogeneous Coordinates and the Projective Plane

There are many ways to construct the projective plane. We describe two constructions, one algebraic and one geometric, since each in its own way provides enlightenment.

We begin with a famous problem from number theory, namely the solution of the equation

\[ x^N + y^N = 1 \]  
(Fermat Equation #1)

in rational numbers \( x \) and \( y \). Suppose that we have found a solution, say \( x = a/c \) and \( y = b/d \), where we write fractions in lowest terms and with positive denominators. Substituting and clearing denominators gives the equation

\[ a^N d^N + b^N c^N = c^N d^N. \]
It follows that \( c^N \mid a^N d^N \), but \( \gcd(a, c) = 1 \) by assumption, so we conclude that \( c^N \mid d^N \), and hence \( c \mid d \). Similarly \( d^N \mid b^N c^N \) and \( \gcd(b, d) = 1 \), which implies that \( d \mid c \). Therefore \( c = \pm d \), and since we’ve assumed that \( c \) and \( d \) are positive, we find that \( c = d \). Thus any solution to Fermat Equation #1 in rational numbers has the form \((a/c, b/c)\), and thus gives a solution in integers \((a, b, c)\) to the homogeneous equation

\[
X^N + Y^N = Z^N \quad \text{(Fermat Equation #2)}
\]

Conversely, any integer solution \((a, b, c)\) to the second Fermat equation with \( c \neq 0 \) gives a rational solution \((a/c, b/c)\) to the first. However, different integer solutions \((a, b, c)\) may lead to the same rational solution. For example, if \((a, b, c)\) is an integer solution to Fermat Equation #2, then for any integer \( t \), the triple \((ta, tb, tc)\) is also a solution, and clearly \((a, b, c)\) and \((ta, tb, tc)\) give the same rational solutions to Fermat Equation #1. The moral is that in solving Fermat Equation #2, we should really treat triples \((a, b, c)\) and \((ta, tb, tc)\) as being the same solution, at least for non-zero \( t \). This leads to the notion of homogeneous coordinates, which we describe in more detail later.

There is one more observation that we wish to make before leaving this example, namely the “problem” that Fermat Equation #2 may have some integer solutions that do not correspond to rational solutions of Fermat Equation #1. First, the point \((0, 0, 0)\) is always a solution of the second equation, but this solution is so trivial that we will just discard it. Second, and potentially more serious, is the fact that if \( N \) is odd, then Fermat Equation #2 has the solutions \((1, -1, 0)\) and \((-1, 1, 0)\) that do not give solutions to Fermat Equation #1. To see what is happening, suppose that we take a sequence of solutions

\[
(a_1, b_1, c_1), (a_2, b_2, c_2), (a_3, b_3, c_3), \ldots
\]

such that

\[
(a_i, b_i, c_i) \rightarrow (1, -1, 0) \quad \text{as} \quad i \rightarrow \infty.
\]

Of course, we cannot do this with integer solutions, so now we let the \( a_i, b_i, c_i \)'s be real numbers. The corresponding solutions to Fermat Equation #1 are \((a_i/c_i, b_i/c_i)\), and we see that these solutions approach \((\infty, \infty)\) as \((a_i, b_i, c_i) \rightarrow (1, -1, 0)\). In other words, the extra solutions \((1, -1, 0)\) and \((-1, 1, 0)\) to Fermat Equation #2 somehow correspond to solutions to Fermat Equation #1 that lie “at infinity.” As we will see, the theory of solutions to polynomial equations becomes neater and clearer if we treat these extra points “at infinity” just as we treat all other points.
We are now ready for our first definition of the projective plane, which is essentially an algebraic definition. We define the *projective plane* to be the set of triples \([a, b, c]\) with \(a, b, c\) not all zero, but we consider two triples \([a, b, c]\) and \([a', b', c']\) to be the same point if there is a non-zero \(t\) such that

\[
a = ta', \quad b = tb', \quad c = tc'.
\]

We denote the projective plane by \(\mathbb{P}^2\). In other words, we define an equivalence relation \(\sim\) on the set of triples \([a, b, c]\) by the rule

\[
[a, b, c] \sim [a', b', c'] \quad \text{if} \quad a = ta', b = tb', c = tc' \quad \text{for some non-zero} \quad t.
\]

Then \(\mathbb{P}^2\) is the set of equivalence classes of triples \([a, b, c]\), except that we exclude the triple \([0, 0, 0]\). Thus

\[
\mathbb{P}^2 = \left\{ [a, b, c] : a, b, c \text{ are not all zero} \right\} / \sim.
\]

The numbers \(a, b, c\) are called *homogeneous coordinates* for the point \([a, b, c]\) in \(\mathbb{P}^2\). More generally, for any integer \(n \geq 1\), we define *projective n-space* to be the set of equivalence classes of homogeneous \(n+1\)-tuples,

\[
\mathbb{P}^n = \left\{ [a_0, a_1, \ldots, a_n] : a_0, \ldots, a_n \text{ not all zero} \right\} / \sim,
\]

where

\[
[a_0, \ldots, a_n] \sim [a'_0, \ldots, a'_n] \quad \text{if} \quad a_0 = ta'_0, \ldots, a_n = ta'_n \quad \text{for some non-zero} \quad t.
\]

We eventually want to do geometry in projective space, so we need to define some geometric objects. In the next section we study quite general curves, but for the moment we are content to describe lines in \(\mathbb{P}^2\). We define a *line in \(\mathbb{P}^2\)* to be the set of points \([a, b, c] \in \mathbb{P}^2\) whose coordinates satisfy an equation of the form

\[
\alpha X + \beta Y + \gamma Z = 0
\]

for some constants \(\alpha, \beta, \gamma\) not all zero. Note that if \([a, b, c]\) satisfies such an equation, then so does \([ta, tb, tc]\) for any \(t\), so to check if a point of \(\mathbb{P}^2\) is on a given line, one can use any homogeneous coordinates for the point.

In order to motivate our second description of the projective plane, we consider a geometric question. It is well-known that two points in the usual \((x, y)\)-plane determine a unique line, namely the line that goes through them. Similarly, two lines in the plane determine a unique point, namely the point
where they intersect, unless the two lines happen to be parallel. From both an aesthetic and a practical viewpoint, it would be nice to provide these poor parallel lines with an intersection point of their own. Since the plane itself doesn’t contain the requisite points, we add on extra points by fiat. How many extra points do we need? For example, would it suffice to use one extra point \( P \) and decree that any two parallel lines intersect at \( P \)? The answer is no, and here’s why.

![Figure A.1: Parallel lines with intersection points “at infinity”](image)

Let \( L_1 \) and \( L_2 \) be parallel lines, and let \( P \) be the extra point where they intersect. Similarly, let \( L_1' \) and \( L_2' \) be parallel lines that intersect at the extra point \( P' \), as illustrated in Figure A.1. Suppose that \( L_1 \) and \( L_1' \) are not parallel. Then \( L_1 \) and \( L_1' \) already intersect at some ordinary point, say \( L_1 \cap L_1' = \{Q\} \). But two lines are allowed to have only one point in common, so it follows that the points \( P \in L_1 \) and \( P' \in L_1' \) must be distinct. So we really need to add an extra point for each distinct direction in the ordinary plane, and then we decree that a line \( L \) consists of its usual points together with the extra point determined by its direction.

This leads to our second definition of the projective plane, this time in purely geometric terms. For simplicity, we denote the usual Euclidean plane (also called the affine plane) by

\[
A^2 = \{(x, y): x \text{ and } y \text{ are numbers}\}. 
\]

Then we define the projective plane to be

\[
P^2 = A^2 \cup \{\text{the set of directions in } A^2\},
\]
where *direction* is a non-oriented notion. Two lines have the same direction if and only if they are parallel. Logically we could define a direction in this sense to be an equivalence class of parallel lines, that is, a direction is a collection of all lines parallel to a given line. The extra points in $\mathbb{P}^2$ associated to directions, that is the points in $\mathbb{P}^2$ that are not in $\mathbb{A}^2$, are often called *points at infinity*.

As indicated earlier, a line in $\mathbb{P}^2$ then consists of a line in $\mathbb{A}^2$ together with the point at infinity specified by its direction. The intersection of two parallel lines is the point at infinity corresponding to their common direction. Finally, the set of all points at infinity is itself considered to be a line, which we denote by $L_\infty$, and the intersection of any other line $L$ with $L_\infty$ is the point at infinity corresponding to the direction of $L$. With these conventions, it is easy to see that there is a unique line going through any two distinct points of $\mathbb{P}^2$, and further that any two distinct lines in $\mathbb{P}^2$ intersect in exactly one point. So the projective plane in this geometric incarnation eliminates the need to make a distinction between parallel and non-parallel lines. In fact, $\mathbb{P}^2$ has no parallel lines at all.

We now have two definitions of the projective plane, so it behooves us to show that they are equivalent. First we need a more analytic description of the set of directions in $\mathbb{A}^2$. One way to describe these directions is to use the set of lines in $\mathbb{A}^2$ that go through the origin, since every line in $\mathbb{A}^2$ is parallel to a unique line through the origin. Now the lines through the origin are given by equations $Ay = Bx$ with $A$ and $B$ not both zero. However, it is possible for two pairs to give the same line. More precisely, the pairs $(A, B)$ and $(A', B')$ give the same line if and only if there is a non-zero $t$ such that $A = tA'$ and $B = tB'$. Thus the set of directions in $\mathbb{A}^2$ is naturally described by the points $[A, B]$ of the projective line $\mathbb{P}^1$. This allows us to write our second description of $\mathbb{P}^2$ in the form

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \mathbb{P}^1.$$ 

A point $[A, B] \in \mathbb{P}^1 \subset \mathbb{P}^2$ corresponds to the direction of the line $Ay = Bx$.

How is this related to the definition of $\mathbb{P}^2$ in terms of homogeneous coordinates? Recall that in our original example we associated a point $(x, y) \in \mathbb{A}^2$ with the point $[x, y, 1] \in \mathbb{P}^2$, and similarly a point $[a, b, c] \in \mathbb{P}^2$ with $c \neq 0$ was associated to the point $(a/c, b/c) \in \mathbb{A}^2$. And the remaining points in $\mathbb{P}^2$, namely those with $c = 0$, just give a copy of $\mathbb{P}^1$. In other words, the maps given in Table A.1 show how to identify our two definitions of the projec-
tive plane. It is easy to check that these two maps are inverses. For example, if \( c \neq 0 \), then

\[
[a, b, c] \mapsto (a/c, b/c) \mapsto [a/c, b/c, 1] = [a, b, c].
\]

We leave the remaining verifications to you.

Each of our definitions of the projective plane came with a description of what constitutes a line, so we should also check that the lines match up properly. For example, a line \( L \) in \( \mathbb{P}^2 \) using homogeneous coordinates is the set of solutions \([a, b, c]\) to an equation

\[
\alpha X + \beta Y + \gamma Z = 0.
\]

Suppose first that \( \alpha \) and \( \beta \) are not both zero. Then any point \([a, b, c] \in L\) with \( c \neq 0 \) is sent to the point

\[
(a/c, b/c) \text{ on the line } \alpha x + \beta y + \gamma = 0 \text{ in } \mathbb{A}^2.
\]

And the point \([-\beta, \alpha, 0] \in L\) is sent to the point \([-\beta, \alpha] \in \mathbb{P}^1\), which corresponds to the direction of the line \(-\beta y = \alpha x\). This is exactly right, since the line \(-\beta y = \alpha x\) is precisely the line going through the origin that is parallel to the line \(\alpha x + \beta y + \gamma = 0\). This takes care of all lines except for the line \( Z = 0 \) in \( \mathbb{P}^2 \). But the line \( Z = 0 \) is sent to the line in \( \mathbb{A}^2 \cup \mathbb{P}^1 \) consisting of all of the points at infinity. So the lines in our two descriptions of \( \mathbb{P}^2 \) are consistent.
A.2 Curves in the Projective Plane

An algebraic curve in the affine plane $\mathbb{A}^2$ is defined to be the set of solutions to a polynomial equation in two variables

$$ f(x, y) = 0. $$

For example, the equation $x^2 + y^2 - 1 = 0$ is a circle in $\mathbb{A}^2$, and $2x - 3y^2 + 1 = 0$ is a parabola.

In order to define curves in the projective plane $\mathbb{P}^2$, we need to use polynomials in three variables, since points in $\mathbb{P}^2$ are represented by homogeneous triples. But there is the further difficulty that each point in $\mathbb{P}^2$ can be represented by many different homogeneous triples. It thus makes sense to look only at polynomials $F(X, Y, Z)$ with the property that if $F(a, b, c) = 0$, then $F(ta, tb, tc) = 0$ for all $t$. These turn out to be the homogeneous polynomials, and we use them to define curves in $\mathbb{P}^2$.

More formally, a polynomial $F(X, Y, Z)$ is called a homogeneous polynomial of degree $d$ if it satisfies the identity

$$ F(tX, tY, tZ) = t^d F(X, Y, Z). $$

This identity is equivalent to the statement that $F$ is a linear combination of monomials $X^i Y^j Z^k$ with $i + j + k = d$.

We define a projective curve $C$ in the projective plane $\mathbb{P}^2$ to be the set of solutions to a polynomial equation

$$ C : F(X, Y, Z) = 0, $$

where $F$ is a non-constant homogeneous polynomial. We also call $C$ an algebraic curve, or sometimes just a curve if it is clear that we are working in $\mathbb{P}^2$.

The degree of the curve $C$ is the degree of the polynomial $F$. For example,

$$ C_1 : X^2 + Y^2 - Z^2 = 0 \quad \text{and} \quad C_2 : Y^2 Z - X^3 - XZ^2 = 0 $$

are projective curves, where $C_1$ has degree 2 and $C_2$ has degree 3.

In order to check whether a point $P \in \mathbb{P}^2$ is on the curve $C$, we can take any homogeneous coordinates $[a, b, c]$ for $P$ and check whether $F(a, b, c) = 0$. This is true because any other homogeneous coordinates for $P$ look like $[ta, tb, tc]$ for some non-zero $t$. Then $F(a, b, c)$ and $F(ta, tb, tc) = t^d F(a, b, c)$ are either both zero or both non-zero.

This tells us what a projective curve is when we use the definition of $\mathbb{P}^2$ by homogeneous coordinates. It is very illuminating to relate this to the description of $\mathbb{P}^2$ as $\mathbb{A}^2 \cup \mathbb{P}^1$ where $\mathbb{A}^2$ is the usual affine plane, and the points at
infinity, i.e., the points in $\mathbb{P}^1$, correspond to the directions in $\mathbb{A}^2$. Let $C \subset \mathbb{P}^2$ be a curve given by a homogeneous polynomial of degree $d$,

$$C : F(X, Y, Z) = 0.$$ 

If $P = [a, b, c] \in C$ is a point of $C$ with $c \neq 0$, then according to the identification $\mathbb{P}^2 \leftrightarrow \mathbb{A}^2 \cup \mathbb{P}^1$ described in Table A.1 in Section A.1, the point $P \in C \subset \mathbb{P}^2$ corresponds to the point

$$\left(\frac{a}{c}, \frac{b}{c}\right) \in \mathbb{A}^2 \subset \mathbb{A}^2 \cup \mathbb{P}^1.$$ 

On the other hand, combining $F(a, b, c) = 0$ with the fact that $F$ is homogeneous of degree $d$ shows that

$$0 = \frac{1}{c^d} F(a, b, c) = F \left(\frac{a}{c}, \frac{b}{c}, 1\right).$$

In other words, if we define a new, non-homogeneous, polynomial $f(x, y)$ by the formula

$$f(x, y) = F(x, y, 1),$$

then we get a map

$$\{ [a, b, c] \in C : c \neq 0 \} \longrightarrow \{ (x, y) \in \mathbb{A}^2 : f(x, y) = 0 \},$$

$$[a, b, c] \longmapsto (a/c, b/c).$$

And it is easy to see that this map is one-to-one and onto, since if $(r, s) \in \mathbb{A}^2$ satisfies the equation $f(x, y) = 0$, then clearly $[r, s, 1] \in C$. We call the curve $f(x, y) = 0$ the affine part of the projective curve $C$.

It remains to look at the points $[a, b, c] \in C$ with $c = 0$ and describe them geometrically in terms of the affine part of $C$. The points $[a, b, 0]$ on $C$ satisfy the equation $F(X, Y, 0) = 0$, and they are sent to points at infinity $[a, b] \in \mathbb{P}^1$ in $\mathbb{A}^2 \cup \mathbb{P}^1$. We claim that these points, which recall are really directions in $\mathbb{A}^2$, correspond to the limiting tangent directions of the affine curve $f(x, y) = 0$ as we move along the affine curve out to infinity. In other words, and this is really the intuition to keep in mind, an affine curve $f(x, y)$ is somehow “missing” some points that lie out at infinity, and the points that are missing are the limiting directions as one moves along the curve out toward infinity.

Rather than giving a general proof we illustrate the idea with two examples. First we consider the line

$$L : \alpha X + \beta Y + \gamma Z = 0,$$
say with $\alpha \neq 0$. The affine part of $L$ is the line $L_0 : \alpha x + \beta y + 1 = 0$ in $\mathbb{A}^2$. The points at infinity on $L$ correspond to the points with $Z = 0$. There is only one such point, namely $[-\beta, \alpha, 0]$, which corresponds to the point at infinity $[-\beta, \alpha] \in \mathbb{P}^1$, which in turn corresponds to the direction $-\beta y = \alpha x$ in $\mathbb{A}^2$. This direction is exactly the direction of the line $L_0$. Thus $L$ consists of the affine line $L_0$, together with the single point at infinity corresponding to the direction of $L_0$.

Next we look at the projective curve

$$C : X^2 - Y^2 - Z^2 = 0.$$ 

There are two points on $C$ with $Z = 0$, namely $[1, 1, 0]$ and $[1, -1, 0]$. These two points correspond, respectively, to the points at infinity $[1, 1], [1, -1] \in \mathbb{P}^1$, or equivalently to the directions $y = x$ and $y = -x$ in $\mathbb{A}^2$. The affine part of $C$ is the hyperbola

$$C_0 : x^2 - y^2 - 1 = 0.$$ 

Suppose that we take a sequence of points $(r_1, s_1), (r_2, s_2), \ldots$ on $C_0$ such that these points tend toward infinity along one of the branches of the hyperbola. (Note that there are four choices of direction, since we can let $r_i \to \infty$ or $r_i \to -\infty$, and similarly $s_i \to \infty$ or $s_i \to -\infty$.) If we rewrite $r_i^2 - s_i^2 - 1 = 0$ as
\[
\left( \frac{r_i}{s_i} - 1 \right) \left( \frac{r_i}{s_i} + 1 \right) = \frac{1}{s_i^2},
\]
then the right-hand side goes to 0 as \( i \to \infty \). So we see that if we travel out to \( \infty \) along the hyperbola, then either
\[
\lim_{i \to \infty} \frac{r_i}{s_i} = 1 \quad \text{or} \quad \lim_{i \to \infty} \frac{r_i}{s_i} = -1,
\]
depending on which branch of the hyperbola we travel on; see Figure A.2.

Let \( L_i \) be the tangent line to \( C_0 \) at the point \((r_i, s_i)\). We claim that as \( i \to \infty \), the direction of the tangent line \( L_i \) approaches the direction of one of the lines \( y = \pm x \). This is nothing more than the assertion that the lines \( y = \pm x \) are asymptotes for the curve \( C_0 \). To check this assertion analytically, we implicitly differentiate the equation \( x^2 - y^2 - 1 = 0 \) to get
\[
\frac{dy}{dx} = \frac{x}{y},
\]
and hence
\[
\text{(slope of } L_i) = \text{(slope of } C_0 \text{ at } (r_i, s_i)) = \frac{r_i}{s_i} \xrightarrow{i \to \infty} \pm 1.
\]

The preceding discussion shows that if we start with a projective curve \( C : F(X, Y, Z) = 0 \), then we can write \( C \) as the union of its affine part \( C_0 \) and its points at infinity. Here \( C_0 \) is the affine curve given by the equation
\[
C_0 : f(x, y) = F(x, y, 1) = 0,
\]
and the points at infinity are the points with \( Z = 0 \), which correspond to the limiting directions of the tangent lines to \( C_0 \). The process of replacing the homogeneous polynomial \( F(X, Y, Z) \) by the inhomogeneous polynomial \( f(x, y) = F(x, y, 1) \) is called dehomogenization (with respect to the variable \( Z \)). We would now like to reverse this process.

Thus suppose that we begin with an affine curve \( C_0 \) given by an equation \( f(x, y) = 0 \). We want to find a projective curve \( C \) whose affine part is \( C_0 \), or equivalently, we want to find a homogeneous polynomial \( F(X, Y, Z) \) so that \( F(x, y, 1) = f(x, y) \). This is easy to do, although we want to be careful not to also include the line at infinity in our curve. If we write the polynomial \( f(x, y) \) as \( \sum a_{ij} x^i y^j \), then the degree of \( f \) is defined to be the largest value of \( i + j \) for which the coefficient \( a_{ij} \) is not zero. For example,
\[
\deg(x^2 + xy + x^2 y^2 + y^3) = 4 \quad \text{and} \quad \deg(y^2 - x^3 - ax^2 - bx - c) = 3.
\]
Then the homogenization of a polynomial \( f(x, y) = \sum a_{ij} x^i y^j \) of degree \( d \) is defined to be

\[
F(X, Y, Z) = \sum_{i,j} a_{ij} X^i Y^j Z^{d-i-j}.
\]

It is clear from this definition that \( F \) is homogeneous of degree \( d \) and that \( F(x, y, 1) = f(x, y) \). Further, our choice of \( d \) ensures that \( F(X, Y, 0) \) is not identically zero, so the curve defined by \( F(X, Y, Z) = 0 \) does not contain the entire line at infinity. Thus using homogenization and dehomogenization, we obtain a one-to-one correspondence between affine curves and projective curves that do not contain the line at infinity.

We should also mention that there is nothing sacred about the variable \( Z \). We could just as well dehomogenize a curve \( F(X, Y, Z) \) with respect to one of the other variables, say \( Y \), to get an affine curve \( F(x, 1, z) = 0 \) in the affine \( xz \)-plane. It is sometimes convenient to do this if we are especially interested in one of the points at infinity on the projective curve \( C \). In essence, what we are doing is taking a different line, in this case the line \( Y = 0 \), and making it into the “line at infinity.” An example should make this clearer. Suppose that we want to study the curve

\[
C : Y^2 Z - X^3 - Z^3 = 0 \quad \text{and the point} \quad P = [0, 1, 0] \in C.
\]

If we dehomogenize with respect to \( Z \), then the point \( P \) becomes a point at infinity on the affine curve \( y^2 - x^3 - 1 = 0 \). So instead we dehomogenize with respect to \( Y \), which means setting \( Y = 1 \). We then get the affine curve

\[
z - x^3 - z^3 = 0,
\]

and the point \( P \) becomes the point \( (x, z) = (0, 0) \). In general, by taking different lines to be the line at infinity, we can break a projective curve \( C \) up into a lot of overlapping affine parts, and then these affine parts can be “glued” together to form the entire projective curve.

Up to now we have been working with polynomials without worrying overmuch about what the coefficients of our polynomials look like, and similarly we’ve talked about solutions of polynomial equations without specifying what sorts of solutions we mean. Classical algebraic geometry is concerned with describing the complex solutions to systems of polynomial equations, but in studying number theory, we are more interested in finding solutions whose coordinates are in non-algebraically closed fields such as \( \mathbb{Q} \), or even in rings such as \( \mathbb{Z} \). That being the case, it makes sense to look at curves given by polynomial equations with rational or integer coefficients.
We call a curve \( C \) \textit{rational} if it is the set of zeros of a polynomial having rational coefficients.\(^1\) Note that the solutions of the equation \( F(X, Y, Z) = 0 \) and the equation \( cF(X, Y, Z) = 0 \) are the same for any non-zero \( c \). This allows us to clear the denominators of the coefficients, so a rational curve is in fact the set of zeros of a polynomial with integer coefficients. All of the examples given above are rational curves, since their equations have integer coefficients.

Let \( C \) be a projective curve that is rational, say \( C \) is given by an equation \( F(X, Y, Z) = 0 \) for a homogeneous polynomial \( F \) having rational coefficients. The set of rational points on \( C \), which we denote by \( C(\mathbb{Q}) \), is the set of points of \( C \) having rational coordinates, 

\[
C(\mathbb{Q}) = \{ [a, b, c] \in \mathbb{P}^2 : F(a, b, c) = 0 \text{ and } a, b, c \in \mathbb{Q} \}.
\]

Note that if \( P = [a, b, c] \) is in \( C(\mathbb{Q}) \), it is not necessary that \( a, b, c \) themselves be rational, since a point \( P \) has many different homogeneous coordinates. All that one can say is that \( [a, b, c] \in C \) is a rational point of \( C \) if and only if there is a non-zero number \( t \) so that \( ta, tb, tc \) are all in \( \mathbb{Q} \).

Similarly, if \( C_0 \) is an affine curve that is rational, say \( C_0 : f(x, y) = 0 \), then the set of rational points on \( C_0 \), denoted \( C_0(\mathbb{Q}) \), consists of all \( (r, s) \in C_0 \) with \( r, s \in \mathbb{Q} \). It is easy to see that if \( C_0 \) is the affine piece of a projective curve \( C \), then \( C(\mathbb{Q}) \) consists of \( C_0(\mathbb{Q}) \), together with those points at infinity that happen to be rational. Some of the most famous theorems in number theory involve the set of rational points \( C(\mathbb{Q}) \) on certain curves. For example, the \( N \)'th Fermat curve \( C_N \) is the projective curve 

\[
C_N : X^N + Y^N = Z^N,
\]

and Wiles’ theorem (Fermat’s last theorem) says that \( C_N(\mathbb{Q}) \) consists of only those points with one of \( X, Y, \) or \( Z \) equal to zero.

The theory of Diophantine equations also deals with integer solutions of polynomial equations. Let \( C_0 \) be an affine curve that is rational, say given by an equation \( f(x, y) = 0 \). We define the \textit{set of integer points of} \( C_0 \), which we denote \( C_0(\mathbb{Z}) \), to be the set of points of \( C_0 \) having integer coordinates,

\[
C_0(\mathbb{Z}) = \{ (r, s) \in \mathbb{A}^2 : f(r, s) = 0 \text{ and } r, s \in \mathbb{Z} \}.
\]

\(^1\)We must warn the reader than this terminology is non-standard. In the usual language of algebraic geometry, a curve is called rational if it is birationally isomorphic to the projective line \( \mathbb{P}^1 \), and a curve given by polynomials with rational coefficients is said to be defined over \( \mathbb{Q} \).
Why do we only talk about integer points on affine curves and not on projective curves? The answer is that for a projective curve, the notions of integer point and rational point coincide. Here we might say that a point \([a, b, c] \in \mathbb{P}^2\) is an integer point if its coordinates are integers. But if \(P \in \mathbb{P}^2\) is any point that is given by homogeneous coordinates \(P = [a, b, c]\) that are rational, then we can find an integer \(t\) to clear the denominators of \(a, b, c\), and so \(P = [ta, tb, tc]\) also has homogeneous coordinates that are integers. So for a projective curve \(C\) we would have \(C(\mathbb{Q}) = C(\mathbb{Z})\).

It is also possible to look at polynomial equations and their solutions in rings and fields other than \(\mathbb{Z}\) or \(\mathbb{Q}\) or \(\mathbb{R}\) or \(\mathbb{C}\). For example, one might look at polynomials with coefficients in the finite field \(\mathbb{F}_p\) with \(p\) elements and ask for solutions whose coordinates are also in the field \(\mathbb{F}_p\). You may worry about your geometric intuitions in situations like this. How can one visualize points and curves and directions in \(\mathbb{A}^2\) when the points of \(\mathbb{A}^2\) are pairs \((x, y)\) with \(x, y \in \mathbb{F}_p\)? There are two answers to this question. The first and most reassuring is that you can continue to think of the usual Euclidean plane, i.e., \(\mathbb{R}^2\), and most of your geometric intuitions concerning points and curves will still be true when you switch to coordinates in \(\mathbb{F}_p\). The second and more practical answer is that the affine and projective planes and affine and projective curves are defined algebraically in terms of ordered pairs \((r, s)\) or homogeneous triples \([a, b, c]\) without any reference to geometry. So in proving things one can work algebraically using coordinates, without worrying at all about geometric intuitions. We might summarize this general philosophy as:

**Think Geometrically, Prove Algebraically**

One of the fundamental questions answered by the differential calculus is that of finding the tangent line to a curve. If \(C : f(x, y) = 0\) is an affine curve, then implicit differentiation gives the relation

\[
\frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} \frac{dy}{dx} = 0.
\]

So if \(P = (r, s)\) is a point on \(C\), the tangent line to \(C\) at \(P\) is given by the equation

\[
\frac{\partial f}{\partial x}(r, s)(x - r) + \frac{\partial f}{\partial y}(r, s)(y - s) = 0.
\]

This is the answer provided by elementary calculus. But we clearly have a problem if both partial derivatives are 0. For example, this happens for each of the curves

\[C_1 : y^2 = x^3 + x^2 \quad \text{and} \quad C_2 : y^2 = x^3\]
at the point $P = (0, 0)$. If we sketch these curves, we see that they look at bit strange at $P$; see Figures 1.13 and 1.15 in Section 1.3. The curve $C_1$ crosses over itself at $P$, so it has two distinct tangent directions there. The curve $C_2$, on the other hand, has a cusp at $P$, which means that it comes to a sharp point at $P$. We say that $P$ is a \textit{singular point} of the curve $C : f(x, y) = 0$ if
\[
\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.
\]
We call $P$ a \textit{non-singular point} if it is not singular, i.e., if at least one of the partial derivatives does not vanish, and we say that $C$ is a \textit{non-singular curve} (or a \textit{smooth curve}) if every point of $C$ is non-singular. If $P = (r, s)$ is a non-singular point of $C$, then we define the \textit{tangent line to $C$ at $P$} to be the line
\[
\frac{\partial f}{\partial x}(r, s)(x - r) + \frac{\partial f}{\partial y}(r, s)(y - s) = 0,
\]
as discussed above.

For a projective curve $C : F(X, Y, Z) = 0$ described by a homogeneous polynomial, we make similar definitions. More precisely, if $P = [a, b, c]$ is a point on $C$ with $c \neq 0$, then we go to the affine part of $C$ and check whether the point
\[
P_0 = \left(\frac{a}{c}, \frac{b}{c}\right)
\]
is singular on the affine curve $C_0 : F(x, y, 1) = 0$.

And if $c = 0$, then we can dehomogenize in some other way. For example, if $a \neq 0$, then we check whether the point
\[
P_0 = \left(\frac{b}{a}, \frac{c}{a}\right)
\]
is singular on the affine curve $C_0 : F(1, y, z) = 0$.

We say that $C$ is non-singular (or smooth) if all of its points, including the points at infinity, are non-singular. If $P$ is a non-singular point of $C$, we define the tangent line to $C$ at $P$ by dehomogenizing, finding the tangent line to the affine part of $C$ at $P$, and then homogenizing the equation of the tangent line to get a line in $\mathbb{P}^2$. (An alternative method to check for singularities and find tangent lines on projective curves is described in Exercise A.5.)

When one is faced with a complicated equation, it is natural to try to make a change of variables in order to simplify it. Probably the first significant example of this that you have seen is the process of completing the square to solve a quadratic equation. Thus to solve $Ax^2 + Bx + C = 0$, we multiply by $4A$ and rewrite the equation as
(2Ax + B)^2 + 4AC - B^2 = 0.

This suggests the substitution \( x' = 2Ax + B \), and then we can solve

\[ x'^2 + 4AC - B^2 = 0 \]

to get \( x' = \pm \sqrt{B^2 - 4AC} \).

The crucial final step uses the fact that our substitution is invertible, so we can solve for \( x \) in terms of \( x' \) to obtain the usual quadratic formula

\[ x = \frac{-B + x'}{2A} = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}. \]

More generally, suppose that we are given a projective curve of degree \( d \), say defined by an equation \( C : F(X, Y, Z) = 0 \). In order to change coordinates on \( \mathbb{P}^2 \), we make a substitution

\[
\begin{align*}
X &= m_{11}X' + m_{12}Y' + m_{13}Z', \\
Y &= m_{21}X' + m_{22}Y' + m_{23}Z', \\
Z &= m_{31}X' + m_{32}Y' + m_{33}Z'.
\end{align*}
\]

Then we get a new curve \( C' \) given by the equation \( F'(X', Y', Z') = 0 \), where \( F' \) is the polynomial

\[
F'(X', Y', Z') = F(m_{11}X' + m_{12}Y' + m_{13}Z', m_{21}X' + m_{22}Y' + m_{23}Z', m_{31}X' + m_{32}Y' + m_{33}Z').
\]

The change of coordinates (*) gives a map from \( C' \) to \( C \), that is, given a point \([a', b', c'] \in C'\), we substitute \( X' = a, Y' = b, \) and \( Z' = c \) into (*) to get a point \([a, b, c] \in C\). Further, this map \( C' \to C \) has an inverse provided that the matrix \( M = (m_{ij})_{1 \leq i, j \leq 3} \) is invertible. More precisely, if \( M^{-1} = N = (n_{ij}) \), then the change of coordinates

\[
\begin{align*}
X' &= n_{11}X + n_{12}Y + n_{13}Z, \\
Y' &= n_{21}X + n_{22}Y + n_{23}Z, \\
Z' &= n_{31}X + n_{32}Y + n_{33}Z,
\end{align*}
\]

maps \( C \) to \( C' \). We call a change of coordinates on \( \mathbb{P}^2 \) given by an invertible \( 3 \times 3 \) matrix a projective transformation. Note that if the matrix has rational coefficients, then the corresponding projective transformation gives a one-to-one correspondence between \( C(\mathbb{Q}) \) and \( C'(\mathbb{Q}) \). So the number theoretic problem of finding the rational points on the curve \( C \) is equivalent to the problem of finding the rational points on the curve \( C' \).
A.3 Intersections of Projective Curves

Recall that our geometric construction of the projective plane was based on the desire that every pair of distinct lines should intersect in exactly one point. In this section we are going to discuss the intersection of curves of higher degree.

How many intersection points should two curves have? Let’s begin with a thought experiment, and then we’ll consider some examples and see to what extent our intuition is correct. Let \( C_1 \) be an affine curve of degree \( d_1 \) and let \( C_2 \) be an affine curve of degree \( d_2 \). Thus \( C_1 \) and \( C_2 \) are given by polynomials

\[
C_1 : f_1(x, y) = 0 \quad \text{with} \quad \deg(f_1) = d_1, \\
C_2 : f_2(x, y) = 0 \quad \text{with} \quad \deg(f_2) = d_2.
\]

The points in the intersection \( C_1 \cap C_2 \) are solutions to the simultaneous equations

\[
f_1(x, y) = f_2(x, y) = 0.
\]

Suppose now that we consider \( f_1 \) as a polynomial in the variable \( y \) whose coefficients are polynomials in \( x \). Then \( f_1(x, y) = 0 \), being a polynomial of degree \( d_1 \) in \( y \), should in principle have \( d_1 \) roots \( y_1, \ldots, y_{d_1} \). Now we substitute each of these roots into the second equation \( f_2(x, y) \) to find \( d_1 \) equations for \( x \), namely

\[
f_2(x, y_1) = 0, \quad f_2(x, y_2) = 0, \quad \ldots \quad f_2(x, y_{d_1}) = 0.
\]

Each of these equations is a polynomial in \( x \) of degree \( d_2 \), so in principle each equation should yield \( d_2 \) values for \( x \). Altogether we appear to get \( d_1 d_2 \) pairs \( (x, y) \) that satisfy \( f_1(x, y) = f_2(x, y) = 0 \), which seems to indicate that we should have \( \#(C_1 \cap C_2) = d_1 d_2 \). For example, a curve of degree 2 and a curve of degree 4 should intersect in 8 points, as illustrated in Figure A.3. This assertion, that curves of degree \( d_1 \) and \( d_2 \) intersect in \( d_1 d_2 \) points, is indeed true provided that it is interpreted properly. However, matters are considerably more complicated than they appear at first glance, as will be clear from the following examples. [Can you find all of the ways in which our plausibility argument fails to be a valid proof? For example, the “roots” \( y_1, \ldots, y_{d_1} \) really depend on \( x \), so we should write \( f_2(x, y_i(x)) = 0 \), and then it is not at all clear how many roots we should expect.]

Curves of degree one are lines, and curves of degree two are called conics (short for conic sections). We already know that two lines in \( \mathbb{P}^2 \) intersect in
a unique point, so the next simplest case is the intersection of a line and a conic. Our discussion above leads us to expect two intersection points, so we look at some examples to see what really happens. The (affine) line and conic

\[ C_1 : x + y + 1 = 0 \quad \text{and} \quad C_2 : x^2 + y^2 = 1 \]

intersect in the two points \((-1, 0)\) and \((0, -1)\), as is easily seen by substituting \(y = -x - 1\) into the equation for \(C_2\) and solving the resulting quadratic equation for \(x\); see Figure A.4(a). Similarly,

\[ C_1 : x + y = 0 \quad \text{and} \quad C_2 : x^2 + y^2 = 1 \]

intersect in the two points \(\left(\frac{1}{2}\sqrt{2}, -\frac{1}{2}\sqrt{2}\right)\) and \(\left(-\frac{1}{2}\sqrt{2}, \frac{1}{2}\sqrt{2}\right)\). Note that we have to allow real coordinates for the intersection points, even though \(C_1\) and \(C_2\) are rational curves; see Figure A.4(b).

What about the intersection of the line and conic

\[ C_1 : x + y + 2 = 0 \quad \text{and} \quad C_2 : x^2 + y^2 = 1? \]

They do not intersect at all in the usual Euclidean plane \(\mathbb{R}^2\), as illustrated in Figure A.4(c), but if we allow complex numbers then we again find two intersection points,

\[ \left(-1 + \frac{\sqrt{2}}{2}i, -1 - \frac{\sqrt{2}}{2}i\right) \quad \text{and} \quad \left(-1 - \frac{\sqrt{2}}{2}i, -1 + \frac{\sqrt{2}}{2}i\right). \]
Of course, it is reasonable to allow complex coordinates, since even for polynomials of one variable we need to use complex numbers to ensure that a polynomial of degree $d$ actually has $d$ roots counted with multiplicities.

Next we look at

$$C_1 : x + 1 = 0 \quad \text{and} \quad C_2 : x^2 - y = 0.$$ 

These curves appear to intersect in the single point $(-1, 1)$ as shown in Figure A.4(d), but appearances can be deceiving. Remember that even for two lines, we may need to also look at the points at infinity in $\mathbb{P}^2$. In our case, the line $C_1$ is in the vertical direction, and the tangent lines to the parabola $C_2$ approach the vertical direction, so geometrically $C_1$ and $C_2$ should have a common point at infinity corresponding to the vertical direction. Following our maxim from Section A.2, we now check this assertion algebraically. First we homogenize the equations for $C_1$ and $C_2$ to get the corresponding projective curves

$$\tilde{C}_1 : X + Z = 0 \quad \text{and} \quad \tilde{C}_2 : X^2 - YZ = 0.$$ 

Then $\tilde{C}_1 \cap \tilde{C}_2$ consists of the two points $[-1, 1, 1]$ and $[0, 1, 0]$, as may be seen by substituting $X = -Z$ into the equation for $\tilde{C}_2$. So we get the expected two points provided that we work with projective curves.

All of this looks very good, but the next example illustrates another problem that may occur. Consider the intersection of the line and conic

$$C_1 : x + y = 2 \quad \text{and} \quad C_2 : x^2 + y^2 = 2;$$

see Figure A.4(e). Then $C_1 \cap C_2$ consists of the single point $(1, 1)$, and even if we go to projective curves

$$\tilde{C}_1 : X + Y = 2Z \quad \text{and} \quad \tilde{C}_2 : X^2 + Y^2 = 2Z^2,$$

we still find the single intersection point $[1, 1, 1]$. What is wrong?

Geometrically we immediately see the problem, namely the line $C_1$ is tangent to the circle $C_2$ at the point $(1, 1)$, so in some sense that point should count double. We can also see this algebraically. If we substitute the relation $y = 2 - x$ from $C_1$ into the equation for $C_2$ and simplify, we get the equation $2x^2 - 4x + 2 = 0$, or equivalently $2(x - 1)^2 = 0$. So we do have a quadratic equation to solve for $x$, and normally we would expect to find two distinct roots, but in this case we happen to find one root repeated twice. This makes sense, since even a degree $d$ polynomial of one variable repeated can only be
Figure A.4: Some of the ways in which curves may intersect
said to have \(d\) complex roots if we count multiple roots according to their multiplicities.

This multiplicity problem may also occur if one of the curves is singular at \(P\), even if the two curves do not have the same tangent direction. For example, consider the intersection of the line and the degree three curve

\[ C_1 : x - y = 0 \quad \text{and} \quad C_2 : x^3 - y^2 = 0; \]

see Figure A.4(f). Our intuition says that \(C_1 \cap C_2\) should consider of three points. Substituting \(y = x\) into the equation for \(C_2\) gives \(x^3 - x^2 = 0\). This is a cubic equation for \(x\), but it has only two distinct roots, namely \(x = 0\) and \(x = 1\). Thus \(C_1 \cap C_2\) contains only the two points \((0, 0)\) and \((1, 1)\), but the point \((0, 0)\) needs to be counted twice, which gives the expected three points when we count points with their multiplicity.

Finally, we look at an example where things go spectacularly wrong. Consider the intersection of the line and the conic

\[ C_1 : x + y + 1 = 0 \quad \text{and} \quad C_2 : 2x^2 + xy - y^2 + 4x + y + 2 = 0. \]

When we substitute \(y = -x - 1\) into the equation for \(C_2\), we find that everything cancels out and we are left with \(0 = 0\). This happens because the equation for \(C_2\) factors as

\[ 2x^2 + xy - y^2 + 4x + y + 2 = (x + y + 1)(2x - y + 2), \]

so every point on \(C_1\) lies on \(C_2\). Notice that \(C_2\) is the union of two curves, namely \(C_1\) and the line \(2x - y + 2 = 0\).

In general, if \(C\) is a curve given by an equation \(C : f(x, y) = 0\), then we factor \(f\) into a product of irreducible polynomials

\[ f(x, y) = p_1(x, y)p_2(x, y) \cdots p_n(x, y). \]

Note that \(\mathbb{C}[x, y]\) is a unique factorization domain, so every polynomial has an essentially unique factorization into such a product. Then the \textit{irreducible components of the curve} \(C\) are the curves

\[ p_1(x, y) = 0, \quad p_2(x, y) = 0, \quad \cdots \quad p_n(x, y) = 0. \]

We say that \(C\) is \textit{irreducible} if it has only one irreducible component, or equivalently, if \(f(x, y)\) is an irreducible polynomial. Next, if \(C_1\) and \(C_2\) are two curves, we say that \(C_1\) and \(C_2\) \textit{have no common components} if their irreducible components are distinct. It is not hard to prove that \(C_1 \cap C_2\) consists
of a finite set of points if and only if \( C_1 \) and \( C_2 \) have no common components. Finally, if we work instead with projective curves \( C, C_1, C_2 \), then we make the same definitions using factorizations into products of irreducible homogeneous polynomials in \( \mathbb{C}[X, Y, Z] \).

We now consider the general case of projective curves \( C_1 \) and \( C_2 \), which we assume to have no common components. The intersection \( C_1 \cap C_2 \) is then a finite set of points with complex coordinates. To each point \( P \in \mathbb{P}^2 \) we assign a multiplicity or intersection index \( I(C_1 \cap C_2, P) \). This is a non-negative integer reflecting the extent to which \( C_1 \) and \( C_2 \) are tangent to one another at \( P \) or are not smooth at \( P \). We give a formal definition in Section A.4, but one can get a good feeling for the intersection index from the following properties:

(i) If \( P \notin C_1 \cap C_2 \), then \( I(C_1 \cap C_2, P) = 0 \).

(ii) If \( P \in C_1 \cap C_2 \), if \( P \) is a non-singular point of \( C_1 \) and \( C_2 \), and if \( C_1 \) and \( C_2 \) have different tangent directions at \( P \), then \( I(C_1 \cap C_2, P) = 1 \). In this case, one says that \( C_1 \) and \( C_2 \) intersect transversally at \( P \).

(iii) If \( P \in C_1 \cap C_2 \) and if \( C_1 \) and \( C_2 \) do not intersect transversally at \( P \), then \( I(C_1 \cap C_2, P) \geq 2 \).

With these preliminaries, we are now ready to formally state the theorem that justifies the plausibility argument that we gave at the beginning of this section.

**Theorem A.1 (Bezout’s Theorem).** Let \( C_1 \) and \( C_2 \) be projective curves with no common components. Then

\[
\sum_{P \in C_1 \cap C_2} I(C_1 \cap C_2, P) = (\deg C_1)(\deg C_2),
\]

where the sum is over all points of \( C_1 \cap C_2 \) having complex coordinates. In particular, if \( C_1 \) and \( C_2 \) are smooth curves with only transversal intersections, then \#(\( C_1 \cap C_2 \)) = (\deg C_1)(\deg C_2), and in all cases there is an inequality

\[
\#(C_1 \cap C_2) \leq (\deg C_1)(\deg C_2).
\]

**Proof.** We give the proof of Bezout’s theorem in Section A.4.

It would be hard to overestimate the importance of Bezout’s theorem in the study of projective geometry. We should stress how amazing a theorem it is. The projective plane was constructed so as to ensure that any two lines, i.e.,
curves of degree one, intersect in exactly one point, so one could say that the projective plane is formed by taking the affine plane and adding just enough points to make Bezout’s theorem true for curves of degree one. It then turns out that the projective plane has enough points to make Bezout’s theorem true for all projective curves!

Sometimes Bezout’s theorem is used to determine if two curves are the same, or at least have a common component. For example, if \( C_1 \) and \( C_2 \) are conics, and if \( C_1 \) and \( C_2 \) have five points in common, then Bezout’s theorem tells us that they have a common component. Since the degree of a component can be no larger than the degree of the curve, it follows that there is some line \( L \) contained in both \( C_1 \) and \( C_2 \), or else \( C_1 = C_2 \). Thus there is only one conic going through any five given points as long as no three of them are collinear. This is analogous to the fact that there is a unique line going through two given points. More generally, one see from Bezout’s theorem that if \( C_1 \) and \( C_2 \) are irreducible curves of degree \( d \) with \( d^2 + 1 \) points in common, then \( C_1 = C_2 \). Note, however, that for \( d \geq 3 \), there is in general no curve of degree \( d \) going through \( d^2 + 1 \) preassigned points. This is because the number \( d^2 + 1 \) of conditions to be met is greater than the number \((d + 1)(d + 2)/2\) of unknown coefficients of a homogeneous polynomial of degree \( d \).

We now want to consider a slightly more complicated situation. Suppose that \( C_1 \) and \( C_2 \) are two cubic curves of degree 3, which intersect in 9 distinct points \( P_1, \ldots, P_9 \). Suppose further that \( D \) is another cubic curve that happens to go through the first 8 points \( P_1, \ldots, P_8 \). We claim that \( D \) also goes through the ninth point \( P_9 \). To see why this is true, we consider the collection of all cubic curves in \( \mathbb{P}^2 \), which we denote by \( \mathcal{C}(3) \). An element \( C \in \mathcal{C}(3) \) is given by a homogeneous equation

\[
C : aX^3 + bX^2Y + cXY^2 + dY^3 + eX^2Z + fXYZ + gY^2Z + hXZ^2 + iYZ^2 + jZ^3 = 0,
\]

so \( C \) is determined by the ten coefficients \( a, b, \ldots, j \). Of course, if we multiply the equation for \( C \) by any non-zero constant, then we get the same curve, so really \( C \) is determined by the homogeneous 10-tuple \([a, b, \ldots, j]\). Conversely, if two 10-tuples give the same curve, then they differ by multiplication by a constant. In other words, the set of cubic curve \( \mathcal{C}(3) \) is in a very natural way isomorphic to the projective space \( \mathbb{P}^9 \).

Suppose that we are given a point \( P \in \mathbb{P}^2 \) and ask for all cubic curves that go through \( P \). This describes a certain subset of \( \mathcal{C}(3) \cong \mathbb{P}^9 \), and it is easy to see what this subset is. If \( P \) has homogeneous coordinates \( P = [X_0, Y_0, Z_0] \), then substituting \( P \) into the equation for \( C \) shows that \( C \) contains \( P \) if and
only if the 10-tuple \([a, b, \ldots, j]\) satisfies the homogeneous linear equation

\[
\begin{aligned}
(X_0^3)a + (X_0^2Y_0)b + (X_0Y_0^2)c + (Y_0^3)d + (X_0^2Z_0)e + (X_0Z_0^2)f \\
+ (Y_0^2Z_0)g + (Y_0Z_0^2)h + (Z_0^3)i + (X_0Y_0Z_0)j = 0.
\end{aligned}
\]

N.B., this is a linear equation in the 10 variables \(a, b, \ldots, j\). In other words, for a given point \(P \in \mathbb{P}^2\), the set of cubic curves \(C \in \mathcal{C}^{(3)}\) that contain \(P\) corresponds to the zeros of a homogeneous linear equation in \(\mathbb{P}^9\).

Similarly, if we fix two points \(P, Q \in \mathbb{P}^2\), then the set of cubic curves \(C \in \mathcal{C}^{(3)}\) containing both \(P\) and \(Q\) is given by the common solutions of two linear equations in \(\mathbb{P}^9\), where one linear equation is specified by \(P\) and the other by \(Q\). Continuing in this fashion, we find that for a collection of \(n\) points \(P_1, \ldots, P_n \in \mathbb{P}^2\), there is a one-to-one correspondence between the two sets

\[
\{ C \in \mathcal{C}^{(3)} : P_1, \ldots, P_n \in C \} \quad \text{and} \quad \left\{ \text{simultaneous solutions of a certain system of } n \text{ homogeneous linear equations in } \mathbb{P}^9 \right\}.
\]

For example, suppose that we take \(n = 9\). The solutions to a system of 9 homogeneous linear equations in 10 variables generally consists of the multiples of a single solution. In other words, if \(v_0\) is a non-zero solution, then every solution will have the form \(\lambda v_0\) for some constant \(\lambda\). Now let

\[
C_1 : F_1(X, Y, Z) = 0 \quad \text{and} \quad C_2 : F_2(X, Y, Z) = 0
\]

be cubic curves in \(\mathbb{P}^2\), each going through the given nine points. The coefficients of \(F_1\) and \(F_2\) are then 10-tuples that are solutions to the given system of linear equations, so we conclude that \(F_1 = \lambda F_2\), and hence that \(C_1 = C_2\). Thus we find that, in general, there is exactly one cubic curve in \(\mathbb{P}^2\) that passes through nine given points. Note, however, that for special sets of nine points it is possible to have a one parameter family of cubic curves going through them.

That is the situation in our original problem, to which we now return. Namely, we take two cubic curves \(C_1\) and \(C_2\) in \(\mathbb{P}^2\) that intersect in nine distinct points \(P_1, \ldots, P_9\). Let \(C_1\) and \(C_2\) be given by the equations

\[
C_1 : F_1(X, Y, Z) = 0 \quad \text{and} \quad C_2 : F_2(X, Y, Z) = 0.
\]

We consider the set of all cubic curves \(C \in \mathcal{C}^{(3)}\) that pass through the first eight points \(P_1, \ldots, P_8\). This set corresponds to the simultaneous solutions
of eight homogeneous linear equations in ten variables. The set of solutions of this system consists of all linear combinations of two linearly independent 10-tuples. In other words, if \(v_1\) and \(v_2\) are independent solutions, then every solution has the form \(\lambda_1 v_1 + \lambda_2 v_2\) for some constants \(\lambda_1\) and \(\lambda_2\).2

But we already know two cubic curves passing through the eight points \(P_1, \ldots, P_8\), namely \(C_1\) and \(C_2\). The coefficients of their equations \(F_1\) and \(F_2\) thus give two 10-tuples solving the system of eight homogeneous linear equations, so they span the complete solution set. This means that if \(D\) is any other cubic curve in \(\mathbb{P}^2\) that contains the eight points \(P_1, \ldots, P_8\), then the equation for \(D\) has the form

\[
D : \lambda_1 F_1(X, Y, Z) + \lambda_2 F_2(X, Y, Z) = 0 \quad \text{for some constants } \lambda_1, \lambda_2.
\]

But the ninth point \(P_9\) is on both \(C_1\) and \(C_2\), so \(F_1(P_9) = F_2(P_9) = 0\). It follows from the equation for \(D\) that \(D\) also contains the point \(P_9\), which is exactly what we have been trying to demonstrate.

More generally, the following theorem is true.

**Theorem A.2** (Cayley–Bacharach Theorem). Let \(C_1\) and \(C_2\) be curves in \(\mathbb{P}^2\) without common components of respective degrees \(d_1\) and \(d_2\), and suppose that \(C_1\) and \(C_2\) intersect in \(d_1d_2\) distinct points. Let \(D\) be a curve in \(\mathbb{P}^2\) of degree \(d_1 + d_2 - 3\). If \(D\) passes through all but one of the points of \(C_1 \cap C_2\), then \(D\) must also pass through the remaining point.

It is not actually necessary that \(C_1\) and \(C_2\) intersect in distinct points. For example, if \(P \in C_1 \cap C_2\) is a point of multiplicity two, say because \(C_1\) and \(C_2\) have the same tangent direction at \(P\), then one needs to require that \(D\) also has the same tangent direction at \(P\). The most general result is somewhat difficult to state, so we content ourselves with the following version.

**Theorem A.3** (Cubic Cayley–Bacharach Theorem). Let \(C_1\) and \(C_2\) be cubic curves in \(\mathbb{P}^2\) without common components, and assume that \(C_1\) is smooth. Suppose that \(D\) is another cubic curve that contains eight of the intersection points of \(C_1 \cap C_2\) counting multiplicities. This means that if \(C_1 \cap C_2 = \{P_1, \ldots, P_r\}\), then

\[
I(C_1 \cap D, P_i) \geq I(C_1 \cap C_2, P_i) \quad \text{for } 1 \leq i < r,
\]

2In principle, the set of solutions might have dimension greater than two. We leave it as a (challenging) exercise for you to check that because the eight points \(P_1, \ldots, P_8\) are distinct, the corresponding linear equations are independent; see Exercise A.17.
and
\[ I(C_1 \cap D, P_r) \geq I(C_1 \cap C_2, P_r) - 1. \]

Then \( D \) goes through the ninth point of \( C_1 \cap C_2 \), which in terms of multiplicities means that
\[ I(C_1 \cap D, P_r) \geq I(C_1 \cap C_2, P_r). \]

We conclude this section of the appendix by applying the Cayley–Bacharach theorem to prove a beautiful geometric result of Pascal. Let \( C \) be a smooth conic, for example, a hyperbola, a parabola, or an ellipse. Choose any six points lying on the conic, say labeled consecutively \( P_1, P_2, \ldots, P_6 \), and play connect-the-dots to draw a hexagon. Now take the lines through opposite sides of the hexagon and extend them to find the intersection points as illustrated in Figure A.5, say
\[ \overrightarrow{P_1P_2} \cap \overrightarrow{P_4P_5} = \{Q_1\}, \quad \overrightarrow{P_2P_3} \cap \overrightarrow{P_5P_6} = \{Q_2\}, \quad \overrightarrow{P_3P_4} \cap \overrightarrow{P_6P_1} = \{Q_3\}. \]

**Theorem A.4** (Pascal’s Theorem). *The three points \( Q_1, Q_2, Q_3 \) described above lie on a line.*

To prove Pascal’s theorem, we consider the two cubic curves
\[ C_1 = \overrightarrow{P_1P_2} \cup \overrightarrow{P_3P_4} \cup \overrightarrow{P_5P_6} \quad \text{and} \quad C_2 = \overrightarrow{P_2P_3} \cup \overrightarrow{P_4P_5} \cup \overrightarrow{P_6P_1}. \]

Why do we call \( C_1 \) and \( C_2 \) cubic curves? The answer is that if we choose an equation for the line \( \overrightarrow{P_jP_j} \), say
\[ \alpha_{ij}X + \beta_{ij}Y + \gamma_{ij}Z = 0, \]
then \( C_1 \) is given by the homogeneous cubic equation
\[ (\alpha_{12}X + \beta_{12}Y + \gamma_{12}Z)(\alpha_{34}X + \beta_{34}Y + \gamma_{34}Z)(\alpha_{56}X + \beta_{56}Y + \gamma_{56}Z) = 0, \]
and similarly for \( C_2 \).

Notice that all nine of the points
\[ P_1, P_2, P_3, P_4, P_5, P_6, Q_1, Q_2, Q_3 \quad \text{are on both} \quad C_1 \quad \text{and} \quad C_2. \]

This sets us up to use the Cayley–Bacharach theorem. We take \( D \) to be the cubic curve that is the union of our original conic \( C \) with the line through \( Q_1 \) and \( Q_2 \),
\[ D = C \cup \overrightarrow{Q_1Q_2}. \]
Clearly $D$ contains the eight points $P_1, P_2, P_3, P_4, P_5, P_6, Q_1, Q_2$. The Cayley–Bacharach theorem then tells us that $D$ contains the ninth point in $C_1 \cap C_2$, namely $Q_3$. Now $Q_3$ does not lie on $C$, since otherwise the line $\overrightarrow{P_6P_1}$ would intersect the conic in the three points $P_6, P_1, Q_3$, contradicting Bezout’s theorem. Therefore $Q_3$ must be on the line $\overrightarrow{Q_1Q_2}$. In other words, the points $Q_1$, $Q_2$, and $Q_3$ are collinear, which completes the proof of Pascal’s theorem.

A.4 Intersection Multiplicities and a Proof of Bezout’s Theorem

We give the proof of Bezout’s theorem in the form of a long exercise with hints. It is quite elementary. For the first weak inequality, which is all that is needed in many important applications of the theorem, we use only linear
algebra and the notion of dimension of a vector space. After that, we need
the concepts of commutative ring, ideal, and quotient ring, and the fact that
unique factorization holds in polynomial rings, but that is about all.

Let \( C_1 \) and \( C_2 \) be curves in \( \mathbb{P}^2 \) of respective degrees \( n_1 \) and \( n_2 \), without
common components. Until the last step of the proof we assume that the
line at infinity is not a component of either curve, and we work with affine
coordinates \( x \) and \( y \). Let

\[
C_1 : f_1(x, y) = 0 \quad \text{and} \quad C_2 : f_2(x, y) = 0
\]

be the equations for the two curves in the affine plane \( \mathbb{A}^2 \). The assumptions
we have made mean that the polynomials \( f_1 \) and \( f_2 \) have no common factor
and are of degree \( n_1 \) and \( n_2 \), respectively.

The proof is pure algebra, although the geometric ideas behind it should
be apparent, and it works over any algebraically closed field \( k \). The reader is
welcome to take \( k = \mathbb{C} \), but \( k \) could also be an algebraic closure of a finite
field \( \mathbb{F}_p \), for example. We also note that in this section, \( \dim V \) means the
dimension of \( V \) as a \( k \)-vector space.

Let \( R = k[x, y] \) be a polynomial ring in two variables, and let \((f_1, f_2) = f_1R + f_2R\) be the ideal of \( R \) generated by the polynomials \( f_1 \) and \( f_2 \). The
steps in the proof of Bezout’s theorem are as follows:

(1) We prove the following two inequalities which, on eliminating the middle
term, show that the number of intersection points of \( C_1 \) and \( C_2 \) in \( \mathbb{A}^2 \) is at
most \( n_1 n_2 \):

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

(2) We show that \( (B) \) is an equality if \( C_1 \) and \( C_2 \) do not meet at infinity.

(3) We strengthen \( (A) \) to get

\[
\sum_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} I(C_1 \cap C_2, P)^{(A^+)} \leq \dim \left( R/(f_1, f_2) \right),
\]

where \( I(C_1 \cap C_2, P) \) is a suitably defined intersection multiplicity of \( C_1 \)
and \( C_2 \) at \( P \).

(4) We show that \( (A^+) \) is in fact an equality.

The fact that \( k \) is algebraically closed is not needed for the proofs of the
inequalities in (1) and (3), but it is essential for verifying the equalities in (2)
and (4). Taken together, (2) and (4) give Bezout’s theorem in the case that $C_1$ and $C_2$ do not meet at infinity. To get it in general, there is one more step.

(5) We show that the definition of intersection multiplicity does not change when we make a projective transformation, and that there is a line $L$ in $\mathbb{P}^2$ not meeting any intersection point. Changing coordinates so that the line $L$ is the line at infinity, we then get Bezout in general.

To round out the argument, we include one more segment:

(6) We prove some basic properties satisfied by the intersection multiplicity $I(C_1 \cap C_2, P)$ and show that it depends only on the initial part of the Taylor expansions of $f_1$ and $f_2$ at $P$.

Now we sketch the proof as a series of exercises with hints, breaking each of the segments (1)–(5) into smaller steps.

(1.1) Let $P_1, P_2, \ldots, P_m$ be $m$ different points in the $(x, y)$-plane. Show that for each $i$ there is a polynomial $h_i = h_i(x, y)$ such that $h_i(P_i) = 1$ and $h_i(P_j) = 0$ for $j \neq i$. (Idea. Construct $h_i$ as a product of linear polynomials, using the fact that for each $j \neq i$ there is a line through $P_j$ not meeting $P_i$.)

(1.2) Suppose that the $m$ points $P_i$ from (1.1) lie in $C_1 \cap C_2$. Prove that the polynomials $h_i$ are linearly independent modulo $(f_1, f_2)$, and consequently that

$$m \leq \dim \left( R/(f_1, f_2) \right).$$

This proves inequality $(A)$. (Idea. Consider a possible dependence

$$c_1 h_1 + c_2 h_2 + \cdots + c_m h_m = g_1 f_1 + g_2 f_2 \in (f_1, f_2)$$

with $c_i \in k$. Substitute $P_i$ into the equation to show that every $c_i = 0$.)

This takes care of inequality $(A)$. To prove $(B)$, for each integer $d \geq 0$ we define:

$$\phi(d) = \frac{1}{2} (d + 1)(d + 2) = \frac{1}{2} d^2 + \frac{3}{2} d + 1,$$

$$R_d = \text{(vector space of polynomial } f(x, y) \text{ of degree } \leq d),$$

$$W_d = R_{d-n_1} f_1 + R_{d-n_2} f_2.$$

Thus $W_d$ is the $k$-vector space of polynomials of the form

$$f = g_1 f_1 + g_2 f_2 \quad \text{with } \deg g_i \leq d - n_i \text{ for } i = 1, 2.$$

Notice that $W_d = 0$ if $d < \max\{n_1, n_2\}$, and in any case, $W_d \subset (f_1, f_2)$. 
(1.3) Show that \( \dim R_d = \phi(d) \). (Idea. One way to see this is to note that
\[
\phi(d) - \phi(d - 1) = \text{(number of monomials } x^i y^j \text{ of degree } d) = d + 1
\]
and use induction on \( d \).)

(1.4) For \( d \geq n_1 + n_2 \), show that
\[
R_{d-n_1} f_1 \cap R_{d-n_2} f_2 = R_{d-n_1-n_2} f_1 f_2.
\]
Here is where we use the hypothesis that \( f_1 \) and \( f_2 \) have no common factor.

(1.5) Prove that for \( d \geq n_1 + n_2 \),
\[
\dim R_d - \dim W_d = \phi(d) - \phi(d-n_1) - \phi(d-n_2) - \phi(d-n_1-n_2) = n_1 n_2.
\]
(Idea. If \( f \) is a non-zero polynomial, then \( g \mapsto fg \) defines an isomorphism \( R_{d-j} \sim \to R_{d-j} f \), and hence \( \dim R_{d-j} f = \phi(d-j) \). Now use the lemma from linear algebra which says that
\[
\dim(U + V) = \dim(U) + \dim(V) - \dim(U \cap V)
\]
for subspaces \( U \) and \( V \) of a finite dimensional vector space.)

(1.6) Prove inequality (B) by showing that if \( g_1, g_2, \ldots, g_{n_1 n_2+1} \) are elements of \( R \), then they are linearly dependent modulo \( (f_1, f_2) \). (Idea. Take \( d \) so large that the \( g_j \) are in \( R_d \) and so (1.5) holds. Then use (1.5) to show that there is a non-trivial linear combination \( g = \sum c_j g_j \) such that \( g \in W_d \subset (f_1, f_2) \).

This finishes segment (1). For segment (2), we begin by recalling how one computes the intersections of an affine curve \( f(x, y) = 0 \) with the line at infinity.

(2.1) For each non-zero polynomial \( f = f(x, y) \), let \( f^* \) denote the homogeneous part of \( f \) of highest degree. In other words, if
\[
f = \sum_{i,j} c_{ij} x^i y^j \quad \text{has degree } n, \quad f^* = \sum_{i+j=n} c_{ij} x^i y^j.
\]

Because \( k \) is algebraically closed, we can factor \( f^* \) into linear factors,
\[
f^*(x, y) = \prod_{i=1}^{n} (a_i x + b_i y) \quad \text{with } a_i, b_i \in k \text{ and } n = \deg f = \deg f^*.
\]
Show that the points at infinity on the curve \( f(x, y) = 0 \) are the points with homogeneous coordinates

\[
[X, Y, Z] = [b_i, -a_i, 0].
\]

(Idea. Put \( x = X/Z, y = Y/Z \), etc.)

An example should make this clearer. Consider the polynomials

\[
f(x, y) = x^4 - x^2 y^2 + 3x^3 + xy^2 + 2y^2 + 8x + 3,
\]

\[
f^*(x, y) = x^4 - x^2 y^2 = x^2(x + y)(x - y),
\]

each of which has degree 4. The quartic curve \( f(x, y) = 0 \) thus meets the line at infinity in the points \([0, 1, 0], [1, -1, 0], \text{ and } [1, 1, 0]\). The fact that \( x^2 \) divides \( f^*(x, y) \) means that the curve is tangent to the line at infinity at the point \([0, 1, 0]\).

The remaining steps in segment 2 are as follows:

(2.2) If \( C_1 \) and \( C_2 \) do not meet at infinity, show that \( f_1^* \) and \( f_2^* \) have no common factor.

(2.3) If \( f_1^* \) and \( f_2^* \) have no common factor, show that \( (f_1, f_2) \cap R_d = W_d \) for all \( d \geq n_1 + n_2 \).

(2.4) If \( (f_1, f_2) \cap R_d = W_d \) and \( d \geq n_1 + n_2 \), show that

\[
\dim \left( \frac{R}{(f_1, f_2)} \right) \geq n_1 n_2.
\]

(Idea. (2.2) is an easy consequence of (2.1). To do (2.3), we suppose that \( f \in (f_1, f_2) \cap R_d \) is written in the form \( f = g_1 f_1 + g_2 f_2 \) with \( g_1 \) and \( g_2 \) of smallest possible degree. If \( \deg g_1 > d - n_1 \), then looking at the terms of highest degree shows that \( g_1^* f_1^* + g_2^* f_2^* = 0 \). Then use the fact that \( f_1^* \) and \( f_2^* \) are relatively prime to show that there is an \( h \) such that

\[
\deg(g_1 + hf_2) < \deg(g_1) \quad \text{and} \quad \deg(g_2 + hf_1) < \deg(g_2).
\]

Deduce that \( \deg g_i \leq d - n \), and hence that \( f \in W_d \). For (2.4), note that by (1.5) there are \( n_1 n_2 \) elements in \( R_d \) that are linearly independent modulo \( W_d \), and that if \( (f_1, f_2) \cap R_d = W_d \), then they are linearly independent as elements of \( R \) modulo \( (f_1, f_2) \). Hence \( \dim \frac{R}{(f_1, f_2)} \geq n_1 n_2 \).

To define intersection multiplicity, we introduce the important notion of the local ring \( \mathcal{O}_P \) of a point \( P \in \mathbb{A}^2 \). Let \( K = k(x, y) \) be the fraction field of \( R = k[x, y] \), that is, \( K \) is the field of rational functions of \( x \)
A.4. Intersection Multiplicities and a Proof of Bezout’s Theorem

and \( y \). For a point \( P = (a, b) \) in the \((x, y)\)-plane and a rational function \( \phi = f(x, y)/g(x, y) \in K \), we say that \( \phi \) is defined at \( P \) if \( g(a, b) \neq 0 \), and then we put

\[
\phi(P) = \frac{f(a, b)}{g(a, b)} = \frac{f(P)}{g(P)}.
\]

For a given point \( P \), we define the local ring of \( P \) to be the set

\[
\mathcal{O}_P = \{ \phi \in K : \phi \text{ is defined at } P \}.
\]

We leave the following basic properties of \( \mathcal{O}_P \) as exercises. First, \( \mathcal{O}_P \) is a subring of \( K \), and the evaluation map

\[
\mathcal{O}_P \rightarrow k, \quad \phi \mapsto \phi(P),
\]

is a ring homomorphism of \( \mathcal{O}_P \) onto \( k \) that is the identity on \( k \). Let

\[
\mathcal{M}_P = \{ \phi \in \mathcal{O}_P : \phi(P) = 0 \}
\]

be the kernel of the evaluation homomorphism. Then \( \mathcal{O}_P \) is equal to the direct sum \( \mathcal{O}_P = k + \mathcal{M}_P \) and \( \mathcal{O}_P / \mathcal{M}_P \cong k \). An element \( \phi \in \mathcal{O}_P \) has an inverse in \( \mathcal{O}_P \) if and only if \( \phi \notin \mathcal{M}_P \). Every ideal of \( \mathcal{O}_P \), other than \( \mathcal{O}_P \) itself, is contained in \( \mathcal{M}_P \), so \( \mathcal{M}_P \) is the unique maximal ideal of \( \mathcal{O}_P \). (A ring having a unique maximal ideal is called a local ring. We used another local ring \( R_p \subset Q \) in Section 2.4; see also Exercise 2.7.)

Now let \( (f_1, f_2)_P = \mathcal{O}_P f_1 + \mathcal{O}_P f_2 \) denote the ideal in \( \mathcal{O}_P \) generated by \( f_1 \) and \( f_2 \). Our definition of intersection multiplicity of \( C_1 \) and \( C_2 \) at \( P \), also called the intersection index, is

\[
I(C_1 \cap C_2, P) = \dim\left( \mathcal{O}_P / (f_1, f_2)_P \right).
\]

We are now ready to do segment (3), which means taking inequality (A) and strengthening it to inequality \((A^+)\).

(3.1) Show that

\[
\dim\left( \mathcal{O}_P / (f_1, f_2)_P \right) \leq \dim\left( R / (f_1, f_2) \right).
\]

Deduce from inequality \((B)\) that the intersection multiplicity \( I(C_1 \cap C_2, P) \) is finite. \((\text{Idea. Note that any finite set of elements in } \mathcal{O}_P \text{ can be written over a common denominator. Show that if } g_1/h, g_2/h, \ldots, g_r/h \text{ are elements of } \mathcal{O}_P \text{ that are linearly independent modulo } (f_1, f_2)_P, \text{ then } g_1, g_2, \ldots, g_r \text{ are elements of } R \text{ that are linearly independent modulo } (f_1, f_2)\).\)
(3.2) Show that $\mathcal{O}_P = R + (f_1, f_2)_P$. *(Idea. By (3.1), we may suppose that the elements $g_i/h$ span $\mathcal{O}_P$ modulo $(f_1, f_2)_P$, and because $h^{-1} \in \mathcal{O}_P$, it follows that the polynomials $g_i$ span $\mathcal{O}_P$ modulo $(f_1, f_2)_P$.)

(3.3) Show that if $P \notin C_1 \cap C_2$, then $I(C_1 \cap C_2, P) = 0$. Show that if $P \in C_1 \cap C_2$, then

$$(f_1, f_2)_P \subset \mathcal{M}_P \quad \text{and} \quad I(C_1 \cap C_2, P) = 1 + \dim \left( \mathcal{M}_P / (f_1, f_2)_P \right).$$

Conclude that if $P \in C_1 \cap C_2$, then $I(C_1 \cap C_2, P) \geq 1$, with equality if and only if $(f_1, f_2)_P = \mathcal{M}_P$.

(3.4) Suppose that $P \in C_1 \cap C_2$. Let $r$ satisfy $r \geq \dim(\mathcal{O}_P / (f_1, f_2)_P)$. Show that $\mathcal{M}_P^r \subset (f_1, f_2)_P$. *(Idea. We are to prove that, given any collection of $r$ elements $t_1, t_2, \ldots, t_r$ in $\mathcal{M}_P$, their product $t_1t_2 \cdots t_r$ is in $(f_1, f_2)_P$. Define a sequence of ideals $J_i$ in $\mathcal{O}_P$ by

$$J_i = t_1t_2 \cdots t_i\mathcal{O}_P + (f_1, f_2)_P \quad \text{for } 1 \leq i \leq r, \text{ and } \quad J_{r+1} = (f_1, f_2)_P.$$ 

Then

$$\mathcal{M}_P \supset J_1 \supset J_2 \supset \cdots \supset J_r \supset J_{r+1} = (f_1, f_2)_P.$$ 

Since $r \geq \dim(\mathcal{O}_P / (f_1, f_2)_P)$, it follows that $J_i = J_{i+1}$ for some $i$ with $1 \leq i \leq r$. If $i = r$, then $t_1t_2 \cdots t_r \in (f_1, f_2)_P$ and we are done. If $i < r$, then we have

$$t_1t_2 \cdots t_i = t_1t_2 \cdots t_{i+1}\phi + \psi \quad \text{for some } \phi \in \mathcal{O}_P \text{ and } \psi \in (f_1, f_2)_P,$$

so $t_1t_2 \cdots t_i(1 - t_{i+1}\phi) = \psi \in (f_1, f_2)_P$. But $(1 - t_{i+1}\phi)(P) = 1$, so we have $(1 - t_{i+1}\phi)^{-1} \in \mathcal{O}_P$. Hence

$$t_1t_2 \cdots t_r = \psi t_{i+1} \cdots t_r(1 - t_{i+1}\phi)^{-1} \in (f_1, f_2)_P$$

as claimed.)

(3.5) Let $P \in C_1 \cap C_2 \cap \mathbb{A}^2$, and let $\phi \in \mathcal{O}_P$. Show that there exists a polynomial $g \in R$ such that

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

and

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

*(Idea. The inequalities (A) and (B) that we already proved show that only a finite number of points are involved here, in fact, at most $n_1n_2$ points. Hence, ...
by (1.1), there is a polynomial $h = h(x, y) \in R$ such that $h(P) = 1$ and $h(Q) = 0$ for all $Q \neq P$ with $Q \in C_1 \cap C_2 \cap \mathbb{A}^2$. This means that $h^{-1} \in \mathcal{O}_P$ and $h \in M_Q$ for each of the other points $Q$. For integers $r \geq 1$ we have $h^{-r} \in \mathcal{O}_P$, and if $r$ is sufficiently large, then (3.4) tells us that $h^{-r} \in (f_1, f_2)_P$ for the other points $Q$. By (3.2) there is a polynomial $f \in R$ such that $f \equiv \phi h^{-r} \pmod{(f_1, f_2)_P}$. Then $g = fh^r$ solves the problem.)

(3.6) Show that the natural map

$$
R \longrightarrow \prod_{P \in C_1 \cap C_2 \cap \mathbb{A}^2} \mathcal{O}_P/(f_1, f_2)_P, \quad (\star)
$$

is surjective, and conclude that the inequality $(A^+)$ holds. (Idea. Let $J$ be the kernel of the map (\star). Then $(f_1, f_2) \subset J$, so $\dim(R/(f_1, f_2)) \geq \dim(R/J)$. The surjectivity of the map follows easily from (3.5) and implies that

$$
\dim R/J = (\text{dimension of the target space}) = \sum_P \dim \left( \mathcal{O}_P/(f_1, f_2)_P \right) = \sum_P I(C_1 \cap C_2, P).)
$$

To prove that $(A^+)$ is an equality is now seen to be the same as showing that the kernel $J$ of the map (\star) is equal to $(f_1, f_2)$. So we must show that $J \subset (f_1, f_2)$, the other inclusion being obvious. Let $f \in J$. Our strategy for showing that $f \in (f_1, f_2)$ is to consider the set

$$
L = \{ g \in R : gf \in (f_1, f_2) \}
$$

and to prove that $1 \in L$.

(4.1) Show that $L$ is an ideal in $R$ and that $(f_1, f_2) \subset L \subset R$.

(4.2) Show that $L$ has the following property:

For every $P \in \mathbb{A}^2$ there is a polynomial $g \in L$ such that $g(P) \neq 0$. (**) In fact, property (**) alone implies that $1 \in L$ by the famous Nullstellensatz of Hilbert. But we don’t need the Nullstellensatz in full generality, because we have an additional piece of information about $L$, namely that $(f_1, f_2) \subset L$, and hence $\dim(R/L)$ is finite. Using this, and assuming that $1 \notin L$ in order to prove a contradiction, verify the following assertion.
(4.3) There is an $a \in k$ such that $1 \notin L + R(x - a)$. (Idea. The powers of $x$ cannot all be linearly independent modulo $L$, so there are constants $c_i \in k$ and an integer $n$ such that $x^n + c_1x^{n-1} + \cdots + c_n \in L$. Since $k$ is algebraically closed, we can write this as $(x - a_1)(x - a_2) \cdots (x - a_n) \in L$ with suitable $a_i \in k$. Show that if $1 \notin L + R(x - a_i)$ for all $i = 1, \ldots, n$, then we get a contradiction to the assumption that $1 \notin L$.)

(4.4) There is a $b \in k$ such that $1 \notin L + R(x - a) + R(y - b)$. (Idea. Replace $L$ by $L + R(x - a)$ and $x$ by $y$ and repeat the argument of (4.3).)

(4.5) Let $P = (a, b)$ and show that $g(P) = 0$ for all $g \in L$. This contradicts (4.2) and shows that $1 \in L$. (Idea. Write $g(x, y) = g(a + (x - a), b + (y - b)) = g(a, b) + g_1(x, y)(x - a) + g_2(x, y)(y - b)$ and conclude that $g(a, b) \in L$.)

Our next job is to describe $K, \mathcal{O}_P, \mathcal{M}_P$, and $(f_1, f_2)_P$ in terms of homogeneous coordinates, so that they make sense also for points $P$ at infinity. This will allow us to check that they are invariant under arbitrary projective coordinate change in $\mathbb{P}^2$. To see what to do we put as usual $x = X/Z$ and $y = Y/Z$, and we view $R = k[x, y] = k[X/Z, Y/Z]$ as a subring of the field $k(X, Y, Z)$ of rational functions of $X, Y, Z$. Then $K = k(x, y)$ becomes identified with the set of all rational functions $\Phi = F/G$ of $X, Y, Z$ that are homogeneous of degree 0 in the sense that $F$ and $G$ are homogeneous polynomials of the same degree. Indeed, for $\phi \in K$, we have

$$\phi(x, y) = \frac{f(x, y)}{g(x, y)} = \frac{Z^n f(X/Z, Y/Z)}{Z^n g(X/Z, Y/Z)} = \frac{F(X, Y, Z)}{G(X, Y, Z)} = \Phi(X, Y, Z),$$

say, where $F$ and $G$ are homogeneous of the same degree

$$n = \max\{\deg f, \deg g\}.$$

On the other hand, if $\Phi = F/G$ is a quotient of forms of the same degree, then $\Phi(tX, tY, tZ) = \Phi(X, Y, Z)$, and

$$\Phi(X, Y, Z) = \Phi(x, y, 1) = \frac{F(x, y, 1)}{G(x, y, 1)} \in K.$$

If $P = [A, B, C]$ is a point in $\mathbb{P}^2$ and $\Phi = F/G \in K$, then we say that $\Phi$ is defined at $P$ if $G(A, B, C) \neq 0$, i.e., if $P$ is not on the curve $G(X, Y, Z) = 0$. If $\Phi$ is defined at $P$, we put $\Phi(P) = F(A, B, C)/G(A, B, C)$, where this
ratio is independent of the homogeneous coordinate triple for $P$. Clearly we should put

$$\mathcal{O}_P = \{ \Phi \in K : \Phi \text{ is defined at } P \},$$
$$\mathcal{M}_P = \{ \Phi \in \mathcal{O}_P : \Phi(P) = 0 \}.$$ 

We leave it to the conscientious reader to check the following assertion.

(5.1) If $P = (a, b) = [a, b, 1] \in \mathbb{A}^2$, then these definitions of $\mathcal{O}_P$, of $\Phi(P)$ for $\Phi \in \mathcal{O}_P$, and of $\mathcal{M}_P$ coincide with our earlier definitions.

Now let $C_1 : F_1 = 0$ and $C_2 : F_2 = 0$ be two curves in $\mathbb{P}^2$ without any common components. Let $f_1(x, y) = F_1(x, y, 1)$ and $f_2(x, y) = F_2(x, y, 1)$ be the polynomials defining their affine parts. Define

$$(F_1, F_2)_P = \{ F/G \in \mathcal{O}_P : F \text{ is of the form } F = H_1 F_1 + H_2 F_2 \}.$$ 

(Do you see why we cannot just say that $(F_1, F_2)_P$ is the ideal in $\mathcal{O}_P$ generated by $F_1$ and $F_2$?)

(5.2) Check that if $P \in \mathbb{A}^2$, then $(F_1, F_2)_P = (f_1, f_2)_P$ is the ideal in $\mathcal{O}_P$ generated by $f_1$ and $f_2$.

Of course, we now define the intersection multiplicity of $C_1$ and $C_2$ at a point $P \in \mathbb{P}^2$ by

$$I(C_1 \cap C_2, P) = \dim \left( \mathcal{O}_P / (F_1, F_2)_P \right).$$

We know from (5.2) that this coincides with our earlier definition for $P \in \mathbb{A}^2$.

(5.3) Check that the definitions of $\mathcal{O}_P$ and $(F_1, F_2)_P$, and hence also of the intersection multiplicity $I(C_1 \cap C_2, P)$, are independent of our choice of homogeneous coordinates in $\mathbb{P}^2$, i.e., they are invariant under a linear change of the coordinates $X, Y, Z$.

To finally complete our proof of Bezout’s theorem, we must show that there is a line $L$ in $\mathbb{P}^2$ that does not meet $C_1 \cap C_2$. Then we can take a new coordinate system in which $L$ is the line at infinity, and thereby reduce to the case already proved. To show that $L$ exists we use the following:

(5.4) Prove that given any finite set $S$ of points in $\mathbb{P}^2$, there is a line $L$ not meeting $S$. (Idea. Use that an algebraically closed field $k$ is not finite.)

Finally, the next result allows us to apply (5.4).

(5.5) Prove that $C_1 \cap C_2$ is finite. (Idea. Use the fact that for every line $L$ that is not a component of either $C_1$ or $C_2$, we know, by putting $L$ at infinity and
using part (1) of this proof, that \( C_1 \cap C_2 \) contains a finite number of points not on \( L \).

This completes our proof of Bezout’s Theorem in all its gory detail. To study more closely the properties of the intersection multiplicity \( I(C_1 \cap C_2, P) \) at one point \( P \), we may without loss of generality choose coordinates so that \( P = (0, 0) = [0, 0, 1] \) is the origin in the affine plane, and we can work with affine coordinates \( x, y \). Let \( R = k[x, y] \) as before, and let

\[
\mathcal{M} = \{ f = f(x, y) \in R : f(P) = f(0, 0) = 0 \}.
\]

(6.1) Prove that \( \mathcal{M} = (x, y) = Rx + Ry \) and that \( \mathcal{M}_P = \mathcal{O}_P x + \mathcal{O}_P y \).

It follows that for each \( n \geq 1 \), \( \mathcal{M}^n \) is the ideal in \( R \) generated by the monomials \( x^n, x^{n-1}y, \ldots, xy^{n-1}, y^n \). Hence every polynomial \( f \in R \) can be written uniquely as a polynomial of degree at most \( n \) plus a remainder polynomial \( r \in \mathcal{M}^{n+1} \). Thus

\[
f(x, y) = c_{00} + c_{10}x + c_{01}y + \cdots + c_{ij}x^i y^j + \cdots
+ c_{n0}x^n + c_{n-1,1}x^{n-1}y + \cdots + c_{0n}y^n + r. \quad (*)
\]

(6.2) Prove that every \( \phi = f/g \in \mathcal{O}_P \) can be written uniquely in the form \((*)\) with \( c_{ij} \in k \) and \( r \in \mathcal{M}_P^{n+1} \). In other words, the inclusion \( R \subset \mathcal{O}_P \) induces an isomorphism \( R/\mathcal{M}_P^{n+1} \cong \mathcal{O}_P/\mathcal{M}_P^{n+1} \) for every \( n \geq 0 \). (Idea. We must show that \( \mathcal{O}_P = R + \mathcal{M}_P^{n+1} \) and that \( R \cap \mathcal{M}_P^{n+1} = \mathcal{M}_P^{n+1} \). For the first, show that every \( \phi \in \mathcal{O}_P \) can be written in the form \( \phi = f/(1 - h) \) with \( f \in R \) and \( h \in \mathcal{M} \). Hence

\[
\phi = \frac{f}{1 - h} = f \cdot (1 + h + \cdots + h^n) + \frac{fh^{n+1}}{1 - h} \in R + \mathcal{M}_P^{n+1}.
\]

The second reduces to showing that if \( gf \in \mathcal{M}_P^n \) and \( g(P) \neq 0 \), then \( f \in \mathcal{M}_P^n \). This can be done by considering the terms of lowest degree in \( g \) and \( f \) and \( gf \).

Now we can already compute some intersection indices to see if our definitions give answers that are geometrically reasonable. As a matter of notation, we introduce the symbol

\[
I(f_1, f_2) = \dim \left( \mathcal{O}_P/(f_1, f_2)_P \right)
\]

for the intersection multiplicity of two curves \( f_1 = 0 \) and \( f_2 = 0 \) at the origin.

(6.3) Check that the curve \( y = x^n \) and the \( x \)-axis intersect with multiplicity \( n \) at the origin, i.e., show that \( I(y - x^n, y) = n \). (Idea. Note first that the ideals...
(y - x^n, y) and (x^n, y) are equal, and that this ideal contains \( M^n \). Then, using what we know from (6.2) about \( \mathcal{O}_P/M^n_P \), show that 1, x, \ldots, x^{n-1} is a basis for the vector space \( \mathcal{O}_P/(x^n, y) \mathcal{O}_P \).

(6.4) (Nakayama’s Lemma) Suppose that \( J \) is an ideal of \( \mathcal{O}_P \) contained in a finitely generated ideal \( \Phi = (\phi_1, \phi_2, \ldots, \phi_m) \mathcal{O}_P \). Suppose some elements of \( J \) generate \( \Phi \) modulo \( M_P \Phi \), i.e., \( \Phi = J + M_P \Phi \). Then \( J = \Phi \). (Idea. The case \( \Phi = (\phi_1, \phi_2) \mathcal{O}_P \) is all that we need. To prove that case, write \( \phi_1 = j_1 + \alpha \phi_1 + \beta \phi_2 \) and \( \phi_2 = j_2 + \gamma \phi_1 + \delta \phi_2 \), with \( j_1, j_2 \in J \) and \( \alpha, \beta, \gamma, \delta \in M_P \). Then use the fact that the determinant of the matrix \[
\begin{pmatrix}
1 - \alpha \\ \gamma \\
\beta \\ 1 - \delta
\end{pmatrix}
\] is non-zero in order to express the \( \phi \)'s in terms of the \( j \)'s.)

(6.5) Suppose that \[
f_1 = ax + by + \text{(higher terms)} \quad \text{and} \quad f_2 = cx + dy + \text{(higher terms)},
\] where “higher terms” means elements of \( M^2 \). Show that the following are equivalent.

(i) The curves \( f_1 = 0 \) and \( f_2 = 0 \) meet transversally at the origin, i.e., are smooth with distinct tangent directions there.

(ii) The determinant \( ad - bc \) is not equal to zero.

(iii) \( (f_1, f_2)_P = M_P \), i.e., \( I(f_1, f_2) = 1 \).

(Idea. (i) \( \iff \) (ii) follows directly from the definitions. One way to do (ii) \( \implies \) (iii) is to use (6.4) with \( \phi_1 = x \), \( \phi_2 = y \), and \( J = (f_1, f_2)_P \). To do (iii) \( \implies \) (ii), note that if \( ad - bc = 0 \), then
\[
\dim \left( \frac{(f_1, f_2)_P + M^2_P}{M^2_P} \right) \leq 1,
\]
whereas, by (6.2), \( \dim(M_P/M^2_P) = 2 \).

(6.6) Let \( f(x, y) \in \mathbb{R} \). Show that \( I(f(x, y), y) = m \), where \( x^m \) is the highest power of \( x \) dividing \( f(x, 0) \). (Idea. Use the fact that the ideal \( f(x, y) \) is the same as the ideal \( f(x, 0) \). Then argue as in (6.3).)

(6.7) Let \( C : F(X, Y, Z) = 0 \) be a curve in \( \mathbb{P}^2 \) that does not contain the line \( L_\infty : Z = 0 \). Show that for each point \( Q \in [a, b, 0] \in L_\infty \), we have \( I(C \cap L_\infty, Q) = m \), where \((bX - aY)^m \) is the highest power of \((bZ - aY)\) dividing \( F(X, Y, 0) \). (Idea. Make a suitable coordinate change to reduce to (6.6).)
A.5 Reduction Modulo $p$

Let $\mathbb{P}^2(\mathbb{Q})$ denote the set of rational points in $\mathbb{P}^2$. We say that a homogeneous coordinate triple $[A, B, C]$ is normalized if $A, B, C$ are integers with no common factors. Each point $P \in \mathbb{P}^1(\mathbb{Q})$ has a normalized coordinate triple that is unique up to sign. To obtain it we start with any triple of rational coordinates, multiply through by a common denominator, and then divide the resulting triple of integers by their greatest common divisor. For example,

$$\left[\frac{4}{5}, -\frac{2}{3}, 2\right] = [12, -10, 30] = [6, -5, 15].$$

The other normalized coordinate triple for this point is $[-6, 5, -15]$.

Let $p$ be a fixed prime number, and for each integer $m \in \mathbb{Z}$, let $\tilde{m} \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ denote its residue modulo $p$. If $[l, m, n]$ is a normalized coordinate triple for a point $P \in \mathbb{P}^2(\mathbb{Q})$, then the triple $[\tilde{l}, \tilde{m}, \tilde{n}]$ defines a point $\tilde{P}$ in $\mathbb{P}^2(\mathbb{F}_p)$, since at least one of the three numbers $l, m, n$ is not divisible by $p$. Since $P$ determines the triple $[l, m, n]$ up to sign, the point $\tilde{P}$ depends only on $P$, not on the choice of coordinates for $P$. Thus $P \mapsto \tilde{P}$ gives a well-defined map

$$\mathbb{P}^2(\mathbb{Q}) \longrightarrow \mathbb{P}^2(\mathbb{F}_p),$$

called for obvious reasons the reduction mod $p$ map. Note that reduction mod $p$ does not map $\mathbb{A}^2(\mathbb{Q})$ to $\mathbb{A}^2(\mathbb{F}_p)$. For example,

$$P = \left(\frac{1}{p}, 0\right) = \left[\frac{1}{p}, 0, 1\right] = [1, 0, p] \longrightarrow [\overline{1}, \overline{0}, \overline{p}] = [1, 0, 0] \notin \mathbb{A}^2(\mathbb{F}_p).$$

In fact, if $P = (a, b) = [a, b, 1] \in \mathbb{A}^2(\mathbb{Q})$, then its reduction $\tilde{P}$ is in $\mathbb{A}^2(\mathbb{F}_p)$ if and only if the rational numbers $a$ and $b$ are $p$-integral, i.e., have denominators that are prime to $p$.

Let $C : F(X, Y, Z) = 0$ be a rational curve in $\mathbb{P}^2$. By rational we mean as usual that the coefficients of $F$ are rational numbers. Clearing the denominators of the coefficients and then dividing by the greatest common divisor of their numerators, we may suppose that the coefficients of $F$ are integers with greatest common divisor one. Call such an $F$ normalized. Then $\tilde{F}$, the polynomial that we obtain by reducing the coefficients of $F$ modulo $p$, is non-zero and defines a curve $\tilde{C}$ in characteristic $p$. If $[l, m, n]$ is a normalized coordinate triple and if $F(l, m, n) = 0$, then $\tilde{F}(\tilde{l}, \tilde{m}, \tilde{n}) = 0$, because $x \rightarrow \tilde{x}$ is a homomorphism. In other words, if $P$ is a rational point on $C$, then $\tilde{P}$ is a point on $\tilde{C}$, so reduction mod $p$ takes $C(\mathbb{Q})$ and maps it into $C(\mathbb{F}_p)$. 
If $C_1$ and $C_2$ are curves, it follows that

$$\widehat{(C_1(\mathbb{Q}) \cap C_2(\mathbb{Q}))} \subset \widehat{C_1}(\mathbb{F}_p) \cap \widehat{C_2}(\mathbb{F}_p).$$

Is there some sense in which $\widehat{(C_1 \cap C_2)} = \widehat{C_1} \cap \widehat{C_2}$ if we count multiplicities? After all, the degrees of the reduced curves $\widehat{C_i}$ are the same as those of the $C_i$, so by Bezout’s theorem the intersection before and after reduction has the same number of points if we count multiplicities. But Bezout’s theorem requires that the ground field be algebraically closed, and we don’t have the machinery to extend our reduction mod $p$ map to that case. However, if we assume that all of the complex intersection points are rational, then everything is okay. We treat only the special case in which one of the curves is a line. This case suffices for the application to elliptic curves that we are after, and it is easy to prove.

**Proposition A.5.** Suppose that $C$ is a rational curve and $L$ is a rational line in $\mathbb{P}^2$. Suppose that all of the complex intersection points of $C$ and $L$ are rational. Let $C \cap L = \{P_1, P_2, \ldots, P_d\}$, where $d = \deg(C)$ and each $P_i$ is repeated in the list as many times as its multiplicity. Assume that $\tilde{L}$ is not a component of $\tilde{C}$. Then $\tilde{C} \cap \tilde{L} = \{\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_d\}$ with the correct multiplicities.

**Proof.** Suppose first that $L$ is the line at infinity $Z = 0$. Let $F(X, Y, Z) = 0$ be a normalized equation for $C$. The assumption that $\tilde{L}$ is not a component of $\tilde{C}$ means that $\tilde{F}(X, Y, 0) \neq 0$, i.e., some coefficient of $F(X, Y, 0)$ is not divisible by $p$. For each intersection point $P_i$, let $P_i = [l_i, m_i, 0]$ in normalized coordinates. Then

$$F(X, Y, 0) = c \prod_{i=1}^{d} (m_i X - l_i Y) \quad (*)$$

for some constant $c$. This is true because the intersection points of a curve $F = 0$ with the line $Z = 0$ correspond, with the correct multiplicities, to the linear factors of $F(X, Y, 0)$. Since each of the linear polynomials on the right of $(*)$ is normalized and since some coefficient of $F$ is not divisible by $p$, we see that $c$ must be an integer that is not divisible by $p$. Therefore we can reduce $(*)$ modulo $p$ to obtain

$$\tilde{F}(X, Y, 0) = \tilde{c} \prod_{i=1}^{d} (\tilde{m}_i X - \tilde{l}_i Y), \quad (\tilde{*})$$

which shows that $\tilde{C} \cap \tilde{L} = \{\tilde{P}_1, \tilde{P}_2, \ldots, \tilde{P}_d\}$ as claimed.
What if the line $L$ is not the line $Z = 0$. Then we just make a linear change of coordinates
\[
\begin{pmatrix}
X' \\
Y' \\
Z'
\end{pmatrix} = \begin{pmatrix} n_{11} & n_{12} & n_{13} \\
n_{21} & n_{22} & n_{23} \\
n_{31} & n_{32} & n_{33}
\end{pmatrix}
\begin{pmatrix}
X \\
Y \\
Z
\end{pmatrix}
\]
so that $L$ is the line $Z' = 0$ in the new coordinate system.

Is that all there is to it? No, we must be careful to make sure that our change of coordinates is compatible with reduction modulo $p$. This is not true for general changes with $n_{ij} \in \mathbb{Q}$. However, if we change using a matrix $(n_{ij})$ with integer entries and determinant 1, then the inverse matrix $(m_{ij})$ will have integer entries, and the reduced matrices $(\tilde{n}_{ij})$ and $(\tilde{m}_{ij})$ are inverses giving the corresponding coordinate change in characteristic $p$. And clearly if we change coordinates with $(n_{ij})$ and reduce mod $p$, the result will be the same as if we first reduce mod $p$ and then change coordinates with $(\tilde{n}_{ij})$.

Thus, to complete our proof we must show that for every rational line in $\mathbb{P}^2$ there is an “integral” coordinate change such that in the new coordinates, the line $L$ is the line at infinity. To do this, we let

\[
L : aX + bY + cZ = 0
\]

be a normalized equation for the line $L$ and use the following result.

**Lemma A.6.** Let $(a, b, c)$ be a triple of integers satisfying $\gcd(a, b, c) = 1$. Then there exists a $3 \times 3$ matrix with integer coefficients, determinant 1, and bottom line $(a, b, c)$.

**Proof.** Let $d = \gcd(b, c)$, choose integers $r$ and $s$ such that $rc - sb = d$, and note for later use that $r$ and $s$ are necessarily relatively prime. Now $\gcd(a, d) = 1$, so we can choose $t$ and $u$ such that $td + ua = 1$. Finally, since $\gcd(r, s) = 1$, we can choose $v$ and $w$ such that $vs - wr = u$. Then the matrix
\[
\begin{pmatrix}
t & v & w \\
0 & r & s \\
a & b & c
\end{pmatrix}
\]
has the desired properties. \qed

Using Lemma A.6 completes the proof of Proposition A.5. \qed

Finally, we apply Proposition A.5 to show that the reduction mod $p$ map respects the group law on a cubic curve.
Corollary A.7. Let $C$ be a non-singular rational cubic curve in $\mathbb{P}^2$ and let $O$ be a rational point on $C$, which we take as the origin for the group law on $C$. Suppose that $\tilde{C}$ is non-singular and take $\tilde{O}$ as the origin for the group law on $\tilde{C}$. Then the reduction mod $p$ map $P \mapsto \tilde{P}$ is a group homomorphism $C(\mathbb{Q}) \to \tilde{C}(\mathbb{F}_p)$.

Proof. Let $P, Q \in C(\mathbb{Q})$, and let $R = P + Q$. This means that there are lines $L_1$ and $L_2$ and a rational point $S \in C(\mathbb{Q})$ such that, in the notation of Proposition A.5,

$$C \cap L_1 = \{P, Q, S\} \quad \text{and} \quad C \cap L_2 = \{S, O, R\}.$$ 

Putting tildes on everything, which is allowed by the proposition, we conclude that $\tilde{P} + \tilde{Q} = \tilde{R}$. \qed

Exercises

A.1. Let $\mathbb{P}^2$ be the set of homogeneous triples $[a, b, c]$ as usual, and recall that with this definition a line in $\mathbb{P}^2$ is defined to be the set of solutions of an equation of the form

$$\alpha X + \beta Y + \gamma Z = 0$$

for some numbers $\alpha, \beta, \gamma$ not all zero.

(a) Prove directly from this definition that any two distinct points in $\mathbb{P}^2$ are contained in a unique line.

(b) Similarly, prove that any two distinct lines in $\mathbb{P}^2$ intersect in a unique point.

A.2. Let $K$ be a field, for example $K$ might be the rational numbers or the real numbers or a finite field. Define a relation $\sim$ on $(n+1)$-tuples $[a_0, a_1, \ldots, a_n]$ of elements of $K$ by the following rule:

$$[a_0, a_1, \ldots, a_n] \sim [a'_0, a'_1, \ldots, a'_n] \quad \text{if there is a non-zero } t \in K$$

so that $a_0 = ta'_0, a_1 = ta'_1, \ldots, a_n = ta'_n$.

(a) Prove that $\sim$ is an equivalence relation. That is, prove that for any $(n+1)$-tuples $a = [a_0, a_1, \ldots, a_n], b = [b_0, b_1, \ldots, b_n]$, and $c = [c_0, c_1, \ldots, c_n]$, the relation $\sim$ satisfies the following three conditions:

(i) $a \sim a$ (Reflexive)
(ii) $a \sim b \implies b \sim a$ (Symmetric)
(iii) $a \sim b$ and $b \sim c \implies a \sim c$ (Transitive)

(b) Which of these properties (i), (ii), (iii) fails to be true if $K$ is replaced by a ring $R$ that is not a field? (There are several answers to this question, depending on what the ring $R$ looks like.)
A.3. We saw in Section A.1 that the directions in the affine plane \( \mathbb{A}^2 \) correspond to the points of the projective line \( \mathbb{P}^1 \). In other words, \( \mathbb{P}^1 \) can be described as the set of lines in \( \mathbb{A}^2 \) going through the origin.

(a) Prove similarly that \( \mathbb{P}^2 \) can be described as the set of lines in \( \mathbb{A}^3 \) going through the origin.

(b) Let \( \Pi \subset \mathbb{A}^3 \) be a plane in \( \mathbb{A}^3 \) that goes through the origin, and let \( S_{\Pi} \) be the collection of lines in \( \mathbb{A}^3 \) going through the origin and contained in \( \Pi \). From (a), \( S_{\Pi} \) defines a subset \( L_{\Pi} \) of \( \mathbb{P}^2 \). Prove that \( L_{\Pi} \) is a line in \( \mathbb{P}^2 \), and conversely that every line in \( \mathbb{P}^2 \) can be constructed in this way.

(c) Generalize (a) by showing the \( \mathbb{P}^n \) can be described as the set of lines in \( \mathbb{A}^{n+1} \) going through the origin.

A.4. Let \( F(X, Y, Z) \in \mathbb{C}[X, Y, Z] \) be a homogeneous polynomial of degree \( d \).

(a) Prove that the three partial derivatives of \( F \) are homogeneous polynomials of degree \( d - 1 \).

(b) Prove that
\[
X \frac{\partial F}{\partial X} + Y \frac{\partial F}{\partial Y} + Z \frac{\partial F}{\partial Z} = d \cdot F(X, Y, Z).
\]

(Hint. Differentiate \( F(tX, tY, tZ) = t^d F(X, Y, Z) \) with respect to \( t \).)

A.5. Let \( C : F(X, Y, Z) = 0 \) be a projective curve given by a homogeneous polynomial \( F \in \mathbb{C}[X, Y, Z] \), and let \( P \in \mathbb{P}^2 \) be a point.

(a) Prove that \( P \) is a singular point of \( C \) if and only if
\[
\frac{\partial F}{\partial X}(P) = \frac{\partial F}{\partial Y}(P) = \frac{\partial F}{\partial Z}(P) = 0.
\]

(b) If \( P \) is a non-singular point of \( C \), prove that the tangent line to \( C \) at \( P \) is given by the equation
\[
\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0.
\]

A.6. Let \( C \) be the projective curve given by the equation
\[
C : Y^2 Z - X^3 - Z^3 = 0.
\]

(a) Show that \( C \) has only one point at infinity, namely the point \([0, 1, 0]\) corresponding to the vertical direction \( x = 0 \).

(b) Let \( C_0 : y^2 - x^3 - 1 = 0 \) be the affine part of \( C \), and let \((r_i, s_i)\) be a sequence of points on \( C_0 \) with \( r_i \to \infty \). Let \( L_i \) be the tangent line to \( C_0 \) at the point \((r_i, s_i)\). Prove that as \( i \to \infty \), the slopes of the lines \( L_i \) approach infinity, i.e., they approach the slope of the line \( x = 0 \).

A.7. Let \( f(x, y) \) be a polynomial.

(a) Expand \( f(tx, ty) \) as a polynomial in \( t \) whose coefficients are polynomials in \( x \) and \( y \). Prove that the degree of \( f(tx, ty) \), considered as a polynomial in the variable \( t \), is equal to the degree of the polynomial \( f(x, y) \).
(b) Prove that the homogenization $F(X, Y, Z)$ of $f(x, y)$ is given by

$$F(X, Y, Z) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right), \quad \text{where } d = \deg(f).$$

A.8. For each of the given affine curves $C_0$, find a projective curve $C$ whose affine part is $C_0$. Then find all of the points at infinity on the projective curve $C$.

(a) $C_0 : 3x - 7y + 5 = 0.$
(b) $C_0 : x^2 + xy - 2y^2 + x - 5y + 7 = 0.$
(c) $C_0 : x^3 + x^2 y - 3xy^2 - 3y^3 + 2x^2 - 2 + 5 = 0.$

A.9. For each of the following curves $C$ and points $P$, either find the tangent line to $C$ at $P$ or else verify that $C$ is singular at $P$.

(a) $C : y^2 = x^3 - x, \quad P = (1, 0).$
(b) $C : X^2 + Y^2 = Z^2, \quad P = [3, 4, 5].$
(c) $C : x^2 + y^4 + 2xy + 2x + 2y + 1 = 0, \quad P = (-1, 0).$
(d) $C : X^3 + Y^3 + Z^3 = XYZ, \quad P = [1, -1, 0].$

A.10. (a) Prove that a projective transformation of $\mathbb{P}^2$ sends lines to lines.
(b) More generally, prove that a projective transformation of $\mathbb{P}^2$ sends curves of degree $d$ to curves of degree $d$.

A.11. Let $P, P_1, P_2, P_3$ be points in $\mathbb{P}^2$, and let $L$ be a line in $\mathbb{P}^2$.

(a) If $P_1, P_2,$ and $P_3$ do not lie on a line, prove that there is a projective transformation of $\mathbb{P}^2$ so that

$$P_1 \mapsto [0, 0, 1], \quad P_2 \mapsto [0, 1, 0], \quad P_3 \mapsto [1, 0, 0].$$

(b) If no three of $P_1, P_2, P_3,$ and $P$ lie on a line, prove that there is a unique projective transformation as in (a) that also sends $P$ to $[1, 1, 1]$.

(c) Prove that there is a projective transformation of $\mathbb{P}^2$ so that $L$ is sent to the line $Z' = 0$.

(d) More generally, if $P$ does not lie on $L$, prove that there is a projective transformation of $\mathbb{P}^2$ so that $L$ is sent to the line $Z' = 0$ and $P$ is sent to the point $[0, 0, 1]$.

A.12. For each of the pairs of curves $C_1, C_2$, find all of the points in the intersection $C_1 \cap C_2$. Be sure to include points with complex coordinates and points at infinity.

(a) $C_1 : x - y = 0, \quad C_2 : x^2 - y = 0.$
(b) $C_1 : x - y - 1 = 0, \quad C_2 : x^2 - y^2 + 2 = 0.$
(c) $C_1 : x - y - 1 = 0, \quad C_2 : x^2 - 2y^2 - 5 = 0.$
(d) $C_1 : x - 2 = 0, \quad C_2 : y^2 - x^3 + 2x = 0.$

A.13. For each of the pairs of curves $C_1, C_2$, compute the intersection index $I(C_1 \cap C_2, P)$ at the indicated point $P$. Also sketch the curves and the point in $\mathbb{R}^2.$
Exercises

A.14. Let \( C^{(d)} \) be the collection of curves of degree \( d \) in \( \mathbb{P}^2 \).

(a) Show that \( C^{(d)} \) is naturally isomorphic to the projective space \( \mathbb{P}^N \) for a certain value of \( N \), and find \( N \) explicitly in terms of \( d \).

(b) In Section A.3 we gave a plausibility argument for why the Cayley–Bacharach theorem is true for curves of degree \( d \). Give a similar argument for general curves \( C_1, C_2, \) and \( D \) of degrees \( d_1, d_2, \) and \( d_1 + d_2 - 3 \), respectively.

A.15. Let \( P \in \mathbb{A}^2 \). In this exercise we ask you to verify various properties of \( \mathcal{O}_P \), the local ring at \( P \), as defined in Section A.4.

(a) Prove that \( \mathcal{O}_P \) is a subring of \( K = k(x, y) \).

(b) Prove that the map \( \phi \mapsto \phi(P) \) is a homomorphism of \( \mathcal{O}_P \) onto \( k \). Let \( \mathcal{M}_P \) be the kernel of this homomorphism.

(c) Prove that \( \mathcal{O}_P \) equals the direct sum \( k + \mathcal{M}_P \).

(d) Prove that \( \phi \in \mathcal{O}_P \) is a unit if and only if \( \phi \notin \mathcal{M}_P \).

(e) Let \( I \subset \mathcal{O}_P \) be an ideal of \( \mathcal{O}_P \). Prove that either \( I = \mathcal{O}_P \), or else \( I \subset \mathcal{M}_P \).

Deduce that \( \mathcal{M}_P \) is the unique maximal ideal of \( \mathcal{O}_P \).

A.16. Let \( P_1, P_2, P_3, P_4, P_5 \) be five distinct points in \( \mathbb{P}^2 \).

(a) Show that there exists a conic \( C \), i.e., a curve of degree two, passing through the five points.

(b) Show that \( C \) is unique if and only if no four of the five points lie on a line.

(c) Show that \( C \) is irreducible if and only if no three of the five points lie on a line.

A.17. In this exercise we guide you in proving the cubic Cayley–Bacharach theorem in the case that the eight points are distinct. Let \( C_1 : F_1 = 0 \) and \( C_2 : F_2 = 0 \) be cubic curves in \( \mathbb{P}^2 \) without common component which have eight distinct points \( P_1, P_2, \ldots, P_8 \) in common. Suppose that \( C_3 : F_3 = 0 \) is a third cubic curve passing through these same eight points. Prove that \( C_3 \) is on the “line of cubics” joining \( C_1 \) and \( C_2 \), i.e., prove that there are constants \( \lambda_1 \) and \( \lambda_2 \) such that

\[
F_3 = \lambda_1 F_1 + \lambda_2 F_2.
\]

In order to prove this result, assume that no such \( \lambda_1, \lambda_2 \) exist and derive a contradiction as follows:

(i) Show that \( F_1, F_2, \) and \( F_3 \) are linearly independent.

(ii) Let \( P' \) and \( P'' \) be any two points in \( \mathbb{P}^2 \) different from each other and different from the \( P_i \). Show that there is a cubic curve passing through all ten points \( P_1, \ldots, P_8, P', P'' \). (Hint. Show that there exist constants \( \lambda_1, \lambda_2, \lambda_3 \) such that \( F = \lambda_1 F_1 + \lambda_2 F_2 + \lambda_3 F_3 \) is not identically zero and such that the curve \( F = 0 \) does the job.)
(iii) Show that no four of the eight points $P_i$ are collinear, and no seven of them lie on a conic. (Hint. Use the fact that $C_1$ and $C_2$ have no common component.)

(iv) Use the previous exercise to observe that there is a unique conic $Q$ going through any five of the eight points $P_1, \ldots, P_8$.

(v) Show that no three of the eight points $P_i$ are collinear. (Hint. If three are on a line $L$, let $Q$ be the unique conic going through the other five, choose $P'$ on $L$ and $P''$ not on $L$. Then use (ii) to get a cubic which has $L$ as a component, so is of the form $C = L \cup Q'$ for some conic $Q'$. This contradicts the fact that $Q$ is unique.)

(vi) To get the final contradiction, let $Q$ be the conic through the five points $P_1, P_2, \ldots, P_5$. By (iii), at least one (in fact two) of the remaining three points is not on $Q$. Call it $P_6$, and let $L$ be the line joining $P_7$ to $P_8$. Choose $P'$ and $P''$ on $L$ so that again the cubic $C$ through the ten points has $L$ as a component. Show that this gives a contradiction.

A.18. Show that if $C_1$ and $C_2$ are both singular at the point $P$, then their intersection index satisfies $I(C_1 \cap C_2, P) \geq 3$.

A.19. Consider the affine curve $C : y^4 - xy - x^3 = 0$. Show that at the origin $(x, y) = (0, 0)$, the curve $C$ meets the $y$-axis four times, the $x$-axis three times, and every other line through the origin twice.

A.20. Show that the separation of real conics into hyperbolas, parabolas, and ellipses is an affine business and has no meaning projectively, by giving an example of a quadratic homogeneous polynomial $F(X, Y, Z)$ with real coefficients such that:

- $F(x, y, 1) = 0$ is a hyperbola in the real $(x, y)$-plane,
- $F(x, 1, z) = 0$ is a parabola in the real $(x, z)$-plane,
- $F(1, y, z) = 0$ is an ellipse in the real $(y, z)$-plane.
Appendix B

Transformation to Weierstrass Form

We illustrate the transformation of a cubic equation to Weierstrass form, using the procedure described in Section 1.3, for the curve

\[ C : X^3 + 2Y^3 + 4Z^3 - 7XYZ = 0 \]

and the point \( O = [1, 1, 1] \).

Before starting, we observe that in general, the tangent line in \( \mathbb{P}^2 \) to a curve described by a homogeneous equation

\[ F(X, Y, Z) = 0 \]

at the point \( P_0 = [X_0, Y_0, Z_0] \in \mathbb{P}^2 \) is given by the homogeneous linear equation

\[ \frac{\partial F}{\partial X}(P_0)X + \frac{\partial F}{\partial Y}(P_0)Y + \frac{\partial F}{\partial Z}(P_0)Z = 0. \]

Looking at Figure 1.10, we see that a good first step is to move the point \( O \) to the point \( [1, 0, 0] \), so we make the substitution

\[ X_1 = X, \quad Y_1 = Y - X, \quad Z_1 = Z - X. \]

This transforms the equation for \( C \) into

\[ C : X_1^2Y_1 + 6X_1Y_1^2 + 2Y_1^3 + 5X_1^2Z_1 - 7X_1Y_1Z_1 + 12X_1Z_1^2 + 4Z_1^3 = 0. \]

The tangent line to \( C \) at \( O = [1, 0, 0] \) is \( Y_1 - 5Z_1 = 0 \), and according to Figure 1.10, we want this tangent line to be the line \( Z = 0 \). So we make the substitution
\[ X_2 = X_1, \quad Y_2 = Y_1, \quad Z_2 = Y_1 - 5Z_1, \]

which gives the equation
\[
C : 635X_2Y_2^2 + 254Y_2^3 - 125X_2^2Z_2 + 55X_2Y_2Z_2 - 12Y_2^2Z_2 \\
+ 60X_2Z_2^2 + 12Y_2Z_2^2 - 4Z_2^3 = 0.
\]

The tangent line at \( O = [1, 0, 0] \) is now the line \( Z_2 = 0 \). To find the other intersection point of this line with \( C \), we substitute \( Z_2 = 0 \) into the equation for \( C \). This leads to \( 127Y_2^2(5X_2 + 2Y_2) = 0 \), and thus the third intersection point is
\[
O^*O = [2, -5, 0].
\]

Again looking at Figure 1.10, we move this point to \([0, 1, 0]\) by making the substitution
\[
X_3 = 5X_2 + 2Y_2, \quad Y_3 = Y_2, \quad Z_3 = Z_2,
\]

which gives
\[
C : 127X_3Y_3^2 - 5X_3^2Z_3 + 31X_3Y_3Z_3 - 54Y_3^2Z_3 + 12X_3Z_3^2 \\
- 12Y_3Z_3^2 - 4Z_3^3 = 0.
\]

The tangent line to \( C \) at the point \([0, 1, 0]\) is now easily computed; it turns out to be \( 127X_3 - 54Z_3 = 0 \). A final look at Figure 1.10 shows that this line should be moved to \( X = 0 \), so we make the substitution (note that we want the line \( Z = 0 \) and the point \([1, 0, 0]\) to stay where they are)
\[
X_4 = 127X_3 - 54Z_3, \quad Y_4 = Y_3, \quad Z_4 = Z_3.
\]

This transforms \( C \) into
\[
C : 16129X_4Y_4^2 - 5X_4^2Z_4 + 3937X_4Y_4Z_4 + 984X_4Z_4^2 \\
+ 19050Y_4Z_4^2 + 32000Z_4^3 = 0.
\]

Don’t despair, we’re almost done. We dehomogenize using \( x_5 = X_4/Z_4 \) and \( y_5 = Y_4/Z_4 \) to get
\[
C : 3200 + 984x_5 - 5x_5^2 + 19050y_5 + 3937x_5y_5 + 16129x_5y_5^2 = 0.
\]

Next we multiply by \( x_5 \) and let \( x_6 = x_5 \) and \( y_6 = x_5y_5 \), which gives
\[
C : 3200x_6 + 984x_6^2 - 5x_6^3 + 19050y_6 + 3937x_6y_6 + 16129y_6^2 = 0.
\]
To make the coefficient of $x_6^3$ equal to 1 and the coefficient of $y_6^2$ equal to 4, we set $x_7 = 20x_6$ and $y_7 = 2540y_6 = 4 \cdot 5 \cdot 127y_6$ and obtain

$$C : 256000x_7 + 3936x_7^2 - x_7^3 + 12000y_7 + 124x_7y_7 + 4y_7^2 = 0.$$ 

Finally, we complete the square in $y_7$ by setting

$$x = x_7 \quad \text{and} \quad y = 2y_7 + 31x_7 + 3000,$$

which puts $C$ into Weierstrass form,\(^1\)

$$C : y^2 = x^3 - 2975x^2 - 70000x + 9000000.$$ 

Tracing through all of the substitutions, we find that the transformation taking the original equation

$$C : X^3 + 2Y^3 + 4Z^3 - 7XYZ = 0$$

to the Weierstrass equation is given by the formulas

$$x = \frac{100(33X + 40Y + 54Z)}{4X + Y - 5Z},$$

$$y = \frac{-63500(6X^2 - 7XY - 18Y^2 + 21XZ - 14YZ + 12Z^2)}{(4X + Y - 5Z)^2}.$$ 

\(^1\)The further substitution $(x, y) = (25x_0, 125y_0)$ gives an equation with smaller integer coefficients, $y_0^2 = x_0^3 - 119x_0^2 - 112x_0 + 576.$
# List of Notation

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$P * Q$</td>
<td>third intersection of $\overrightarrow{PQ}$ and cubic curve, 9</td>
</tr>
<tr>
<td>$\mathcal{O}$</td>
<td>specified base point on cubic curve, 11</td>
</tr>
<tr>
<td>$+$</td>
<td>addition on a cubic curve, 12</td>
</tr>
<tr>
<td>$-P$</td>
<td>inverse of point on cubic curve, 13</td>
</tr>
<tr>
<td>$C(\mathbb{Q})$</td>
<td>the rational points on a cubic curve, 39</td>
</tr>
<tr>
<td>$C(\mathbb{R})$</td>
<td>the real points on a cubic curve, 39</td>
</tr>
<tr>
<td>$C(\mathbb{C})$</td>
<td>the complex points on a cubic curve, 39</td>
</tr>
<tr>
<td>$g_2, g_3$</td>
<td>Eisenstein series, coefficients of Weierstrass equation, 41</td>
</tr>
<tr>
<td>$\wp$</td>
<td>Weierstrass $\wp$-function, 41</td>
</tr>
<tr>
<td>$\text{ord}(x)$</td>
<td>the $p$-adic order of a rational number $x$, 48</td>
</tr>
<tr>
<td>$C(p^n)$</td>
<td>points on $C$ with specified $p$-divisibility, 49</td>
</tr>
<tr>
<td>$R, R_p$</td>
<td>ring of integers localized at $p$, 50</td>
</tr>
<tr>
<td>$\text{Disc}(f)$</td>
<td>discriminant of the polynomial $f$, 60</td>
</tr>
<tr>
<td>$H(P)$</td>
<td>height of a point on a cubic curve, 66</td>
</tr>
<tr>
<td>$h(P)$</td>
<td>height of a point on a cubic curve, 66</td>
</tr>
<tr>
<td>$\Gamma$</td>
<td>notation for $C(\mathbb{Q})$, 80</td>
</tr>
<tr>
<td>$\overline{C}$</td>
<td>curve with degree two map $C \to \overline{C}$, 81</td>
</tr>
<tr>
<td>$\overline{\overline{C}}$</td>
<td>curve with degree two map $\overline{C} \to \overline{\overline{C}}$, 81</td>
</tr>
<tr>
<td>$\phi(\Gamma)$</td>
<td>the image of $\Gamma$ by $\phi$, 89</td>
</tr>
<tr>
<td>$\mathbb{Q}^*$</td>
<td>the multiplicative group of non-zero rational numbers, 91</td>
</tr>
<tr>
<td>$\mathbb{Q}^{*2}$</td>
<td>the group of squares of elements of $\mathbb{Q}^*$, 91</td>
</tr>
<tr>
<td>$\alpha$</td>
<td>a homomorphism $\Gamma \to \mathbb{Q}^*/\mathbb{Q}^{*2}$, 91</td>
</tr>
<tr>
<td>$\mathbb{Z}$</td>
<td>the group of integers, 95</td>
</tr>
<tr>
<td>$\mathbb{Z}_m$</td>
<td>the cyclic group $\mathbb{Z}/m\mathbb{Z}$, 95</td>
</tr>
<tr>
<td>$\Gamma[2]$</td>
<td>subgroup of $\Gamma$ of points of order dividing two, 96</td>
</tr>
<tr>
<td>$C_{\alpha s}$</td>
<td>non-singular points on a singular cubic curve, 107</td>
</tr>
<tr>
<td>$\mathbb{F}_q$</td>
<td>finite field with $q$ elements, 117</td>
</tr>
<tr>
<td>$C(\mathbb{F}_p)$</td>
<td>the points on the curve $C$ with coordinates in $\mathbb{F}_p$, 118</td>
</tr>
<tr>
<td>$R, S, T$</td>
<td>cosets of cubes in $\mathbb{F}_p^*$, 123</td>
</tr>
<tr>
<td>$[XYZ]$</td>
<td>number of solutions of $x + y + z = 0$, 123</td>
</tr>
<tr>
<td>$\zeta$</td>
<td>a $p$’th root of unity, 125</td>
</tr>
<tr>
<td>$\theta_p$</td>
<td>angle whose cosine is $(M_p - p - 1)/2\sqrt{p}$, 132</td>
</tr>
<tr>
<td>Notation</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>$\pi(X)$</td>
<td>number of primes $p \leq X$, 133</td>
</tr>
<tr>
<td>$\tilde{z}$</td>
<td>the image of $z$ in $\mathbb{F}_p$, 133</td>
</tr>
<tr>
<td>$\tilde{C}$</td>
<td>the curve $C$ with coefficients reduced mod $p$, 134</td>
</tr>
<tr>
<td>$\tilde{P}$</td>
<td>the reduction mod $p$ of a point in $C(\mathbb{Q})$, 134</td>
</tr>
<tr>
<td>$\Phi$</td>
<td>the subgroup of $C(\mathbb{Q})$ of points of finite order, 134</td>
</tr>
<tr>
<td>Taxi($N$)</td>
<td>the $N$’th taxicab number, 174</td>
</tr>
<tr>
<td>$\beta$</td>
<td>equals $\sqrt[3]{b}$ in proof of Thue’s theorem, 177</td>
</tr>
<tr>
<td>$|t|$</td>
<td>largest of the absolute values of the coordinates of $t$, 183</td>
</tr>
<tr>
<td>$[K : \mathbb{Q}]$</td>
<td>the degree of a field, 207</td>
</tr>
<tr>
<td>$\text{Aut}(K)$</td>
<td>automorphism group of a field, 208</td>
</tr>
<tr>
<td>$\text{Gal}(K/\mathbb{Q})$</td>
<td>Galois group of a field over $\mathbb{Q}$, 208</td>
</tr>
<tr>
<td>$\text{Aut}_F(K)$</td>
<td>group of automorphisms of $K$ fixing $F$, 210</td>
</tr>
<tr>
<td>$\text{Gal}(K/F)$</td>
<td>Galois group of automorphisms of $K$ fixing $F$, 210</td>
</tr>
<tr>
<td>$C(K)$</td>
<td>the set of $K$-rational points on the curve $C$, 213</td>
</tr>
<tr>
<td>$\lambda_n$</td>
<td>the multiplication-by-$n$ map on an elliptic curve, 217</td>
</tr>
<tr>
<td>$C[n]$</td>
<td>kernel of multiplication-by-$n$, 217</td>
</tr>
<tr>
<td>$\mathbb{Q}[C[n]]$</td>
<td>field of definition of $C[n]$, 222</td>
</tr>
<tr>
<td>$\text{GL}_r(R)$</td>
<td>general linear group with coefficients in the ring $R$, 224</td>
</tr>
<tr>
<td>$\rho_n$</td>
<td>representation on $n$-torsion, 225</td>
</tr>
<tr>
<td>$K_n$</td>
<td>the field $\mathbb{Q}(i)(C[n])$ for the curve $y^2 = x^3 + x$, 236</td>
</tr>
<tr>
<td>$E_{A,B,C}$</td>
<td>Frey curve $y^2 = x(x - A^n)(x + B^n)$, 246</td>
</tr>
<tr>
<td>$\tilde{E}_p$</td>
<td>the reduction of the elliptic curve modulo $p$, 247</td>
</tr>
<tr>
<td>$\Gamma(s)$</td>
<td>the classical $\Gamma$-function, 249</td>
</tr>
<tr>
<td>$\Gamma_0(N)$</td>
<td>a modular subgroup of $\text{SL}_2(\mathbb{Z})$, 251</td>
</tr>
<tr>
<td>$\mathbb{H}$</td>
<td>the complex upper half-plane, 251</td>
</tr>
<tr>
<td>$\text{Disc}(f)$</td>
<td>the discriminant of the polynomial $f$, 256</td>
</tr>
<tr>
<td>$\psi_n$</td>
<td>the $n$’th division polynomial of an elliptic curve, 257</td>
</tr>
<tr>
<td>$\text{End}(A)$</td>
<td>the endomorphism ring of the abelian group $A$, 258</td>
</tr>
<tr>
<td>$\mathbb{P}^2$</td>
<td>the projective plane, 267</td>
</tr>
<tr>
<td>$\mathbb{P}^n$</td>
<td>projective $n$-space, 267</td>
</tr>
<tr>
<td>$\mathbb{A}^2$</td>
<td>the affine plane, 268</td>
</tr>
<tr>
<td>$L_\infty$</td>
<td>the line at infinity in $\mathbb{P}^2$, 269</td>
</tr>
<tr>
<td>$\deg$</td>
<td>the degree of a polynomial, 274</td>
</tr>
<tr>
<td>$C(\mathbb{Q})$</td>
<td>the set of rational points on $C$, 276</td>
</tr>
<tr>
<td>$C_0(\mathbb{Z})$</td>
<td>set of integer points of $C_0$, 276</td>
</tr>
<tr>
<td>$C(3)$</td>
<td>the collection of all cubic curves in $\mathbb{P}^2$, 286</td>
</tr>
<tr>
<td>$\dim V$</td>
<td>dimension of a vector space, 291</td>
</tr>
<tr>
<td>$R$</td>
<td>the polynomial ring $k[x, y]$, 291</td>
</tr>
<tr>
<td>$\mathcal{O}_P$</td>
<td>local ring at $P$, 295</td>
</tr>
<tr>
<td>$I(C_1 \cap C_2, P)$</td>
<td>intersection index, 295</td>
</tr>
<tr>
<td>$\tilde{m}$</td>
<td>the image of $m$ in $\mathbb{F}_p$, 302</td>
</tr>
<tr>
<td>$\tilde{P}$</td>
<td>the image of the point $P$ in $\mathbb{P}^2(\mathbb{F}_p)$, 302</td>
</tr>
<tr>
<td>$C(d)$</td>
<td>the collection of all degree $d$ curves in $\mathbb{P}^2$, 308</td>
</tr>
</tbody>
</table>
References


[45] C.L. Siegel, The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$. J. Lond. Math. Soc. (2) 1, 66–68 (1926)


Index

A
abelian extension of \( \mathbb{Q}(i) \), 236
abelian Galois group, 211
abelian group
automorphism group, 258
domain, 258
finitely generated, 95
absolute value \( p \)-adic, 60
addition on cubic (elliptic) curve, 12
is associative, 14
is commutative, 13
additive group
of \( \mathbb{Q} \) not finitely generated, 114
affine curve
non-singular, 278
singular point, 278
tangent line, 277, 278
affine part of projective curve, 272
affine plane, 268
curve in, 271
Agrawal–Kayal–Saxena primality test, 139
algebraic curve, 271
degree of, 271
algebraic number theory, 80, 254
algorithm powering, 140, 163
Alice, 152
arc length, 31
arithmetic dynamics, 115
associative law, 14
automorphism group, 208, 210
of abelian group, 258
automorphism of a field, 208
auxiliary polynomial, 182
does not vanish, 193
is small, 190
auxiliary polynomial theorem, 188
B
babystep-giantstep algorithm to solve the DLP, 166
Baker’s theorem, 170, 202
Bezout’s theorem, 10, 285
proof of, 290–301
birational equivalence, 16
birational transformation, 16, 31
Birch–Swinnerton-Dyer conjecture, 250
Bob, 152
C
canonical height, 111
zero iff point has finite order, 112
Carmichael number, 139, 162
Cauchy sequence, 111
Cayley–Bacharach theorem, 10, 288, 308
cubic, 288, 308
chaotic dynamical system, 57
circle, rational parametrization, 3, 28
circle group, 40
product of two, 43
class field theory, 211, 213
CM, see complex multiplication
collinear points, determinant condition for, 113
collision algorithm, 154, 166
Index

common component, 284
complex multiplication, 231
elliptic curve without, 229
lattice with, 235
complex points, 38, 217, 233, 243
complexity of a rational number, 65
component
common, 284
irreducible, 284
conductor, 250
congruence subgroup, 160
conic, 1
determinant, 28
group law on, 114
integer point on, 169
intersection with a line, 28, 280
number of mod p points, 119, 157
Pascal’s theorem, 289
rational, 1
through five specified points, 308
$C(p^r)$, 49
contains no points of finite order, 55
is subgroup of $C(Q)$, 54
cryptosystem, 152
Elgamal, 154, 155, 165
private key, 153
public key, 153
RSA, 140, 153, 164
cubic Cayley–Bacharach theorem, 288, 308
cubic curve, 8
action of Galois on points, 214
addition, 12
algebraic map is homomorphism, 233
at most one singular point, 107
birationally equivalent to
Weierstrass normal form, 16, 18
canonical height, 111
collection of all, 286
complex multiplication, 231
complex points, 39
conductor, 250
discriminant, 46, 56, 81, 117, 134
division polynomial, 257
double-and-add algorithm, 147
duplication formula, 27, 36, 75, 81, 230
dermotomorphism, 231
dermotomorphism ring, 232, 259, 260
equation with integer coefficients, 45
examples of groups of rational points, 101
explicit formulas for group law, 23, 73
field generated by torsion points, 218
field of definition of $C[n]$, 222
finitely many integer points, 177
finiteness property of height, 66
formula for $2^{\text{rank}}$, 98
Galois representation, 225
group law on singular, 107, 113, 114
group of points over finite field, 45
height of $2P$, 67, 75–80, 203
height of $y$ coordinate, 72
height of a point, 66
height of a sum, 67, 71–75, 111
homogeneous equation, 23
homomorphism from rational points to $Q^*/Q^{*2}$, 92
index of $2C(Q)$ in $C(Q)$, 67
integer point, 167–202
integrality of multiples of $P$, 205
intersection with a line, 9
intersection with tangent line, 9
isogeny, 230
kernel of multiplication-by-$n$, 217
$K$-rational point, 213
Lenstra factorization algorithm, 147, 149
$L$-function, 248
Mazur’s theorem, 58
Mordell’s theorem, 88–95
multiplication-by-$n$ map, 217, 230
of high rank, 106
period parallelogram, 42, 83
point at infinity is inflection, 23
point of finite order has integer coordinates, 55
point of order four, 57, 63
point of order three, 131
is inflection point, 59
points over finite field, 117–157, 247, 249
rank of group of rational points, 96, 250
rational, 8
rational point, 39, 117
rational point denominators are $e^2$ and $e^3$, 48, 71
real points, 39
reduced modulo $p$, 134, 247
reduction modulo $p$ map on points, 134, 135, 161, 302
reduction modulo $p$ respects group law, 305
reduction modulo $p$ theorem, 136, 161
representation on $n$-torsion, 225
semi-stable reduction, 247
Siegel’s theorem, 168
singular, 21, 106–110, 247
singular has infinitely many integer points, 169
singular has parametrization, 22
small $h$ height, 66
subgroup of points of finite order, 134
torsion subgroup, 134
torsion subgroup of group of rational points, 96
uniform bound for torsion, 58
with many integer points, 173, 203
without CM, 229
cubic Fermat curve, 121, 163
cubic Gauss sum, 125
equidistribution of, 132
cubic polynomial discriminant, 46, 56, 60, 62, 81, 117, 129
cubic residue, 123
curve
action of Galois on points, 214
algebraic, 271
collection of all degree $d$, 308
defined over $\mathbb{Q}$, 276
degree of, 271
integer point, 276
irreducible, 284
irreducible component, 284
$K$-rational point, 213
non-singular, 278
of genus $g$, 120
points at infinity, 272, 273
projective, 271
rational, 276
rational points on, 276
reduction modulo $p$ map on points, 302
singular point, 278, 306
smooth, 278
tangent line, 277, 278, 306
transversal intersection, 285
cusp form, 252
cyclotomic field, 209
Galois group, 210
cyclotomic representation, 226
D
decomposition group, 254
defined at $P$, rational function is, 295, 298
degree
of a curve, 271
of a field, 207
of a polynomial, 274, 306
of homogeneous polynomial, 271
dehomogenization, 274
descent theorem, 68
determinant, 28, 254
condition for colinearity, 113
is unit for invertible matrix, 258
Diffie–Hellman key exchange, 155, 165
digital signature, 156
dimension of a vector space, 291
Diophantine approximation, 178
Diophantine approximation theorem, 178, 197, 200
effectivity, 201
Dirichlet series, 248
Dirichlet’s theorem, 204
Dirichlet’s unit theorem, 169
discrete logarithm problem, 153
collision algorithm, 154, 166
in different groups, 155
index calculus, 154, 156
on an abstract group, 154
quantum computer solves, 156
discriminant, 45, 46, 56, 81, 117, 129, 256
linear combination of \( f \) and \( f' \), 46
of cubic polynomial, 60, 62
of degree \( n \) polynomial, 60
of Frey curve, 246, 255
of quadratic polynomial, 60
reduced modulo \( p \), 134
*Disquisitiones Arithmeticae*, 121
divisibility sequence, 205
division polynomial, 257
DLP, *see* discrete logarithm problem
double-and-add algorithm, 140, 147, 163
duplication formula, 27, 30, 33, 36, 47, 62, 75, 230
decomposed as composition, 81
duplication map, 36
dynamical system, 115

**E**

ECDLP, *see* elliptic curve discrete logarithm problem
effectivity

Diophantine approximation theorem, 201
Mordell’s theorem, 95
Siegel’s theorem, 170
Thue’s theorem, 201
Eichler–Shimura theorem, 158
Elgamal cryptosystem, 154, 155, 165

elliptic curve, 20
action of Galois on points, 214
addition, 12
algebraic map is homomorphism, 233
Birch–Swinnerton-Dyer conjecture, 250
canonical height, 111
complex multiplication, 231
complex parametrization, 42, 83
complex points, 38, 39, 217, 233, 243
ductor, 250
discriminant, 46, 56, 81, 117, 134
division polynomial, 257
double-and-add algorithm, 147
duplication formula, 27, 33, 36, 75, 81, 230
domorphism, 231
domorphism ring, 232, 259, 260
equation with integer coefficients, 45
examples of groups of rational points, 101
field generated by torsion points, 218
field of definition of \( C[n] \), 222
finitely many integer points, 177
finiteness property of height, 66
formula for \( 2^{\text{rank}} \), 98
Frey, 245
functional equation of \( L(E, s) \), 250
Galois representation, 225
group of points over finite field, 45
height of \( 2P \), 67, 75–80, 203
height of \( y \) coordinate, 72
height of a point, 66
height of a sum, 67, 71–75, 111
homomorphism from rational points to \( \mathbb{Q}^*/\mathbb{Q}^{*2} \), 92

ellipse, 309
arc length, 20, 31
Pascal’s theorem, 289
how it got its name, 32
index of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$, 67
integer point, 167–202
integrality of multiples of $P$, 205
isogeny, 230
kernel of multiplication-by-$n$, 217
$K$-rational point, 213
Lenstra factorization algorithm, 147, 149
$L$-function, 248
Mazur’s theorem, 58
modular, 252
Mordell’s theorem, 88, 95
multiplication-by-$n$ map, 217, 230
of high rank, 106
period parallelogram, 42, 83
point at infinity is inflection, 23
point of finite order has integer coordinates, 55
point of order four, 57, 63
point of order three is inflection point, 59
points of order three, 131
points of order two and three, 35, 37
points over finite field, 117–157, 247, 249
rank of group of rational points, 96, 250
rational point, 39, 117
rational point denominators are $e^2$ and $e^3$, 48, 71
real points, 38, 39
reduced modulo $p$, 134, 247
reduction modulo $p$ map on points, 134, 135, 161, 302
reduction modulo $p$ respects group law, 305
reduction modulo $p$ theorem, 136, 161
representation on $n$-torsion, 225
semi-stable reduction, 247
Siegel’s theorem, 168
singular, 21, 247
small $h$ height, 66
subgroup of points of finite order, 134
torsion subgroup, 134
torsion subgroup of group of rational points, 96
uniform bound for torsion, 58
with many integer points, 173, 203
without CM, 229
elliptic curve cryptography, 152–157
invention of, 155
elliptic curve discrete logarithm problem, 154
collision algorithm, 154, 166
harder than DLP in $\mathbb{F}_p^*$, 155, 156
quantum computer solves, 156
elliptic divisibility sequence, 205
elliptic function, 41, 83
endomorphism, 231
commutes with Galois, 236
product of, 232
sum of, 232
endomorphism ring, 232, 259, 260
of abelian group, 258
equivalence relation, 305
Euclidean algorithm, 142
extended, 148, 162, 163
running time, 143
Euclidean plane, 268
Euler product, 248
Eve, 152
exponential function, 212

F
factorization, 139
Lenstra elliptic curve algorithm, 147, 149
Pollard $p − 1$ algorithm, 144, 163
Fermat curve, 276
cubic, 121, 163
genus, 120, 245
number of points mod $p$, 157
Fermat equation, 8, 209, 265
Fermat infinite descent, 70
Fermat’s last theorem, 8, 71, 132, 245, 276
for exponent four, 103
Fermat’s little theorem, 104, 139
converse is false, 139
Fibonacci sequence, 205
field
automorphism, 208
automorphism group, 208, 210
cyclotomic, 209
degree of, 207
Galois extension, 208, 210
splitting, 208
field of definition, 222
finite field, multiplicative group is
cyclic, 122
finite order, 35
finitely generated abelian group, 95
finiteness property of height, 65
four group, 36, 103
Frey curve, 245, 246
discriminant, 246, 255
Frobenius element, 254
fundamental theorem of arithmetic, 139

G
g2, g3, 41, 262
Galois extension, 208, 210
Galois group, 208
abelian, 211
abelian over \( \mathbb{Q}(i) \), 236
action on points, 214, 256
commutes with endomorphism,
236
cyclotomic field, 210
decomposition group, 254
Frobenius element, 254
Serre’s theorem, 229
Galois representation, 225
Galois theory, fundamental theorem of,
210
\( \Gamma \)-function, 249
\( \Gamma_0(N) \), 251
gap principle, 204
Gauss sum, 125, 158, 256
quadratic, 211
Gauss’ lemma, 195
Gauss’ theorem, 121
general linear group, 224, 259
genus of Fermat curve, 120, 245
Germain’s theorem, 245
GL2, 224, 259
greatest common divisor, 142
group
descent theorem, 68
element of finite order, 35
finitely generated abelian, 95
of roots of unity, 40
group action, 256
group law
duplication formula, 27, 75,
81, 230
explicit formulas, 23, 73
on cubic curve, 12, 23, 73
on singular cubic curve, 23, 107
H
half-angle formula, 6, 29
Hasse principle counterexample, 11
Hasse’s theorem on quadratic equations,
8
Hasse–Weil theorem, 120, 147, 247, 249
for Fermat curve, 157
height, 65
always non-negative, 66
canonical, 111
finiteness property, 65
number of rational numbers smaller
than \( \kappa \), 111
of \( 2P \), 67, 75–80, 203
of \( y \) coordinate, 72
of a point, 66
of a sum, 67, 71–75, 111
of rational function at rational
point, 76
of \( \mathcal{O} \), 66
parallelogram law, 111
small \( h \), 66
<table>
<thead>
<tr>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hellegouarch curve, 245</td>
</tr>
<tr>
<td>Hensel’s lemma, 29</td>
</tr>
<tr>
<td>hexagon, 289</td>
</tr>
<tr>
<td>homogeneous coordinates, 267</td>
</tr>
<tr>
<td>normalized, 302</td>
</tr>
<tr>
<td>homogeneous cubic curve, 23</td>
</tr>
<tr>
<td>homogeneous of degree 0, 298</td>
</tr>
<tr>
<td>homogeneous polynomial, 271</td>
</tr>
<tr>
<td>partial derivative relation, 306</td>
</tr>
<tr>
<td>homogenization, 275, 307</td>
</tr>
<tr>
<td>hyperbola, 309</td>
</tr>
<tr>
<td>Pascal’s theorem, 289</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jugendtraum, 212</td>
</tr>
<tr>
<td>for ( \mathbb{Q}(i) ), 243, 244</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td>key exchange, 155, 165</td>
</tr>
<tr>
<td>Kronecker’s Jugendtraum, 212</td>
</tr>
<tr>
<td>for ( \mathbb{Q}(i) ), 243, 244</td>
</tr>
<tr>
<td>Kronecker–Weber theorem, 211</td>
</tr>
<tr>
<td>for quadratic extension, 211, 256</td>
</tr>
<tr>
<td>Kummer’s conjecture, 131</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>L</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lang’s integer point and rank conjecture, 176</td>
</tr>
<tr>
<td>Lattès map, 57</td>
</tr>
<tr>
<td>lattice, 41, 59, 217, 233, 243</td>
</tr>
<tr>
<td>complex multiplication, 235</td>
</tr>
<tr>
<td>Legendre’s theorem, 7</td>
</tr>
<tr>
<td>Lenstra elliptic curve algorithm, 147, 149</td>
</tr>
<tr>
<td>level, 251</td>
</tr>
<tr>
<td>level lowering theorem, 253</td>
</tr>
<tr>
<td>( L )-function, 248</td>
</tr>
<tr>
<td>Birch–Swinnerton-Dyer conjecture, 250</td>
</tr>
<tr>
<td>functional equation, 250</td>
</tr>
</tbody>
</table>

| Lie group, 40 |
| line at infinity, 269 |
| in the projective plane, 267 |
| integer point on, 168, 205 |
| intersection with conic, 28, 280 |
| number of mod \( p \) points, 119 |
| point at infinity, 272 |
| local ring, 61, 294, 295, 308 |
| localization, 239 |

<table>
<thead>
<tr>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANIAC computer, 132</td>
</tr>
<tr>
<td>matrix</td>
</tr>
<tr>
<td>invertible iff determinant is unit, 258</td>
</tr>
<tr>
<td>scalar, 237</td>
</tr>
</tbody>
</table>
Mazur’s theorem, 58
examples of torsion groups, 62
Millennium prize, 250
Miller–Rabin primality test, 139
modular elliptic curve, 252
modular form, 132, 160, 252
modular group, 251
modularity conjecture/theory, 132, 158, 246, 252
module, 223
Mordell’s theorem, 9, 16, 65, 88, 95
examples, 101
for curves with rational point of order two, 95
formula for 2-rank, 98
is not effective, 95
multiplication-by-n map, 217, 230
kernel of, 217
multiplicative group, 217
of Q∗ not finitely generated, 114
of finite field is cyclic, 122
multiplicity, 285, 291, 295, 299

N
Nagell–Lutz theorem, 45, 56, 102, 133, 167, 214, 239
not if and only if, 46, 56, 167
on curve with point of order two, 112
strong form, 56, 62
used to show point has infinite order, 137, 172
Nakayama’s lemma, 301
negative of a point, 13, 24
Néron–Ogg-Shafarevich criterion, 255
non-singular point, 278
non-vanishing theorem, 193, 197, 198
normal form, 16
normal subgroup, 210
normalized coordinates, 302
normalized polynomial, 302
n’th power map, 217
Nullstellensatz, 297
number field, degree of, 207
number field, sieve, 153

O
O (identity on cubic curve), 11
order
of a rational number at p, 48, 60
of element of a group, 35

P
p-adic absolute value, 60
p-adic number, 8, 49
p-adic order, 48, 60
p-adic topology, 61
parabola, 309
Pascal’s theorem, 289
Pell’s equation, 169, 202
period, 41
period parallelogram, 42, 83
periodic point, 115
pigeonhole principle, 184
plane
affine, 268
Euclidean, 268
projective, 267
point
K-rational, 213
local ring at, 294, 295, 308
point at infinity, 118, 269, 272
is inflection, 23
point of finite order
field generated by, 218
field of definition, 222
has integer coordinates, 55
iff canonical height zero, 112
non-zero modulo p, 136
point of order four, 57, 63
point of order three, 35, 37
is inflection point, 59
point of order two, 35, 37
Pollard p − 1 algorithm, 144, 146, 163
Pollard ρ algorithm, 155
polynomial
auxiliary, 182, 190, 193
degree, 274, 306
dehomogenization, 274
discriminant, 60, 256
homogeneous, 271
homogenization, 275, 307
normalized, 302
powering algorithm, 140, 163
\( P \ast Q \), 9
preperiodic point, 115
primality test, 139
prime number theorem, 133
prime, Weiferich, 245
primitive integer point, 204
primitive right triangle, 4, 28
primitive root of unity, 157, 209
private key cryptosystem, 153
projective curve, 271
affine part, 272
collection of all degree \( d \), 308
degree of, 271
non-singular, 278
points at infinity, 272
rational points are integer points, 277
singular point, 278, 306
tangent line, 306
projective plane, 267
as set of directions in \( \mathbb{A}^2 \), 268
change of coordinates, 279
curve in, 271
line at infinity, 269
line in, 267
points at infinity, 269
reduction modulo \( p \) map, 302
projective space, 267
equivalence relation defining, 305
normalized homogeneous coordinates, 302
rational points are integer points, 277
projective transformation, 17, 279
sends lines to lines, 307
pseudo-prime, 162
\( p \)’th root of unity, 125, 157
public key cryptosystem, 153
Pythagorean theorem, 4

Q
quadratic formula, 279
quadratic Gauss sum, 158, 211
quadratic non-residue, 158
quadratic polynomial, discriminant of, 60
quadratic residue, 119, 157
quantum computer, 156
quotient rule, 196

R
rank
elliptic curve with high, 106
of a finitely generated abelian group, 96
of group of rational points, 96, 250
rational conic, 1
rational cubic, 8
rational curve, 276
rational function, 115, 295
defined at \( P \), 295, 298
homogeneous of degree 0, 298
rational line, 1
two intersect in rational point, 28
rational number, 1
height, 65
rational parametrization, 3
rational point, 1
height, 65, 66
is integer point in projective space, 277
on curve, 276
two determine rational line, 28
rational points, 117
real points, 38
reduction modulo \( p \), 134, 247, 302–305
map on \( \mathbb{P}^1 \), 302
map on curve, 134, 135, 161, 302
of a point, 302
respects group law on elliptic curve, 305
reduction modulo \( p \) theorem, 136, 161
representation, 225
  change of basis, 227, 259, 262
cyclotomic, 226
Galois, 225
trace of, 254
Ribet’s theorem, 253
Riemann hypothesis, 120
Riemann zeta function, 248
right triangle, 4
rigidity theorem, 233
ring, local, 294, 307
$R$-module, 223
root of unity, 40, 125, 209
  primitive, 157
Roth’s theorem, 200
  exponent is best possible, 204
$R_p$, 50
RSA cryptosystem, 140, 153, 164

S
Sato–Tate conjecture, 133, 158
scalar matrix, 237
Selmer, 11
semi-stable reduction, 247
  split, 247
semicubical parabola, 21
Serre’s theorem, 229
Shank’s algorithm, 166
Siegel’s lemma, 183
Siegel’s theorem, 168
  easy case, 170, 171, 203
  effectiveness, 170
singular cubic curve, 21, 106–110, 247
  group law, 23, 107, 113, 114
singular elliptic curve, 21, 247
singular point, 278, 306
Skolem’s method, 170
smallness theorem, 190, 197–199
smooth curve, 278
split semi-stable reduction, 247
splitting field, 208
square and multiply algorithm, 140, 163
Sterling’s formula, 146
sum of two cubes, 170
symmetric group, 225, 228

T
tangent line, 277, 278, 306
tangent, half-angle formula, 6, 29
taxicab equation, 170, 171
  number of solutions, 173, 203
  size of solutions, 172
taxicab number, 170, 174
taylor series, 190, 212
Thue’s theorem, 177, 178, 197, 200
  effectivity, 201
torsion point, field generated by, 218
torsion subgroup, 134
  injects modulo $p$, 136
  of a finitely generated abelian
group, 96
torus, 43
trace, 254
transversal intersection, 285
triangle inequality, 61, 184, 191
triangle, right, 4

U
unique factorization domain, 284
unit group, 9, 80
unit theorem, 169
upper half-plane, 251

W
Weierstrass elliptic function, 41, 83
Weierstrass equation, 41
  with integer coefficients, 45
Weierstrass normal form, 16
Weierstrass $\wp$-function, 41, 59, 244, 262
  is doubly periodic, 59
  is even, 59
Weiferich’s theorem, 245
Weil conjectures, 121
Wiles’ theorem, 71, 252, 276
Wronskian polynomial, 193

Z
zeta function, 248