Ideals, Varieties, and Algorithms by David A. Cox

Frosty

January 31, 2026

Contents

1 Geometry, Algebra, and Algorithms 1
1.1 Polynomials and Affine Space 1
1.2 Affine Varieties 4
1.3 Parametrizations of Affine Varieties 9

1 Geometry, Algebra, and Algorithms

1.1 Polynomials and Affine Space

Problem 2

Let $\mathscr{F}_2$ be the field from Exercise 1.

1. Consider the polynomial $g(x, y) = x^2y + y^2x \in \mathscr{F}_2[x, y]$. Show that $g(x, y) = 0s$ for every $(x, y) \in \mathscr{F}_2^2$, and explain why this does not contradict Proposition 5.
2. Find a nonzero polynomial in $\mathscr{F}_2[x, y, z]$ which vanishes at every point of $\mathscr{F}_2^3$. Try to find one involving three variables.
3. Find a nonzero polynomial in $\mathscr{F}_2[x_1, \dots, x_n]$ which vanishes at every point of $\mathscr{F}_2^n$. Can you find one in which all of $x_1, \dots, x_n$ appear?

Solution (1): It is clear that if $x = 0$ or $y = 0$, then $g(x, y) = 0$. Now, if $x = y = 1$, then

$$g(x, y) = 1^2 \cdot 1 + 1^2 \cdot 1 = 1 + 1 = 0.$$

Thus $g(x, y) = 0$ for all $(x, y) \in \mathscr{F}_2^2$.

Solution (2): Consider the polynomial $g \in \mathscr{F}_2[x, y, z]$ defined by

$$g(x, y, z) = (x^2 - x)(y^2 - y)(z^2 - z),$$

which is clearly 0 at all $(x, y, z) \in \mathscr{F}_2 \times \mathscr{F}_2 \times \mathscr{F}_2$.

Solution (3): Consider the polynomial $g \in \mathscr{F}_2[x_1, \dots, x_n]$ defined by

$$g(x_1, \dots, x_n) = (x_1^2 - x_1) \cdots (x_n^2 - x_n),$$

which is clearly 0 at all $(x_1, \dots, x_n) \in \mathscr{F}_2 \times \cdots \times \mathscr{F}_2$.

Problem 3

(Requires abstract algebra) Let p be a prime number. The ring of integers modulo p is a field with p elements, which we will denote $\mathscr{F}_p$.

1. Explain why $\mathscr{F}_p \setminus \{0\}$ is a group under multiplication.
2. Use Lagrange's theorem to show that $a^{p-1} = 1$ for all $a \in \mathscr{P} \setminus \{0\}$.
3. Prove that $a^p = a$ for all $a \in \mathscr{F}_p$. [Hint: Treat the cases $a = 0$ and $a \neq 0$ separately.]
4. Find a nonzero polynomial in $\mathscr{F}_p[x]$ that vanishes at all points in $\mathscr{F}_p$. [Hint: Use part (c).]

Solution (1): It is well known that for any ring R the set of units $U(R)$ under multiplication forms a group. All elements $x \neq 0$ in $\mathscr{F}_p$ have inverses and are thus in $U(\mathscr{F}_p)$. Therefore $\mathscr{F}_p \setminus \{0\}$ is a group under multiplication.

Solution (2): Don't have preqreuisites.

Proof. Let $a \in \mathscr{F}_p$. Suppose $a = 0$. Then $a^p = 0^p = 0 = a$. Suppose $a \neq 0$. Then $a^{p-1} = 1$ by part 2. Then $a \cdot a^{p-1} = a \cdot 1 \iff a^p = a$ as required. ∎

Solution (4): Consider the polynomial $g(x) = x^p - x \in \mathscr{F}_p[x]$. Now, for all $a \in \mathscr{F}_p$ we have $a^p = a$ by part 3, thus $g(a) = 0$.

Problem 5

In the proof of Proposition 5, we took $f \in k[x_1, \ldots, x_n]$ and wrote it as a polynomial in x_n with coefficients in $k[x_1, \ldots, x_{n-1}]$. To see what this looks like in a specific case, consider the polynomial

$$f(x, y, z) = x^5y^2z - x^4y^3 + y^5 + x^2z - y^3z + xy + 2x - 5z + 3.$$

1. Write f as a polynomial in x with coefficients in $k[y, z]$.
2. Write f as a polynomial in y with coefficients in $k[x, z]$.
3. Write f as a polynomial in z with coefficients in $k[x, y]$.

Solution (1):

$$f(x) = (y^2z)x^5 - (y^3)x^4 + (z)x^2 + (y + 2)x - y^3z + y^5 - 5z + 3$$

Solution (2):

$$f(y) = y^5 - (x^4 - z)y^3 + (x^5z)y^2 + (x)y + x^2z + 2x - 5z + 3$$

Solution (3):

$$f(z) = (x^5y^2 + x^2 - y^3 - 5)z - x^4y^3 + y^5 + xy + 2x + 3$$

Problem 6

Inside of $\mathbb{C}^n$, we have the subset $\mathbb{Z}^n$, which consists of all points with integer coordinates.

1. Prove that if $f \in \mathbb{C}[x_1, \dots, x_n]$ vanishes at every point of $\mathbb{Z}^n$, then f is the zero polynomial. [Hint: Adapt the proof of Proposition 5.]
2. Let $f \in \mathbb{C}[x_1, \dots, x_n]$, and let M be the largest power of any variable that appears in f. Let $\mathbb{Z}^n_{M+1}$ be the set of all points of $\mathbb{Z}^n$, all coordinates which lie between 1 and $M+1$, inclusive. Prove that if f vanishes at all points of $\mathbb{Z}^n_{M+1}$, then f is the zero polynomial.

Proof. Suppose $f \in \mathbb{C}[x_1, \dots, x_n]$ vanishes at every point of $\mathbb{Z}^n$. We will use induction on the number of variables n. When $n = 1$. It is well known that a nonzero polynomial in $\mathbb{C}[x]$ of degree m has at most m distinct roots. For our particular $f \in \mathbb{C}[x]$, we are assuming $f(a) = 0$ for all $a \in \mathbb{Z}$. Since $\mathbb{Z}$ is infinite, this means that f has infinitely many roots, and, hence, f must be the zero polynomial.

Now assume that the theorem holds for $n-1$ variables. By collecting the various powers of x_n, we can write f in the form

$$f = \sum_{i=0}^{N} g_i(x_1, \dots, x_{n-1}) x_n^i,$$

where $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$. We will show that each g_i is the zero polynomial in $n-1$ variables, which will force f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$.

If we fix $(a_1, \dots, a_{n-1}) \in \mathbb{Z}^{n-1}$, we get the polynomial $f(a_1, \dots, a_{n-1}, x_n) \in \mathbb{C}[x_n]$. By our hypothesis on f, this vanishes for every $a_n \in \mathbb{Z}$. It follows from the case $n = 1$ that $f(a_1, \dots, a_{n-1}, x_n)$ is the zero polynomial in $\mathbb{C}[x_n]$. Using the above formula for f, we see that all coefficients of $f(a_1, \dots, a_{n-1}, x_n)$ vanish. Since $(a_1, \dots, a_{n-1})$ was arbitrarily chosen in $\mathbb{Z}^{n-1}$, it follows that each $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$ gives the zero function on $\mathbb{Z}^{n-1}$. Our inductive assumption then implies each g_i is the zero polynomial in $\mathbb{C}[x_1, \dots, x_{n-1}]$. This forces f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$. ∎

Proof. Suppose $f \in \mathbb{C}[x_1, \dots, x_n]$ vanishes at every point of $\mathbb{Z}^n_{M+1}$. We will use induction on the number of variables n. When $n = 1$. It is well known that a nonzero polynomial in $\mathbb{C}[x]$ of degree at most M has at most M distinct roots. For our particular $f \in \mathbb{C}[x]$, we are assuming $f(a) = 0$ for all $a \in \mathbb{Z}_{M+1}$. Since $\mathbb{Z}_{M+1}$ has $M+1$ elements, this means that f has $M+1$ roots, and, hence, f must be the zero polynomial.

Now assume that the theorem holds for $n-1$ variables. By collecting the various powers of x_n, we can write f in the form

$$f = \sum_{i=0}^{N} g_i(x_1, \dots, x_{n-1}) x_n^i,$$

where $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$. We will show that each g_i is the zero polynomial in $n-1$ variables, which will force f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$.

If we fix $(a_1, \dots, a_{n-1}) \in \mathbb{Z}^{n-1}_{M+1}$, we get the polynomial $f(a_1, \dots, a_{n-1}, x_n) \in \mathbb{C}[x_n]$. By our hypothesis on f, this vanishes for every $a_n \in \mathbb{Z}_{M+1}$. It follows from the case $n = 1$ that $f(a_1, \dots, a_{n-1}, x_n)$ is the zero polynomial in $\mathbb{C}[x_n]$. Using the above formula for f, we see that all coefficients of $f(a_1, \dots, a_{n-1}, x_n)$ vanish. Since $(a_1, \dots, a_{n-1})$ was arbitrarily chosen in $\mathbb{Z}^{n-1}_{M+1}$, it follows that each $g_i \in \mathbb{C}[x_1, \dots, x_{n-1}]$ gives the zero function on $\mathbb{Z}^{n-1}_{M+1}$. Our inductive assumption then implies each g_i is the zero polynomial in $\mathbb{C}[x_1, \dots, x_{n-1}]$. This forces f to be the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$. ∎

1.2 Affine Varieties

Problem 1

Sketch the following affine varieties in $\mathbb{R}^2$:

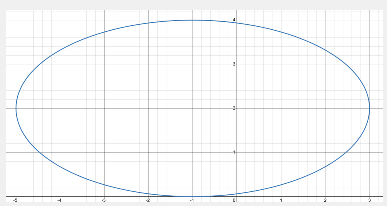
1. $\mathbf{V}(x^2 + 4y^2 + 2x - 16y + 1)$
2. $\mathbf{V}(x^2 - y^2)$
3. $\mathbf{V}(2x + y - 1, 3x - y + 2)$

In each case, does the variety have the dimension you would intuitively expect it to have?

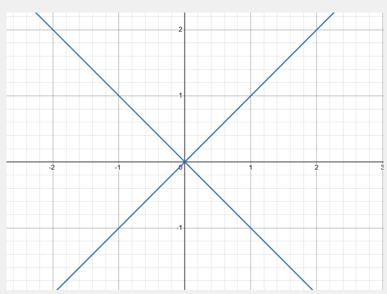
Solution (1): I would expect it to have two dimensions. Notice

$$\begin{aligned}
x^2 + 4y^2 + 2x - 16y + 1 = 0 &\iff x^2 + 2x + 1 + 4y^2 - 16y = 0 \\
&\iff (x+1)^2 + 4(y^2 - 4y) = 0 \\
&\iff (x+1)^2 + 4(y^2 - 4y + 4 - 4) = 0 \\
&\iff (x+1)^2 + 4((y-2)^2 - 4) = 0 \\
&\iff (x+1)^2 + 4(y-2)^2 - 16 = 0 \\
&\iff \frac{(x+1)^2}{4} + \frac{(y-2)^2}{1} = 4
\end{aligned}$$

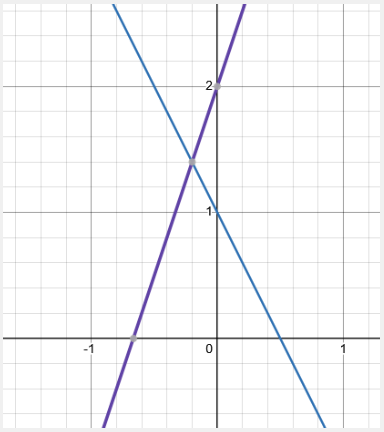
Which is an ellipse.



Solution (2): I would expect it to have two dimensions. If we solve $x^2 - y^2$ for y we find $y = \pm x$ which is two lines with slope of 1 passing through the origin.



Solution (3): I would expect it to be a single point. We can solve for x, y and find $x = -\frac{1}{5}$, $y = \frac{7}{5}$.



Problem 6

Let us show that all finite subset of k^n are affine varieties.

1. Prove that a single point $(a_1, \dots, a_n) \in k^n$ is an affine variety.
2. Prove that every finite subset of k^n is an affine variety. [Hint: Lemma 2 will be useful.]

Proof. Let $(a_1, \dots, a_n)$ be an arbitrary point in k^n. Consider the following set of polynomials

$$\mathscr{P} = \{x_i - a_i \mid 1 \leq i \leq n\}.$$

For which the point $(a_1, \dots, a_n)$ is the exact solution. Thus

$$\mathbf{V}(\mathscr{P}) = \{(a_1, \dots, a_n)\}.$$

Therefore a single point in k^n is an affine variety. ∎

Proof. Let $V \subset k^n$ be a finite set. Then V can be written as

$$V = \bigcup_{i=1}^{m} \{p_i\},$$

where each $p_i \in k^n$. By part (1), each $\{p_i\}$ is an affine variety. By Lemma 2, a finite union of affine varieties is an affine variety. Thus V is an affine variety. ∎

Problem 8

It can take some work to show that something is *not* an affine variety. For example, consider the set

$$X = \{(x, x) \mid x \in \mathbb{R}, x \neq 1\} \subseteq \mathbb{R}^2$$

which is the straight line $x = y$ with the point $(1, 1)$ removed. To that X is not an affine variety, suppose that $X = \mathbf{V}(f_1, \dots, f_s)$. Then each f_i vanishes on X, and if we can show that f_i also vanishes at $(1, 1)$, we will get the desired contradiction. Thus, here is what you are to prove: if $f \in \mathbb{R}[x, y]$ vanishes on X, then $f(1, 1) = 0$. [Hint: Let $g(t) = f(t, t)$ which is a polynomial $\mathbb{R}[t]$. Now apply the proof of proposition 5 on 1.]

Proof. Suppose $f \in \mathbb{R}[x, y]$ vanishes on X. Let $g(t) = f(t, t)$, which is a polynomial in $\mathbb{R}[t]$. Then $g(x) = 0$ for all $x \in \mathbb{R}$ with $x \neq 1$. Since a nonzero polynomial in $\mathbb{R}[t]$ can have only finitely many roots, it follows from Proposition 5 that g must be the zero polynomial. Therefore $g(1) = f(1, 1) = 0$, which is a contradiction. ∎

Problem 9

Let $\mathbf{R} = \{(x, y) \in \mathbb{R}^2 \mid y > 0\}$ be the upper half plane. Prove that $\mathbf{R}$ is not an affine variety.

Proof. Suppose $f \in \mathbb{R}[x, y]$ vanishes on $\mathbf{R}$. Fix any $y_0 > 0$ and consider the polynomial in one variable $g(x) = f(x, y_0) \in \mathbb{R}[x]$. Since $f(x, y_0) = 0$ for all $x \in \mathbb{R}$ by Proposition 5, g is the zero polynomial. Because $y_0 > 0$ was arbitrary it follows that that $f(x, y) = 0$ for all $(x, y) \in \mathbf{R}$. Therefore f is the zero polynomial. ∎

Problem 10

Let $\mathbb{Z}^n \subseteq \mathbb{C}^n$ consist of those points with integer coordinates. Prove that $\mathbb{Z}^n$ is not an affine variety. [Hint: See Exercise 6 1.]

Proof. Suppose $f \in \mathbb{C}[x_1, \dots, x_n]$ vanishes on $\mathbb{Z}^n$. Fix integers $k_2, \dots, k_n \in \mathbb{Z}$ and consider the polynomial

$$g(x_1) = f(x_1, k_2, \dots, k_n) \in \mathbb{C}[x_1].$$

Since $g(x_1) = f(x_1, k_2, \dots, k_n) = 0$ for all $x_1 \in \mathbb{Z}$, by Proposition 5 it follows that g is the zero polynomial. Because $k_2, \dots, k_n$ were arbitrary integers, it follows that $f(x_1, x_2, \dots, x_n) = 0 \quad$ for all $(x_1, \dots, x_n) \in \mathbb{Z}^n$. Therefore f is the zero polynomial in $\mathbb{C}[x_1, \dots, x_n]$. ∎

Problem 11

So far, we have discussed varieties in $\mathbb{R}$ or $\mathbb{C}$. It is also possible to consider varieties over the field $\mathbb{Q}$, although the questions here tend to be *much* harder. For example, let n be a positive integer, and consider the variety $F_n \subseteq \mathbb{Q}^2$ defined by
$$x^n + y^n = 1.$$
Notice that there are some obvious solutions when x or y is zero. We call these *trivial solutions*. An interesting question is whether or not there are any nontrivial solutions.

1. Show that F_n has two trivial solutions if n is odd and four trivial solutions of n is even.
2. Show that F_n would have a nontrivial solution for some $n \geq 3$ if and only if Fermat's Last Theorem were false.

Theorem 1. Fermat's Last Theorem *states that, for $n \geq 3$, the equation*

$$x^n + y^n = z^n$$

has no solutions where x, y and z are nonzero integers. The general case of this conjecture was proved by Andrew Wiles in 1994 using some very sophisticated number theory. The proof is extremely *difficult.*

Proof. Suppose n is odd. If $x = 0$ then $y = 1$. Similarly, if $y = 0$ then $x = 1$. Thus we have two solutions: $(0, 1), (1, 0)$.

Suppose n is even. If $x = 0$ then $y = \pm 1$. Similarly, if $y = 0$ then $x = \pm 1$. Thus we have four solutions: $(0, \pm 1), (\pm 1, 0)$. ∎

Proof. Suppose F_n has a nontrivial solution for some $n \geq 3$. Then suppose $x, y \in \mathbb{Q}$ such that $x^n + y^n = 1$. Furthermore, suppose $x = \frac{a}{b}, y = \frac{c}{d}$ where $a, b, c, d \in \mathbb{Z}$. Then

$$\left(\frac{a}{b}\right)^n + \left(\frac{c}{d}\right)^n = \frac{a^n}{b^n} + \frac{c^n}{d^n} = 1.$$

Multiply through by $b^n d^n$ to obtain
$$(ad)^n + (cb)^n = (bd)^n.$$

Since $a, b, c, d \in \mathbb{Z}$ and $n \geq 3$, this is a solution to Fermat's Last Theorem.

Conversely, suppose Fermat's Last Theorem is false. Then there exists nonzero integers x, y, z and $n \geq 3$ such that $x^n + y^n = z^n$. Dividing through by z^n gives

$$\left(\frac{x}{z}\right)^n + \left(\frac{y}{z}\right)^n = 1.$$

Therefore F_n has a nontrivial solution for some $n \geq 3$. ∎

Problem 15

In Lemma 2, we showed that if V and W are affine varieties, then so are there union $V \cup W$ and intersection $V \cap W$. In this exercise we will study how other set-theoretic operations affect affine varieties.

1. Prove that finite unions and intersections of affine varieties are again affine varieties. [Hint: Induction].
2. Give an example to show that an infinite union of affine varieties need not be an affine variety. Hint: By Exercise 8-10, we know some subsets of k^n that are not affine varieties. Suprisingly, an infinite intersection of affine varieties is still an affine variety. This is a consequence of the Hilbert Basis Theorem, which will be discussed in Chapter 2.
3. Given an example to show that the set-theoretic difference $V \setminus W$ of two affine varieties need not be an affine varietiy.
4. Let $V \subseteq k^n$ and $W \subseteq k^m$ be two affine varieties, and let

$$V \times W = \{(x_1, \dots, x_n, y_1, \dots, y_m) \in k^{n+m} \mid (x_1, \dots, x_n) \in V, (y_1, \dots, y_n) \in W\}$$

be their Cartesian product. Prove that $V \times W$ is an affine variety in k^{n+m}. [Hint: If V is defined by $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, then we can regard $f_1, \dots, f_s$ as polynomials in $k[x_1, \dots, x_n, y_1, \dots, y_m]$, and similarly for W. Show that this gives defining equations for the Cartesian product.]

Proof. By Lemma 2 we know the base case holds for the union and intersection of two affine varieties. Suppose Lemma 2 holds for the union and intersection of $n-1$ affine varieties. Let $V = \{v_1, \dots, v_n\}$ be a set of n affine varieties. Then

$$\mathscr{U} = \bigcup_{i=1}^{n} v_i = \bigcup_{i=1}^{n-1} v_i \cup v_n,$$

and

$$\mathscr{I} = \bigcap_{i=1}^{n} v_i = \bigcap_{i=1}^{n-1} v_i \cap v_n.$$

Now, by our hypothesis $\bigcup_{i=1}^{n-1} v_i$ and $\bigcap_{i=1}^{n-1} v_i$ are affine varieties. Then by Lemma 2, $\bigcup_{i=1}^{n-1} v_i \cup v_n$ and $\bigcap_{i=1}^{n-1} v_i \cap v_n$ are also affine varieties. Thus $\mathscr{U}$ and $\mathscr{I}$ are affine varieties. ∎

Proof. Consider the union of all points in $\mathbb{Z}^n$. Each point is an affine variety by Problem 6. However, by Problem 10, their union (which is $\mathbb{Z}^n$) is not an affine variety. ∎

Proof. Consider the varieties $V_1 = \{(x, y) \mid x = y\}$ and $V_2 = \{(1, 1)\}$. By Problem 8, $V_1 \setminus V_2$ is not an affine variety. ∎

Proof. Let $V \subseteq k^n$ be defined by polynomials $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ and $W \subseteq k^m$ be defined by polynomials $g_1, \dots, g_t \in k[y_1, \dots, y_m]$. Then, let $f_1, \dots, f_s \in k[x_1, \dots, x_n, y_1, \dots, y_m]$ and $g_1, \dots, g_t \in k[x_1, \dots, x_n, y_1, \dots, y_m]$. Then

$$V \times W = \mathbf{V}(f_1, \dots, f_s, g_1, \dots, g_t) \subseteq k^{n+m},$$

so $V \times W$ is an affine variety. ∎

1.3 Parametrizations of Affine Varieties

Problem 1

Parametrize all solutions of the linear equations

$$x + 2y - 2z + w = 1,$$

$$x + y + z - w = 2.$$

Proof. We use row reduction to find the simplified equations:

$$x - 4z + 3w = 3, \quad y - 3z + 2w = -1.$$

Then let $s = w$ and $t = z$. Then

$$x = 3 + 4t - 3s, \quad y = -1 + 3t - 2s.$$

∎

Problem 2

Use a trigonometric identity to show that

$$x = \cos(t),$$

$$y = \cos(2t)$$

parametrizes a portion of a parabola. Indicate exactly what portion of the parabola is covered.

Proof. We have

$$y = \cos(2t) = 2\cos^2(t) - 1 = 2x^2 - 1.$$

Since $\mathrm{Ran}(\cos) = [-1, 1]$, we have $\mathrm{Ran}(x(t)) = [-1, 1]$, and thus $\mathrm{Ran}(y = 2x^2 - 1) = [-1, 1]$. ∎

Problem 3

Given $f \in k[x]$, find a parametrization of $V(y - f(x))$.

Proof. We want to parametrize $y - f(x) = 0$. Let $t = x$, then $y = f(x) = f(t)$. Thus we have $(x, y) = (t, f(t))$ where $t \in k$. ∎

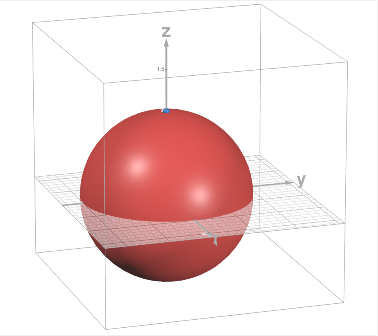
Problem 6

The goal of this problem is to that the sphere $x^2+y^2+z^2 = 1$ in 3-dimensional space can be parametrized by

$$x = \frac{2u}{u^2+v^2+1},$$
$$y = \frac{2v}{u^2+v^2+1},$$
$$z = \frac{u^2+v^2-1}{u^2+v^2+1}.$$

The idea is to adapt the argument used for the circle $x^2 + y^2 = 1$ to 3-dimensional space.

1. Given a point $(u, v, 0)$ in the (x, y)-plane, draw the line from this point to the "north pole" $(0, 0, 1)$ of the sphere, and let (x, y, z) be the other point where the line meets the sphere. Draw a picture to illustrate this, and argue goemetrically that mapping (u, v) to (x, y, z) gives a parametrization of the sphere minus the north pole.
2. Show that the line connecting $(0, 0, 1)$ to $(u, v, 0)$ is parametrized by $(tu, tv, 1-t)$, where t is a parameter that moves along the line.
3. Substitute $x = tu$, $y = tv$ and $z = 1-t$ into the equation for the sphere $x^2 + y^2 + z^2 = 1$. Use this to derive the formulas given at the beggining of the problem.



Proof. The figure above shows the unit sphere in 3-space. It is clear that if we are to draw all lines from $(0, 0, 1)$ to $(u, v, 0)$ where $u, v \in \mathbb{R}$ then we would be able to intersect all points on the sphere other than $(0, 0, 1)$. Now, taking a point (u, v) we can compute the line through $(u, v, 0)$ and $(0, 0, 1)$ and find the point at which it intersects the unit sphere. ∎

Proof. Notice

$$\begin{aligned}(x, y, z) &= (0, 0, 1) + t((u, v, 0) - (0, 0, 1)) \\ &= (0, 0, 1) + t(u, v, -1) \\ &= (tu, tv, 1-t)\end{aligned}$$

∎

Proof. We have

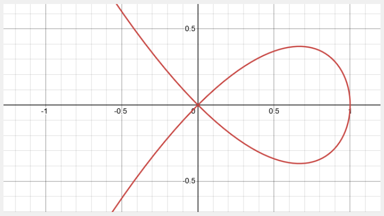
$$x^2 + y^2 + z^2 = 1 \iff t^2u^2 + t^2v^2 + t^2 - 2t = 0 \iff t(tu^2 + tv^2 + t - 2) = 0$$

Now $t = 0$ corresponds with $(0, 0, 1)$ thus we want $tu^2 + tv^2 + t - 2 = 0$. Solving for t we find $t = \frac{2}{u^2+v^2+1}$. Plugging t into $(x(t), y(t), z(t))$ gives the desired equations. ∎

Problem 8

Consider the curved defined by $y^2 = cx^2 - x^3$, where c is some constant. Here is a picture of the curve when $c > 0$. Our goal is to parametrize this curve.

1. Show that a line will meet this curve at either $0, 1$, or 3 points. Illustrate you answer with a picture. [Hint: Let the equation of the line by either $x = a$ or $y = mx + b$.]
2. Show that a nonvertical line through the origin meets the curve at exactly one other point $m^2 \neq c$. Draw a picture to illustrate this, and see if you can come up with an intuitive explanation for as to why this happens.
3. Now draw the vertical line $x = 1$. Given a point $(1, t)$ on this line, draw the line connecting $(1, t)$ to the origin. This will interesect the curve in a point (x, y). Draw a picture to illustrate this, and argue geometrically that this gives a parametrization of the entire curve.



Proof. Suppose $x = a$. Then

$$y^2 = ca^2 - a^3 = a^2(c - a).$$

If $c < a$ then there is no solution. If $c = a$ then $y = 0$ and there is a single solution $(a, 0)$. If $c > a$ then there are two solutions

$$y = \pm a\sqrt{c - a}.$$

Thus a vertical line meets the curve in $0, 1$, or 2 points.

Now suppose $y = mx + b$. Substituting into the equation of the curve gives

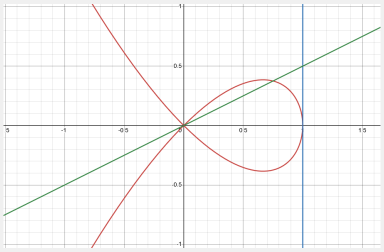
$$(mx + b)^2 = cx^2 - x^3 \tag{1}$$
$$\iff x^3 + (m^2 - c)x^2 + 2mbx + b^2 = 0. \tag{2}$$

This is a cubic equation in x, so a nonvertical line meets the curve in at most three points. ∎

Proof. Suppose $y = mx$ and $m^2 \neq c$. Substituting into the equation of the curve gives

$$\begin{aligned} m^2x^2 &= cx^2 - x^3 \\ \iff x^3 + (m^2 - c)x^2 &= 0 \\ \iff x^2(x + m^2 - c) &= 0. \end{aligned}$$

Thus $x = 0$ is a root corresponding to the origin, and the other intersection point is $x = c - m^2$. Therefore every nonvertical line through the origin with $m^2 \neq c$ meets the curve in exactly one other point. ∎



Proof. Consider the vertical line $x = 1$ and a point $(1, t)$ on this line. The line connecting $(1, t)$ to the origin has equation $y = tx$. Substituting into the equation of the curve gives

$$\begin{aligned} t^2x^2 &= cx^2 - x^3 \\ \iff x^3 + (t^2 - c)x^2 &= 0 \\ \iff x^2(x + t^2 - c) &= 0. \end{aligned}$$

Ignoring the double root $x = 0$ we have $x = c - t^2$. and therefore $y = t(c - t^2)$. Therefore the curve is parametrized by

$$x(t) = c - t^2, \qquad y(t) = t(c - t^2).$$

∎

Problem 10

Around 180 B.C.E., Diocles wrote the book *On Burning Mirrors*. One of the curves he considered was the *cissoid* and he used it to solve the problem of duplication of the cube [see part (c) below]. The cissoid has the equation $y^2(a + x) = (a - x)^3$, where a is a constraint. This gives the following curve in the plane:

1. Find an algebraic parametrization of the cissoid.
2. Diocles described the cissoid using the following geometric construction. Given a circle of radius a (which we will take as centered at the origin), pick x between a and $-a$, and draw the line L connecting $(a, 0)$ to the point $P = (-x, \sqrt{a^2 - x^2})$ on the circle. This determines a point $Q = (x, y)$ on L:
   Prove that the cissoid is the locus of all such points Q.
3. The duplication of the cube is the classical Greek problem of trying to construct $\sqrt[3]{2}$ using ruler and compass. It is known that this is impossible given just a ruler and compass. Diocles showed that if in addition, you allow the use of the cissoid, then one construct $\sqrt[3]{2}$. Here is how it works. Draw the line connecting $(-a, 0)$ to $(0, -a/2)$. This line will meet the cissoid at a point (x, y). Then prove that

   $$2 = \left(\frac{a - x}{y}\right)^3,$$

   which shows how to construct $\sqrt[3]{2}$ using ruler, compass, and cissoid.