BÉZOUT'S THEOREM, PART 1

GLENN SUN
UCLA MATH CIRCLE ADVANCED 1

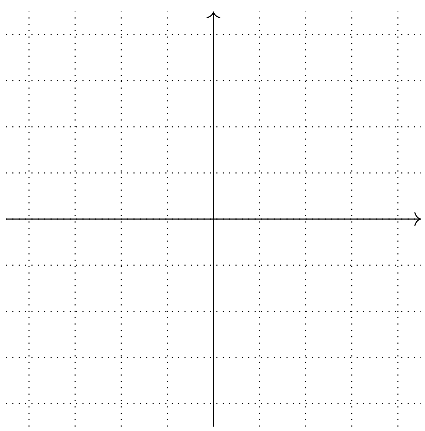
APRIL 30, 2023

1 Introduction

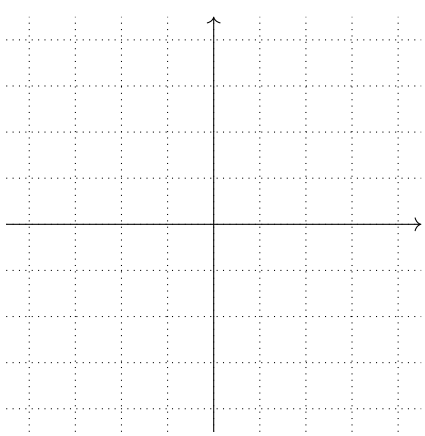
Over the next two weeks, we will study *algebraic geometry.* Algebraic geometry is the study of curves (geometry) defined by polynomials (algebra). You may already familiar with some of these. For example, we will study lines, parabolas, circles, and more.

Problem 1. Plot the following curves in the plane. (If you're stuck, some things to try: complete the square, factor the expression, plug in numbers, or ask for help!)

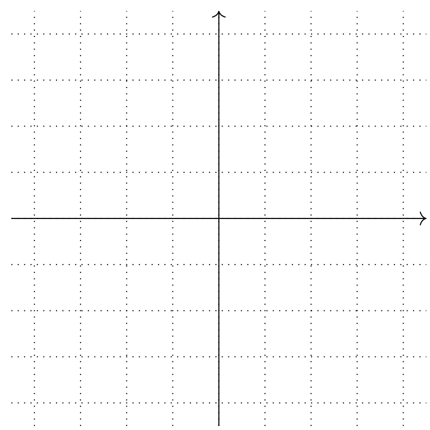
1. $x + 2y = 0$



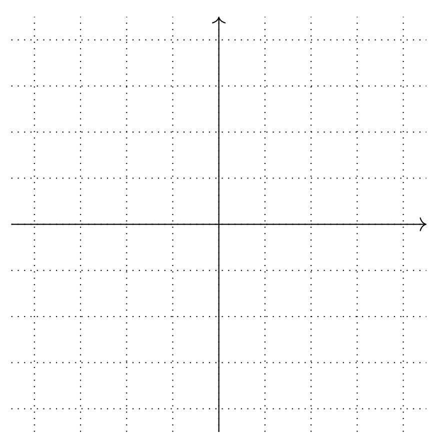
2. $x^2 + y^2 = 1$



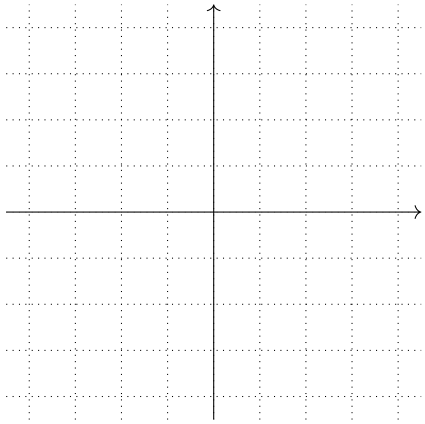
3. $x^2 + y^2 - 2y - 3 = 0$



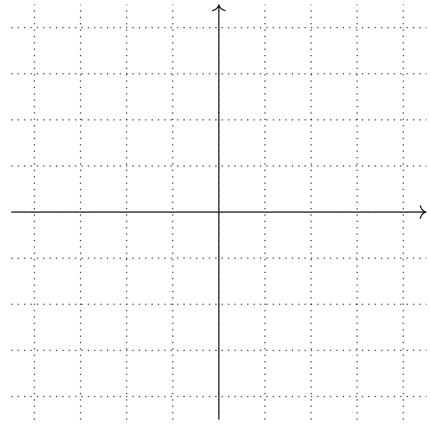
4. $xy - 4 = 0$



5. $x^2 = y^2$



6. (Challenge) $x^3 - xy^2 = 0$



A little different than what you might be used to: when we say "polynomial", we mean an expression that can include powers of both x and y. So the LHS of everything you graphed in Problem 1 is a polynomial. The *degree* of a polynomial with 2 variables is the largest sum of exponents in any term. For example, the polynomial $f(x, y) = x^2y + y$ has degree 3.

Problem 2. What were the degrees of the polynomials considered in Problem 1?

Given a polynomial $f(x, y)$, the set of points where $f(x, y) = 0$ (which is the curve that you have been graphing) is called the *zero set* of f. A single line is the zero set of a degree 1 polynomial. As you saw in Problem 1.2 through 1.5, there are lots of different shapes for zero sets of degree 2 polynomials: 1.2 and 1.3 are circles, 1.4 is called a *hyperbola*, a parabola is also possible (for example, $f(x, y) = x^2 - y$), and 1.5 is two lines.

Today's main question is: How many *points of intersection* do two zero sets have? In other words, how many solutions are there to the system of equations $f(x, y) = 0$, $g(x, y) = 0$?

Problem 3. Let's practice solving systems of equations. (Hint: draw their graphs!)

1. $\begin{cases} x^2 - y = 0 \\ x - 1 = 0 \end{cases}$

2. $\begin{cases} x^2 - y^2 = 0 \\ x - y = 0 \end{cases}$

3. $\begin{cases} x^2 + y^2 - 2 = 0 \\ (x-2)^2 + y^2 - 2 = 0 \end{cases}$

4. (Challenge) $\begin{cases} xy = 1 \\ x^2 + y^2 = \frac{17}{4} \end{cases}$

Problem 4. How many intersections could there be between the zero sets of... (list *all* the possibilities!)

1. ...two degree 1 polynomials?

2. ...one degree 1 polynomial and one degree 2 polynomial?

3. ...two degree 2 polynomials?

Problem 5. Let $f(x, y)$ have degree n and $g(x, y)$ have degree m. Make a conjecture about how the number of intersections between $f = 0$ and $g = 0$ relates to n and m.

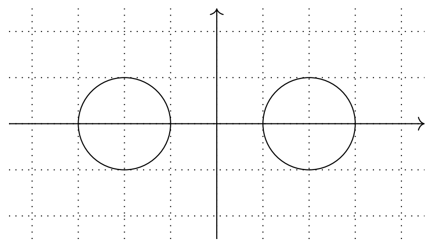
However, this situation is rather unsatisfactory. In some sense, whenever the number of intersections is not exactly mn, it feels like some kind of "edge case": maybe the lines are parallel, or two curves are tangent rather than intersecting, etc. **Our goal is to find a sense in which the number of intersections is *always exactly mn.*** This is called Bézout's theorem, and we'll spend this class and next class figuring it out.

We can actually quickly identify the case of infinite intersections. Based on Problem 3.2, you might already have a clue...

Problem 6. We will investigate polynomials whose zero sets have infinitely many intersections.

1. Read Problem 3.2 again. Using geometric reasoning about their zero sets, why were there infinitely many solutions?

2. Find the polynomial $f(x, y)$ such that $f(x, y) = 0$ is the following shape:



3. When do two zero sets have infinitely many intersections? (Not asking for a proof, just an answer.)

   This is an important question to get correctly, so call an instructor to check once you have your answer.

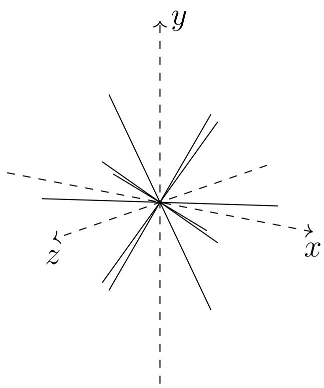
From now on, we will assume that our polynomials don't have a common factor, so the number of intersections will be finite. Now, it just remains to figure out why two zero sets could appear to be "missing" intersections, i.e. have fewer intersections than the product of their degrees.

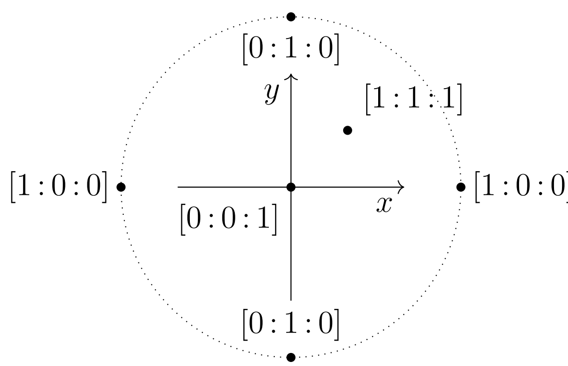
2 The projective planes $\mathbb{RP}^2$ and $\mathbb{CP}^2$

Two distinct lines almost always intersect at exactly one point, except a tiny annoying case when they don't: parallel lines. It's an edge case, because if you tweak the slope of one line just a little bit, they will intersect. Now we will find a world where this doesn't happen.

We define the *real projective plane* $\mathbb{RP}^2$ to be the set of lines through the origin in 3D space $\mathbb{R}^3$ (left picture). When write the ratio $[x:y:z]$, we refer to the line passing through the origin and (x, y, z). It's a ratio because all multiples of (x, y, z) are on the same line.

Another visualization (right) takes the intersection of all these lines with the plane $z = 1$. Every line (except those on the xy-plane) intersects $z = 1$ at exactly one point, giving a copy of the plane $\mathbb{R}^2$. The lines on the xy-plane create an extra "ring of infinities" around $\mathbb{R}^2$.





Based on the second picture, even though our lines of $\mathbb{RP}^2$ lie in 3D space, the space itself really behave more like a 2D space. So let me introduce some potentially confusing words. Define a *projective point* to be a line through the origin in $\mathbb{R}^3$.

Problem 7. Let's play around with projective points.

1. In the picture on the left, draw the line corresponding to the projective point $[1:0:0]$. Why do we write $[1:0:0]$ in two places in the right picture?

2. In the picture on the right, draw all of the dots corresponding to the projective points $[-1:-2:1]$ and $[-1:1:0]$.

3. How would you update the picture on the right if you had to draw in the projective point $[100:100:1]$?

Problem 8. We would like to arrive at a satisfactory definition of a "projective line".

1. In the picture on the right, draw the "projective line" between the projective points $[0:0:1]$ and $[1:1:1]$, as you would expect. Now try to visualize what you've drawn in the picture on the left. What is the shape of a projective line in the picture on the left?

2. With your visual description, explain why every two distinct projective lines intersect at exactly one projective point. (Solving the parallel lines problem!)

3. "A line that looks like $Ax + By + C = 0$ in the picture on the right corresponds to the plane $Ax + By + Cz = 0$ in the picture on the left." Explain this claim.

4. Find the equation of the projective line between $[0:0:1]$ and $[1:1:1]$.

5. (Challenge) Find the equation of the projective line between $[1:0:0]$ and $[0:1:0]$.

Notice that because projective points are really ratios, an equation in $\mathbb{RP}^2$ only makes sense if whenever $[x:y:z]$ is a solution, then so is $[kx:ky:kz]$. For example, the projective line $Ax+By+Cz=0$ described in Problem 8.3 makes sense, because if $Ax+By+Cz=0$, we also have $A(kx)+B(ky)+C(kz)=k(Ax+By+Cz)=k\cdot 0=0$.

Problem 9. Explain why a polynomial equation makes sense in $\mathbb{RP}^2$ if and only if every term has the same degree.

We say that a polynomial $f(x,y,z)$ is *homogeneous* if all of its terms have the same degree. Much like the equivalence in Problem 8.3, one can convert between general polynomials over $\mathbb{R}^2$ and homogeneous polynomials over $\mathbb{RP}^2$. The *homogenization* of a polynomial $f(x,y)$ of degree n is the polynomial

$$\hat{f}(x,y,z)=z^n f(\tfrac{x}{z},\tfrac{y}{z}).$$

Problem 10. Let's explore homogenization.

1. Show that $\hat{f}$ is always homogeneous.

2. Show that $f(x,y)=\hat{f}(x,y,1)$ for all x and y. (Hence, dehomogenizing a polynomial just means intersecting with $z=1$, as in the second picture.)

The last thing to note is that we have been using $\mathbb{RP}^2$ to draw useful pictures, but as you might expect, it's helpful mathematically to instead work in $\mathbb{CP}^2$, the complex projective plane. It's entirely analogous to how $x^2 + 1 = 0$ has two solutions over $\mathbb{C}$ but zero over $\mathbb{R}$.

Problem 11. For each of the following systems of equations (in $\mathbb{C}^2$), convert them to homogeneous polynomials and find all projective solutions (in $\mathbb{CP}^2$). How many solutions are there over $\mathbb{R}^2$ vs $\mathbb{CP}^2$? Is the number you expect by looking at degrees?

1. $y = x^2$ and $x = 1$.

2. $y = x^2 + 1$ and $y = 0$.

3. (Challenge) $x^2 + y^2 = 1$ and $x^2 + y^2 = 4$.

For some of these systems, we're still missing a few intersections. To figure how to find them, see you next week!

3 Bonus: Infinite intersections, reprise

At the end of section 1, we claimed that the zero sets of f and g have infinitely many intersections if and only if f and g have a common factor, but we didn't prove it.

Problem 12. Which direction of the if and only if is easy to prove?

To prove the harder direction, we will need an unexpected tool: Bézout's lemma from number theory. (The same Bézout as our main theorem! But in a seemingly different area of math.)

Bezout's lemma states that for all integers x and y, there exists integers a and b such that $\gcd(x, y) = ax + by$ (the greatest common divisor). Moreover, we can find a and b using the following procedure, known as the Euclidean algorithm. (We demonstrate with $x = 122$ and $y = 100$.) Using long division, we write:

$$\begin{aligned}
122 \div 100 &= 1 \text{ remainder } 22 \\
100 \div 22 &= 4 \text{ remainder } 12 \\
22 \div 12 &= 1 \text{ remainder } 10 \\
12 \div 10 &= 1 \text{ remainder } 2 \\
10 \div 2 &= 5 \text{ remainder } 0
\end{aligned}$$

In each step, we divide the previous dividend by the previous remainder, and we end when the remainder is 0. The GCD is the last non-zero remainder (2), and we can substitute equations backwards to recover:

$$\begin{aligned}
2 &= 12 - 1 \times 10 \\
&= 12 - 1 \times (22 - 12 \times 1) && = 2 \times 12 - 1 \times 22 \\
&= 2 \times (100 - 22 \times 4) - 1 \times 22 && = 2 \times 100 - 9 \times 22 \\
&= 2 \times 100 - 9 \times (122 - 100 \times 1) && = 11 \times 100 - 9 \times 122
\end{aligned}$$

So $a = -9$ and $b = 11$ works.

Problem 13. Find one integer solution to the equation $34a + 13b = 1$.

Problem 14. In this problem, we complete the proof that the zero sets of f and g have finitely many points of intersection if and only if they have no common components.

1. Adapt the Euclidean algorithm to show that for any polynomials $f(x)$ and $g(x)$, there exist polynomials $p(x)$ and $q(x)$ such that $\gcd(f, g) = pf + qg$. (This is not true for f and g with multiple variables. Why?)

2. Let $f(x, y)$ and $g(x, y)$ satisfy $\gcd(f, g) = 1$. Prove that there exist polynomials $p(x, y)$, $q(y)$, $r(x, y)$, and $s(y)$ such that

$$1 = \frac{pf}{q} + \frac{rg}{s}.$$

3. Prove that the zero sets of f and g have no common components if and only if their zero sets have finitely many points of intersection.