

Math 495 Handout: February 12, 2008

Alex Kasman
Department of Mathematics
College of Charleston

A Glimpse of Algebraic Geometry: Elliptic Curves

- What is algebraic geometry? At its simplest, it is the observation of Descartes that you all know well: if we use variables like x and y to represent coordinates in a space, then the set of points satisfying equations like $y = x^2$ form a geometric object that we can study. A deeper observation, which we will see today, is that these objects inherit an algebraic structure of their own. At its most extreme, algebraic geometry is the realization that you can associate a geometric object of some sort to *any* commutative algebra (the object is called a “scheme” and this theory is due to Grothendieck)...and then beyond that there is even non-commutative geometry. But, I don't think we will be doing either of those things here.

➤ Some algebraic geometry that you know:

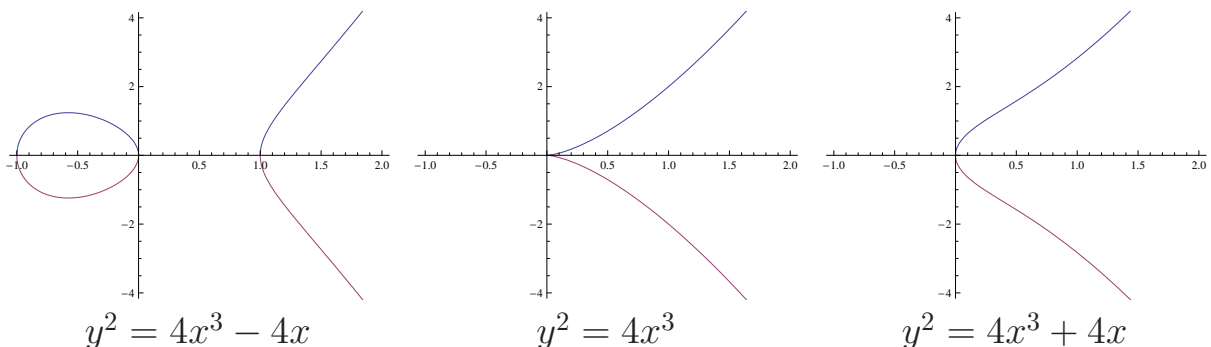
- **The Object:** What curve is associated to the equation $x^2 + y^2 = 1$? Of course, it is the unit circle centered at the origin in the xy -plane. That's because this equation is equivalent to saying that the distance from the point to the origin is exactly equal to 1.
- **Generating Function:** Can you think of a function $f(z)$ with the property that $x = f(z)$ and $y = f'(z)$ will give a point on the circle for every choice of z ...and every point on the circle comes from some choice of z ? (In other words, $r(z) = \langle f(z), f'(z) \rangle$ parametrizes the circle.)
- **An Algebraic Structure:** Let p and q be two points on the circle. I want to come up with a rule for *adding* them to get another point on the circle. (I want the circle to be “closed under addition”.) We can do this: add the angle they make with the x axis and take the point at that new angle.

➤ Something More interesting – Elliptic Curves:

- **The Object:** *Almost* as famous as the circle is the curve with equation:

$$y^2 = 4x^3 - k_1x - k_2.$$

This gives an *elliptic curve*. This is not to be confused with an “ellipse” (which is just a squashed circle). Depending on the values of k_1 and k_2 , the elliptic curve will look basically like one of these diagrams:



You can tell what the graph will look like by considering the number $27k_2^2 - k_1^3$. If this number is positive then the graph has two components. If it is negative then it has one component. (Technically, if it is zero then the curve is not actually an elliptic curve but rather a *singular* elliptic curve, which many people consider to be a different beast altogether.)

Question 1: What do these different situations have to do with the graph of the function $f(x) = 4x^3 - k_1x - k_2$?

- You may be wondering why we only consider the coefficient 4 on the x^3 term and 0 on the x^2 term. There really is no reason. In fact, the cubic polynomial on the right could be arbitrary and it would still be an elliptic curve...but as we will see, we can always put it in this form by an appropriate change of coordinates.
- Elliptic curves may not be quite as well known as circles...but they are really very famous and useful. There are methods of cryptography based on elliptic curves. The proof of Fermat's Last Theorem depends on elliptic curves. And, as we will see, they show up very naturally in the context of the KdV equation.
- **Generating Function:** There is a function called the "Weierstrass p-function" written $\wp(z; k_1, k_2)$ (or just $\wp(z)$ for short if k_1 and k_2 are understood) which has the property that for every z in its domain, $x = \wp(z)$ and $y = \wp'(z)$ satisfy the equation of the elliptic curve. Although every point on the curve comes from some value of z , there are z 's for which these functions are undefined. ($\wp(0)$, for instance, is never defined.) However, this makes sense since people like to think of there being a "point at infinity" on the curve that closes it off and when the generating functions are undefined, it just means that we are at that point.
- What is the "formula" for \wp ? Well, there is an infinite series expansion that you can find in books or on the Web. But, that's as close as you get to a "formula" for it. (Seems disappointing? Don't forget, that's all we have for sine and cosine, too!) You won't need this series expansion for this class, but we will be working with Mathematica. Note that they are written `WeierstrassP[z, {k1, k2}]` and `WeierstrassPPrime[z, {k1, k2}]`. Mathematica can manipulate them symbolically and can also compute approximate values of them from the infinite series definition.

Question 2: Define `p[z_] := WeierstrassP[z, {4, 0}]` in Mathematica and verify that it satisfies $p'[z]^2 - 4p[z]^3 + 4p[z] = 0$.
(Mathematica doesn't seem to know that this expression should be true. How can we check?)

So, for any choice of k_1 and k_2 , we know that $\wp(z; k_1, k_2)$ solves the differential equation

$$(\wp')^2 = 4\wp^3 - k_1\wp - k_2.$$

Question 3: There must be more than just one solution. We need a free parameter (a "constant of integration") somewhere. Where can I insert a constant γ into the solution so that it still satisfies the same equation?

- Actually, the best way to think of this "constant" is as a *point on the curve*. Consider "there is a solution to this equation for every point on the curve". Not only is this a nice way of saying it, it takes into account the fact that you can select different values of the constant that still result in the same function because of its periodicity *and* is easily recognized in the fact that plugging $z = 0$ into the function and its derivative will give you the coordinates of that point!

Question 4: What equation does the function $w(z) = a\wp(z) + b$ satisfy? (Note: This is the same idea as changing variables on the curve to get a more general cubic polynomial on the right hand side.)

- **Group Law:** The group law on an elliptic curve is simple, cool and important. To add points p and q on the curve, you draw a straight line through them. The line will intersect the curve at one more point. Take that point and reflect it across the x -axis. The result is what we call $p + q$. (Well, it is possible that the line does not intersect the curve at another point. If that happens, then the “third point” is the point at infinity. The point at infinity stays the same when it is reflected across the x -axis and so that would be the sum in that case.) Using these rules makes the elliptic curve into an actual group according to the traditional definitions of algebra.

Question 5: A group needs an “identity element”, which when added to a point leaves it the same. In this case, that identity element is the point at infinity. A group also needs an inverse for every element. What is the inverse of a point p ?

- **The p-function respects the group law!** Suppose p and q are points on the elliptic curve and such that $p = (\wp(z_1), \wp'(z_1))$ and $q = (\wp(z_2), \wp'(z_2))$. Then the point $p + q$ has coordinates $(\wp(z_1 + z_2), \wp'(z_1 + z_2))$! I hope you can see how amazing this is. It means that the ordinary addition of numbers gets turned into the group law on the elliptic curve by the p-function. Because of the periodicity of the p-function, this means that the group law on the elliptic curve is something like addition in modular arithmetic where you can add any two numbers but then just take the remainder after the quotient.
- **Complex Numbers:** I am supposing that somewhere in your training you have encountered the imaginary number i which satisfies $i^2 = -1$. Despite the misleading names “imaginary” and “complex”, it turns out that working with this number can actually make many real mathematics problems much simpler. That is the case both with solitons and with elliptic curves. If there is interest, we could spend much more time on this particular topic later. At this point, however, I only want to mention one idea which will be important to our current goal of connecting soliton equations and elliptic curves.

➤ **Sometimes you can add an imaginary number to the argument of a real function and get another real function!** This may seem strange. For instance, if I start with a function like $f(x) = x^2$ then it is clear that f will give a real number output for every real number input. However, if I make a new function $g(x) = f(x + i)$ then when I put in a real number like $x = 2$ I get $g(2) = (2 + i)^2 = 4 + 4i - 1 = 3 + 4i$...a complex number. However, if the formula and the constant added are chosen just right, then it can be possible to get from one real function to another this way.

- For example, you will recall that we saw earlier in the course the identity

$$\sin(x + \pi) = -\sin(x).$$

As it turns out, a similar formula applies to the related function $\sinh(x)$ (the hyperbolic sine). We get

$$\sinh(x + i\pi) = -\sinh(x).$$

(If you want to check this or understand better why it works, you can rewrite \sinh in terms of exponential functions and use the famous formula $e^{\pi i} = -1$.)

- The reason this is relevant is that in the case of the elliptic curves whose (real) graphs are made up of two separate components, you need to add an imaginary constant to jump from one component to the other. That is, there is a constant γ so that $\wp(z + \gamma i)$ still takes real values for every real number z plugged into it...but now the function is periodic without singularities!
- This imaginary number you can add to z is called a “half period” and it depends on k_1 and k_2 . Mathematica even claims to be able to find them for you with `WeierstrassHalfPeriods[{k1, k2}]` ...but I have found that usually it doesn't know what they are either.
- The important point will be the way all of this relates to *solitons* and we will see that next time.

Homework

1. In this question we will consider the elliptic curve with equation

$$y^2 = 4x^3 - 28x + 24.$$

- (a) There are two points on the curve with x coordinate equal to 3. What are the coordinate of those points?
 - (b) Find the sum of the points $p = (2, 0)$ and $q = (0, 2\sqrt{6})$. (That is, I want you to apply the geometric method of adding points to find the third point on the curve which is their sum. This will involve finding the equation of the line containing those points and solving for the third point. Show all steps and explain what you're doing.)
2. What would you do to add a point on the elliptic curve to *itself*? Use concepts from Calc 1 in a well argued paragraph to explain why this method makes sense.
 3. The function

$$f(x) = 3\wp(x + 9; 2, -5) + 8$$

satisfies the differential equation $(f')^2 = af^3 + bf^2 + cf + d$. What are a, b, c and d ?