Arithmetic on Curves (with pictures!)

by Shrenik Shah

We are going to define and explore basic properties of curves in the first part of this lecture. In the second part, we will explain the arithmetic of curves and mention some applications to cryptography.

Introduction

You are all already familiar with curves. Some examples you have seen include $y = x^2$, $y = x^3 - x$, and $x^2 + y^2 = 1$.

In fact, for any polynomial p, $p(x, y) = 0$ defines a curve. We can take the polynomial to have rational, real, or complex coefficients, and define the curve to be the solutions to that polynomial over $\mathbb{Q}^2, \mathbb{R}^2$, or $\mathbb{C}^2$. The curves of the form $y = f(x)$ are called *graphs*, and constitute the majority of the curves you have seen before.

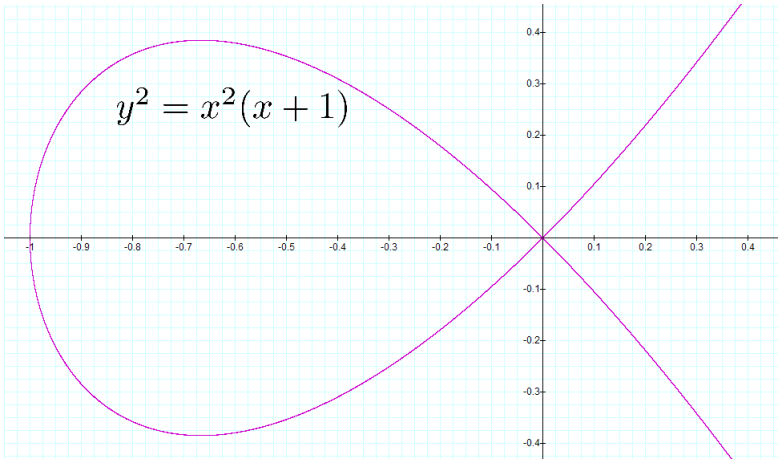
Curves can have interesting properties: Consider $y^2 = x^3$ and $y^2 = x^2(x + 1)$. Both of these curves have a point that appears differently than the others on the curve. In $y^2 = x^3$, the point $(0, 0)$ is "sharp" in a sense; we call this phenomenon a *cusp*. The point $(0, 0)$ in $y^2 = x^2(x + 1)$ has two parts of the curve passing through it, and is called a *node*.

Maps

We can see the coordinate x as actually defining a map between the points of the curve C and the x-axis. Indeed, given a point (x_0, y_0), the map x sends this point to x_0. Similarly, the map y sends this point to y_0. We can define new maps by adding and multiplying these maps, so in fact, every polynomial $q(x, y)$ defines a map on C. Moreover, two polynomials $q_1(x, y)$ and $q_2(x, y)$ define the same map if $q_1(x, y) - q_2(x, y)$ is a function that maps the entire curve to 0. One such function is $p(x, y)$. We'll define a map from a curve C to an n-dimensional space to be given by a polynomial $q_i(x, y)$ in each coordinate. If a bijective map has an inverse map, we call it an isomorphism.

As an example, any graph $y = f(x)$ is isomorphic via the map x to the x-axis, since this map has the inverse $x \mapsto (x, f(x))$.

Another example, which is not quite a map in the sense we just described, allows us to map the curve $y^2 = x^2(x + 1)$ to the x-axis as well. Can you see a way to find a similar map for the curve $y^2 = x^3$?



Pythagorean Triples

An application of the idea of a "map" just discussed allows one to parametrize Pythagorean triples. Consider the curve $x^2 + y^2 = z^2$, where $x, y, z \in \mathbb{Z}$ are integers. These points lie on the curve $\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$, or

$X^2+Y^2=1$, over $\mathbb{Q}^2$. Given a point (X,Y) on this curve, the line connecting this point and $(1,0)$ has rational slope. We'll in fact show the converse; one can obtain any point on the curve by picking a rational slope t and computing the point (X,Y) on the intersection of the line of slope t through $(1,0)$ with the curve. This line has the form $Y=t(X-1)$. Then $1=X^2+t^2(X-1)^2$, which we rewrite as $(t^2+1)X^2-2t^2X+(t^2-1)=0$. Using the quadratic formula, which gives

$$X=\frac{2t^2\pm\sqrt{4t^4-4(t^2+1)(t^2-1)}}{2(t^2+1)}=\frac{t^2\pm1}{t^2+1}$$

we obtain the second solution $X=\frac{t^2-1}{t^2+1}$. The corresponding value of Y, given by $Y=t(X-1)$, is given by $X=\frac{2t}{t^2+1}$. One can check that $X^2+Y^2=1$, as we wanted. This gives us all the *rational* points on the curve; with a few more observations you can figure out all the integer points on the curve.

Elliptic Curves

Let us focus on a special class of curves: those of the form $y^2=x^3+ax+b$. (We will require a technical constraint on discriminant of the polynomial x^3+ax+b, but it will be simpler to avoid this consideration for now.)

Note that on $\mathbb{C}$, $\mathbb{R}$, or $\mathbb{Q}$, we have an operation $+$ which assigns to two numbers s,t their "sum" $s+t$. The sum satisfies $s+t=t+s, (r+s)+t=r+(s+t)$, and has an identity element 0. We will find that the points on the curve $y^2=x^3+ax+b$ will have a similar property.

Given two points $P_1=(x_1,y_1), P_2=(x_2,y_2)$ on this curve, we can form the slope of the line between these points, $m=\frac{y_1-y_2}{x_1-x_2}$. (We will deal with the special case where $x_1=x_2$ later.) Then the line itself can be written down using the formula $y=m(x-x_1)+y_1$. As we will show, this line intersects the curve in a third point, which we shall solve for by substituting this expression for y: $(m(x-x_1)+y_1)^2=x^3+ax+b$, or

$$x^3-m^2x^2+(-2my_1+2m^2x_1+a)x-m^2x_1^2+2mx_1y_1-y_1^2+b.$$

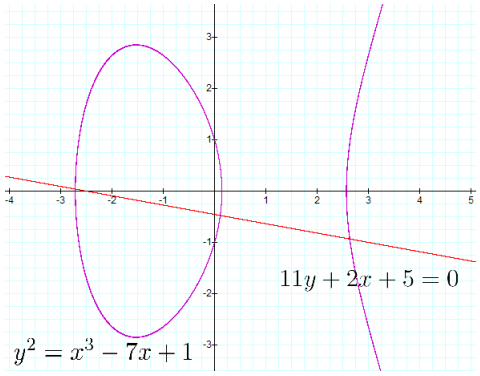
Since the coefficient m^2 is the sum of the roots of the polynomial, which one can show by expanding

$$(x-r_1)(x-r_2)(x-r_3)=x^3-(r_1+r_2+r_3)x^2+(r_1r_2+r_2r_3+r_3r_1)x-r_1r_2r_3,$$

while x_1,x_2 are already roots, we can find the x-coordinate of the third point as $x_3=m^2-x_1-x_2$, and the y-coordinate from the equation of the line, $y_3=m(x_3-x_1)+y_1$.

We *define* $P_1+P_2+P_3=0$, or $P_1+P_2=-P_3$. We define the *negation* of a point to simply be its reflection over the x-axis, meaning that $-(x,y)=(x,-y)$. The third point on this line connecting (x,y) and $(-x,y)$ is the point at infinity, and the identity of this additive group. Note that adding a point to itself cannot be done with the formula above; one needs to use a *tangent line* to the curve for this.

As an example, the following is a graph of $y^2=x^3-7x+1$, with the line $11y+2x+5=0$ drawn.



Projective Space

In the above, we had to talk about a "point at infinity," which turned out to be the identity element of the group. It turns out that a kind of space called projective space allows one to think concretely about "points at infinity," by adding points in geometrically clear ways. Formally, the projective plane is defined to be all 3-tuples $[X, Y, Z]$ where $X, Y, Z \in \mathbb{R}$ (or $\mathbb{C}$ or $\mathbb{Q}$, for example), except that we call $[X, Y, Z]$ and $[\lambda X, \lambda Y, \lambda Z]$, where $\lambda \neq 0$, the same point. We also don't include $[0, 0, 0]$. Then the points of the form $[x, y, 1]$ form the usual plane $\mathbb{R}^2$, but points of the form $[x, y, 0]$ where $(x, y) \neq (0, 0)$ form the points at infinity. Geometrically, we add a point at infinity corresponding to the slope of every line in the plane, so that every line meets itself at infinity.

An Application to Cryptography

We'll show how to send secret messages using elliptic curves. This algorithm is called "Elgamal Public Key Encryption."

Setup: Suppose that Bob wants to be able to receive secret messages. He publishes an elliptic curve E, p, a point P, and the point sP, where s is his secret key.

Encryption: Alice sends her message M, which is encoded as a point on the curve E, by picking a secret integer r and computing and sending $C_1 = rP$, $C_2 = M + rsP$.

Decryption: Bob decrypts the message M by computing $C_2 - sC_1 = M$.

Geometry of Elliptic Curves over $\mathbb{C}$

This is just a last comment that will seem particularly mysterious: While elliptic curves over $\mathbb{C}$ seem to be hard to visualize, they can be rather helpful in understanding their geometry better. Over $\mathbb{C}$, an elliptic curve is none other than a than the surface of a "doughnut." Indeed, one can find a map that shows that the points of an elliptic curve are naturally in bijection with the points of $\mathbb{C}/\Lambda$, where $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$, where $\text{Im } \tau > 0$. This allows one to both classify elliptic curves and tell whether two elliptic curves are the same. Moreover, $\mathbb{C}/\Lambda$ has an obvious addition rule given by arithmetic, which is exactly the same as addition of points on E.

Concluding Remarks

If you want to:

- Read more about elliptic curves and cryptography: Ask me and I'll send you the latest draft of an expository paper on the subject I'm writing for the *Harvard College Mathematics Review*. My email address is ⟨nilradical@gmail.com⟩.
- Learn more about curves in general: A good book written by Frances Kirwan is *Complex Algebraic Curves*.
- Learn about elliptic curves from the perspective of complex analysis: Lars Ahlfors' text *Complex Analysis* is an excellent introduction.
- Learn more about the arithmetic of elliptic curves: Joseph Silverman and John Tate have an excellent book called *Rational Points on Elliptic Curves*.