EECS 70 Discrete Mathematics and Probability Theory
Summer 2021

Note 9

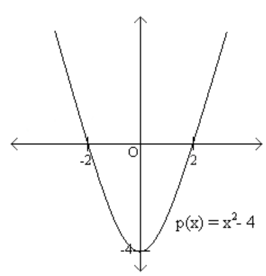
Polynomials

Polynomials constitute a rich class of functions which are both easy to describe and widely applicable in topics ranging from Fourier analysis, cryptography and communication, to control and computational geometry. You've seen them earlier in many contexts like Taylor approximation and other contexts in EECS16B, and so they are familiar to you. In this note, we will discuss further properties of polynomials which make them so useful. The key idea here is to extend what you already know about polynomials over the real and complex numbers to modulo arithmetic. We will then describe how to take advantage of these properties to develop a secret-sharing scheme.

Recall that a *polynomial* in a single variable is an expression that has an associated function.[1] The polynomial expression $p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$. Here the *variable* x and the *coefficients* a_i are usually real numbers. For example, $p(x) = 5x^3 + 2x + 1$ is a polynomial of *degree* $d = 3$. Its coefficients are $a_3 = 5$, $a_2 = 0$, $a_1 = 2$, and $a_0 = 1$. Polynomials have some remarkably simple, elegant and powerful properties, which we will explore in this note.

The polynomial function can be viewed as a function in some domain with multiplication and addition operations, by evaluating the expression in the natural manner. For example, $p(x) = 5x^3 + 2x + 1$ can be evaluated at $x = 3$ and to obtain $p(3) = 5(3)^3 + 2(3) + 1 = 142$.

To proceed, a familiar definition: we say that a is a *root* of the polynomial $p(x)$ if $p(a) = 0$. For example, the degree 2 polynomial $p(x) = x^2 - 4$ has two roots, namely 2 and -2, since $p(2) = p(-2) = 0$. If we plot the polynomial $p(x)$ in the x-y plane, then the roots of the polynomial are just the places where the curve crosses the x axis:



We now state two fundamental properties of polynomials that we will prove in due course.

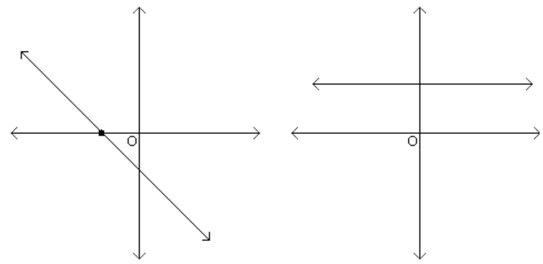
Property 1: A non-zero polynomial of degree d has at most d roots.

Property 2: Given $d+1$ pairs $(x_1, y_1), \ldots, (x_{d+1}, y_{d+1})$, with all the x_i distinct, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i) = y_i$ for $1 \le i \le d+1$.

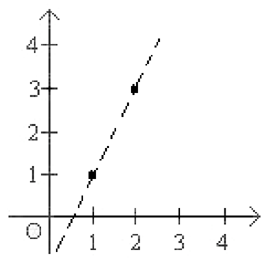
Let us consider what these two properties say in the case that $d = 1$. A plot over the reals of a linear (degree

[1] In the reals, the association is unique. In modular arithmetic modulo a prime p, it isn't necessarily unique as modulo p, by Fermat's Little Theorem, $x^p = x \mod p$ for a prime p. Still, there is a uniquely associated polynomial expression to a function where the expression does not have terms with exponents larger than $p-1$ under arithmetic modulo a prime p. Our applications generally assume that this is the expression we are working with.

1) polynomial $y = a_1x + a_0$ is a line that may not go through the origin. Property 1 says that if a line is not the x-axis (i.e., if the polynomial is not $y = 0$), then it can intersect the x-axis in at most one point.



Property 2 says that two points uniquely determine a line.



Polynomial Interpolation

Property 2 says that two points uniquely determine a degree 1 polynomial (a line), three points uniquely determine a degree 2 polynomial, four points uniquely determine a degree 3 polynomial, and so on. Given $d+1$ pairs $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, how do we determine the polynomial $p(x) = a_dx^d + \cdots + a_1x + a_0$ such that $p(x_i) = y_i$ for $i = 1$ to $d+1$? We will give an algorithm for reconstructing the coefficients $a_0, \dots, a_d$, and therefore the polynomial $p(x)$. Another standard algorithm that is more clearly linear-algebraic is described in the next note, because it will be important as a stepping stone.

The method here is called *Lagrange interpolation* and it should remind you of the Chinese Remainder Theorem: Let us start by solving an easier problem. Suppose that we are told that $y_1 = 1$ and $y_j = 0$ for $2 \le j \le d+1$. Now can we reconstruct $p(x)$? Yes, this is easy! Consider $q(x) = (x - x_2)(x - x_3) \cdots (x - x_{d+1})$. This is a polynomial of degree d (the x_i's are constants, and x appears d times). Also, we clearly have $q(x_j) = 0$ for $2 \le j \le d+1$. But what is $q(x_1)$? Well, $q(x_1) = (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_{d+1})$, which is some constant not equal to 0 (since x_1 is not equal to any of the other x_i). Thus if we let $p(x) = q(x)/q(x_1)$ (dividing is ok since $q(x_1) \neq 0$), we have the polynomial we are looking for. For example, suppose you were given the pairs $(1,1)$, $(2,0)$, and $(3,0)$. Then we can construct the degree $d = 2$ polynomial $p(x)$ by letting $q(x) = (x-2)(x-3) = x^2 - 5x + 6$, and $q(x_1) = q(1) = 2$. Thus, we can now construct $p(x) = q(x)/q(x_1) = (x^2 - 5x + 6)/2$.

Of course, the problem is no harder if we single out some arbitrary index i instead of 1: i.e. $y_i = 1$ and $y_j = 0$ for $j \neq i$. Let us introduce some notation: denote by $\Delta_i(x)$ the degree d polynomial that goes through these $d+1$ points. Then $\Delta_i(x) = \frac{\Pi j \neq i (x - x_j)}{\Pi j \neq i (x_i - x_j)}$.

We now return to the original problem. Given $d+1$ pairs $(x_1, y_1), \dots, (x_{d+1}, y_{d+1})$, we first construct the $d+1$ polynomials $\Delta_1(x), \dots, \Delta_{d+1}(x)$ as described above. Now we claim that we can write $p(x) = \sum_{i=1}^{d+1} y_i \Delta_i(x)$. Why does this work? First notice that $p(x)$ is a polynomial of degree d, as required, since it is the sum of polynomials of degree d. And when it is evaluated at x_i, d of the $d+1$ terms in the sum evaluate to 0 and the i-th term evaluates to y_i times 1, as required.

In the above construction, we can think of the polynomials $\Delta_i(x)$ as a "natural basis" for all polynomials whose values are specified at the points $\{x_j\}$. Note that these basis polynomials depend only on the x_j, and not on the values y_j at the points. We then sum the basis polynomials Δ_i, with coefficients equal to the values y_i, to construct the desired polynomial $p(x)$.

As an example, suppose we want to find the degree-2 polynomial $p(x)$ that passes through the three points $(x_1,y_1)=(1,1)$, $(x_2,y_2)=(2,2)$ and $(x_3,y_3)=(3,4)$. The three polynomials Δ_i are as follows:

$$\Delta_1(x)=\frac{(x-2)(x-3)}{(1-2)(1-3)}=\frac{(x-2)(x-3)}{2}=\frac{1}{2}x^2-\frac{5}{2}x+3;$$
$$\Delta_2(x)=\frac{(x-1)(x-3)}{(2-1)(2-3)}=\frac{(x-1)(x-3)}{-1}=-x^2+4x-3;$$
$$\Delta_3(x)=\frac{(x-1)(x-2)}{(3-1)(3-2)}=\frac{(x-1)(x-2)}{2}=\frac{1}{2}x^2-\frac{3}{2}x+1.$$

The polynomial $p(x)$ is therefore given by

$$p(x)=1\cdot\Delta_1(x)+2\cdot\Delta_2(x)+4\cdot\Delta_3(x)=\frac{1}{2}x^2-\frac{1}{2}x+1.$$

You should verify that this polynomial does indeed pass through the above three points.

Proof of Property 2

We are now in a position to prove Property 2 stated earlier, namely:

Property 2: Given $d+1$ pairs $(x_1,y_1),\dots,(x_{d+1},y_{d+1})$, with all the x_i distinct, there is a unique polynomial $p(x)$ of degree (at most) d such that $p(x_i)=y_i$ for $1\le i\le d+1$.

We have shown above how to find a polynomial $p(x)$ such that $p(x_i)=y_i$ for $d+1$ pairs $(x_1,y_1),\dots,(x_{d+1},y_{d+1})$. This proves part of Property 2 (the existence of the polynomial). How do we prove the second part, that the polynomial is unique? Suppose for contradiction that there is another polynomial $q(x)$ such that $q(x_i)=y_i$ for all $d+1$ pairs above. Now consider the polynomial $r(x)=p(x)-q(x)$. Since we are assuming that $q(x)$ and $p(x)$ are different polynomials, $r(x)$ must be a non-zero polynomial of degree at most d. Therefore, Property 1 (to be proved below) implies it can have at most d roots. But on the other hand $r(x_i)=p(x_i)-q(x_i)=0$ at $d+1$ distinct points x_i, so $r(x)$ has at least $d+1$ roots. Contradiction. Therefore, $p(x)$ is the unique polynomial that satisfies the $d+1$ conditions.

Polynomial Division

Let's take a short digression to discuss polynomial division, which will be useful in the proof of Property 1. If we have a polynomial $p(x)$ of degree d, we can divide by a polynomial $q(x)$ of degree $\le d$ by using long division. The result will be:

$$p(x)=q'(x)q(x)+r(x)$$

where $q'(x)$ is the quotient and $r(x)$ is the remainder. The degree of $r(x)$ must be smaller than the degree of $q(x)$. We can compute the quotient and remainder using long division for polynomials, as illustrated in the following example.

Example. We wish to divide $p(x)=x^3+x^2-1$ by $q(x)=x-1$:

- First we subtract a factor $x^2(x-1)$ to write: $p(x) = x^2(x-1) + (2x^2-1)$.
- Then we subtract a factor $2x(x-1)$ to write the remainder as $2x^2 - 1 = 2x(x-1) + (2x-1)$.
- Then we subtract a factor $2(x-1)$ to write the remainder as $2x - 1 = 2(x-1) + 1$.
- Finally, putting the above three lines together, we get that $p(x) = (x^2+2x+2)(x-1)+1$.

Written out using notation that you might be familiar with:

$$
\begin{array}{r|l}
 & X^2 + 2X + 2 \\
\hline
X-1 & X^3 + X^2 \qquad - 1 \\
 & -X^3 + X^2 \\
\hline
 & 2X^2 \\
 & -2X^2 + 2X \\
\hline
 & 2X - 1 \\
 & -2X + 2 \\
\hline
 & 1
\end{array}
$$

Therefore, the quotient is $q'(x) = x^2+2x+2$, and the remainder is $r(x) = 1$.

Proof of Property 1

Now let us prove Property 1, which we restate from earlier:

Property 1: A non-zero polynomial of degree d has at most d roots.

The idea of the proof is as follows. We will prove the following two claims:

> **Claim 1** If a is a root of a polynomial $p(x)$ with degree $d \geq 1$, then $p(x) = (x-a)q(x)$ for a polynomial $q(x)$ with degree $d-1$.
>
> **Claim 2** A polynomial $p(x)$ of degree d with distinct roots $a_1, \ldots, a_d$ can be written as $p(x) = c(x-a_1)\cdots(x-a_d)$, where c is a real number.

Note that Claim 2 immediately implies Property 1: we just need to show that $a \neq a_i$ for $i = 1, \ldots d$ cannot be a root of $p(x)$. But this follows from Claim 2, since $p(a) = c(a-a_1)\cdots(a-a_d) \neq 0$.

Proof of Claim 1

Dividing $p(x)$ by $(x-a)$ gives $p(x) = (x-a)q(x) + r(x)$, where $q(x)$ is the quotient (of degree $d-1$) and $r(x)$ is the remainder. The degree of $r(x)$ is necessarily smaller than the degree of the divisor $(x-a)$. Therefore $r(x)$ must have degree 0 and therefore is some constant c. But now substituting $x = a$, we get $p(a) = c$. But since a is a root, $p(a) = 0$. Thus $c = 0$ and therefore $p(x) = (x-a)q(x)$.

Proof of Claim 2

Proof by induction on d.

- Base Case: $d = 0$. If $p(x)$ is a polynomial of degree 0 then it is simply a constant c, so it can trivially be written in the desired form.

- Inductive Hypothesis: For some $d \geq 0$, any polynomial of degree d with distinct roots $a_1, \ldots, a_d$ can be written as $p(x) = c(x-a_1)\cdots(x-a_d)$.
- Inductive Step: Let $p(x)$ be a polynomial of degree $d+1$ with distinct roots $a_1, \cdots, a_{d+1}$. By Claim 1, $p(x) = (x-a_{d+1})q(x)$ for some polynomial $q(x)$ of degree d. Since $0 = p(a_i) = (a_i - a_{d+1})q(a_i)$ for all $i \neq d+1$, and $a_i - a_{d+1} \neq 0$, $q(a_i)$ must be equal to 0. Thus $q(x)$ is a polynomial of degree d with distinct roots $a_1, \ldots, a_d$. We can now apply the inductive hypothesis to $q(x)$ to write $q(x) = c(x-a_1)\cdots(x-a_d)$. Substituting in $p(x) = (x-a_{d+1})q(x)$, we obtain $p(x) = c(x-a_1)\cdots(x-a_{d+1})$, as desired.

Finite Fields

Both Property 1 and Property 2 also hold when the values of the coefficients and the variable x are chosen from the complex numbers, or indeed the rational numbers, rather than from the real numbers. However, the proofs[2] do not go through if the values are restricted to being natural numbers or integers. Let us try to understand these facts a little more closely. The only properties of numbers that we used in polynomial interpolation and in the proofs of Properties 1 and 2 are that we can add, subtract, multiply and divide any pair of numbers as long as we are not dividing by 0. (You should go back and check this claim!) Therefore, everything holds just as well for the complex numbers and the rational numbers. On the other hand, we cannot subtract two natural numbers and guarantee that the result is a natural number, and dividing two integers does not generally result in an integer, so everything falls apart for natural numbers and integers.

However, if we work with numbers modulo a prime[3] m, then we can add, subtract, multiply and divide (by any non-zero number modulo m). To check this, recall that x has an inverse mod m if $\gcd(m,x) = 1$, so if m is prime *all* the numbers $\{1, \ldots, m-1\}$ have an inverse mod m. So both Property 1 and Property 2 hold if the coefficients and the variable x are restricted to take on values modulo m. This remarkable fact—that these properties hold even when we restrict ourselves to a *finite* set of values—is the key to several applications that we will presently see.

Let us consider an example of degree $d = 1$ polynomials modulo 5. Let $p(x) = 2x+3 \pmod 5$. The roots of this polynomial are all values x such that $2x+3 \equiv 0 \pmod 5$ holds. Solving for x, we get that $2x = -3 \equiv 2 \pmod 5$, and thus $x = 1 \pmod 5$. Note that this is consistent with Property 1 since we got only one root of a degree-1 polynomial.

Now consider the polynomials $p(x) = 2x+3 \pmod 5$ and $q(x) = 3x-2 \pmod 5$. We can plot the values y of each polynomial as a function of x in the x-y plane. Since we are working modulo 5, there are only 5 possible choices for x, and only 5 possible choices for y:

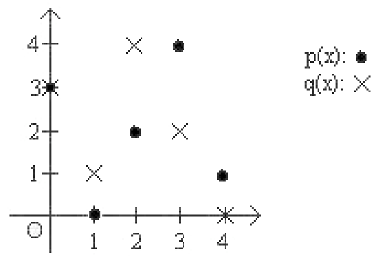
Notice that these two "lines" intersect in exactly one point, $(0,3)$, even though the picture looks nothing at all like lines in the Euclidean plane! Looking at these graphs it might seem remarkable that both Property 1 and Property 2 hold when we work modulo m for any prime number m. But as we stated above, all that was

[2]However, the result of property 1 does hold for polynomials with integer or natural number coefficients with the domain restricted to integers or natural numbers. That is because we have proved something *stronger* by going to the rationals or reals. If a polynomial has no more than d real roots, it certainly has no more than d integer roots. After all, every integer is a real number!

Meanwhile, property 2 does not hold at all if we restrict all the numbers involved to be integers. Try finding a straight line that goes through $(0,0)$ and $(2,1)$. It doesn't have integer coefficients.

[3]Again, it is useful to consider what happens if the m is not a prime. What happens to property 1? Consider $m = 8$ and the equation $x^3 = 0$. How many roots? 0 is a root for sure, but so are $2,4,6$. That is 4 distinct roots to a third-degree polynomial. This means that property 1 does not hold and neither does property 2.

Unlike in the case of the integers, we cannot simply embed the numbers mod 8 into a larger field for which the result holds. This goes to show that we must be careful. It turns out that there is a way construct a finite field with 8 elements, but it is not simply the integers mod 8.



required for the proofs of Properties 1 and 2 was the ability to add, subtract, multiply and divide any pair of numbers (as long as we are not dividing by 0). Therefore, they hold whenever we work with integers modulo a prime m.

When we work with numbers modulo a prime m, we say that we are working over a *finite field*, denoted by F_m or $GF(m)$ (for Galois Field). In order for a set to be called a field, it must satisfy certain axioms which are the building blocks that allow for these properties and others to hold. If you would like to learn more about fields and the axioms they satisfy, you can visit Wikipedia's site and read the article on fields: `http://en.wikipedia.org/wiki/Field_\%28mathematics\%29`. While you are there, if you are interested, you can also read the article on Galois Fields and learn more about some of their applications and elegant properties which will not be covered in this course: `http://en.wikipedia.org/wiki/Galois_field`. (Take Math 113 and Math 114 to really get into this stuff, or take EECS 229B which also covers many of these properties as it builds the fundamentals of error-correcting codes.)

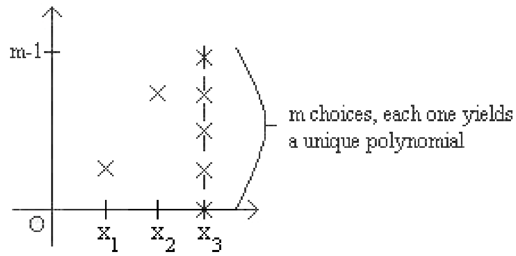
Counting

How many polynomials of degree (at most) 2 are there modulo m? This is easy: there are 3 coefficients, each of which can take on one of m values for a total of m^3. Writing $p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ by specifying its $d+1$ coefficients a_i is known as the *coefficient representation* of $p(x)$. Is there any other way to specify $p(x)$?

Yes, there is! Our polynomial of degree (at most) 2 is uniquely specified by its values at any three points, say $x = 0,1,2$. Once again, the polynomial can take any one of m values at each of these three points, for a total of m^3 possibilities. In general, we can specify a degree d polynomial $p(x)$ by specifying its values at $d+1$ points, say $0,1,\ldots,d$, for a total of m^{d+1} possibilities. These $d+1$ values, $(y_0, y_1, \ldots, y_d)$, are called the *value representation* of $p(x)$. The coefficient representation can be converted to the value representation by evaluating the polynomial at $0,1,\ldots,d$. And, as we've seen, Lagrange interpolation can be used to convert the value representation to the coefficient representation.

So if we are given three pairs $(x_1,y_1),(x_2,y_2),(x_3,y_3)$ then there is a unique polynomial of degree 2 such that $p(x_i) = y_i$. But now, suppose we were only given two pairs $(x_1,y_1),(x_2,y_2)$; how many distinct degree-2 polynomials are there that go through these two points? Notice that there are exactly m choices for y_3, and for each choice there is a unique (and distinct) polynomial of degree two that goes through the three points $(x_1,y_1),(x_2,y_2),(x_3,y_3)$. It follows that there are exactly m polynomials of degree at most 2 that go through two points $(x_1,y_1),(x_2,y_2)$, as shown below:

What if you were only given one point (x_1,y_1)? Well, there are m^2 choices for y_2 and y_3, yielding m^2 polynomials of degree at most 2 that go through the point given. A pattern begins to emerge, as is summarized in the following table:



Polynomials of degree $\leq d$ over F_m	
# of points	# of polynomials
$d+1$	1
d	m
$d-1$	m^2
$\vdots$	$\vdots$
$d-k$	m^{k+1}
$\vdots$	$\vdots$
0	m^{d+1}

Note that the reason that we can count the number of polynomials in this setting is because we are working over a finite field. If we were working over an infinite field such as the reals, there would be infinitely many polynomials of degree d that can go through d points! (Think of a line, which has degree 1. If you were just given one point, there would be infinitely many possibilities for the second point, each of which uniquely defines a line.)

Secret Sharing

In the late 1950's and into the 1960's, during the Cold War, President Dwight D. Eisenhower approved instructions and authorized top commanding officers for the use of nuclear weapons under very serious emergency conditions. Such measures were set up in order to defend the United States in case of an attack in which there was not enough time to confer with the President and decide on an appropriate response. This would allow for a rapid response in case of a Soviet attack on U.S. soil. This is a perfect situation in which a secret sharing scheme could be used to ensure that a certain number of officials must come together in order to successfully launch a nuclear strike, so that for example no single person has the power and control over such a devastating and destructive weapon. Suppose the U.S. government decides that a nuclear strike can be initiated only if at least $k > 1$ major officials agree to it. We want to devise a scheme such that both of the following properties hold:

1. Any group of k of these officials can pool their information to figure out the launch code and initiate the strike.

2. No group of $k-1$ or fewer officials have *any* information about the launch code, even if they pool their knowledge. For example, they should not learn whether the secret is odd or even, a prime number, divisible by some number a, or the secret's least significant bit.

How can we accomplish this[4]?

[4]This is a note where polynomials are playing a starring role and so we are going to use polynomials to do this in a nicely structured way. However, your background with solving systems of linear equations should give you a hint as to how you could

Suppose that there are n officials indexed from 1 to n and the launch code is some natural number s. Let q be a prime number larger than n and s. We will work over $GF(q)$ from now on.

Now pick a random polynomial $P(x)$ of degree $k-1$ such that $P(0) = s$ and give $P(1)$ to the first official, $P(2)$ to the second,..., $P(n)$ to the n^{th}. Then we have:

1. Any k officials, having the values of the polynomial at k points, can use Lagrange interpolation to find P, and once they know what P is, they can compute $P(0) = s$ to learn the secret. Another way to say this is that any k officials have between them a value representation of the polynomial, which they can convert to the coefficient representation, which allows them to evaluate $P(0) = s$.

2. Any group of $k-1$ (or fewer) officials has no information about s! To see this, observe that they know only $k-1$ points through which $P(x)$, an unknown polynomial of degree $k-1$, passes. They wish to reconstruct $P(0) = s$. But by our discussion in the previous section, for each possible value $P(0) = b$, there is a unique polynomial of degree $k-1$ that passes through the $k-1$ points that the officials have as well as through $(0,b)$. Hence the secret could be *any* of the q possible values $\{0,1,\ldots,q-1\}$, so the officials have—in a very precise sense—no information about s. Another way of saying this is that the information of the officials is consistent with q different value representations, one for each possible value of the secret, and thus the officials have no information[5] about s.

Example. Suppose you are in charge of setting up a secret sharing scheme, with secret $s = 1$, where you want to distribute $n = 5$ shares to 5 people such that any $k = 3$ or more people can figure out the secret, but two or fewer cannot. Let's say we are working over $GF(7)$ (note that $7 > s$ and $7 > n$) and you randomly choose the following polynomial of degree $k-1 = 2 : P(x) = 3x^2 + 5x + 1$ (here, $P(0) = 1 = s$, the secret). So you know everything there is to know about the secret and the polynomial, but what about the people that receive the shares? Well, the shares handed out are $P(1) = 2$ to the first official, $P(2) = 2$ to the second, $P(3) = 1$ to the third, $P(4) = 6$ to the fourth, and $P(5) = 3$ to the fifth official. Let's say that officials 3, 4, and 5 get together (we expect them to be able to recover the secret). Using Lagrange interpolation, they compute the following basis functions:

$$\Delta_3(x) = \frac{(x-4)(x-5)}{(3-4)(3-5)} = \frac{(x-4)(x-5)}{2} = 4(x-4)(x-5);$$
$$\Delta_4(x) = \frac{(x-3)(x-5)}{(4-3)(4-5)} = \frac{(x-3)(x-5)}{-1} = 6(x-3)(x-5);$$
$$\Delta_5(x) = \frac{(x-3)(x-4)}{(5-3)(5-4)} = \frac{(x-3)(x-4)}{2} = 4(x-3)(x-4).$$

have come up with this. You know that you generically need k linear equations to solve for k unknowns. When you have fewer than k equations, in general you just get a solution for some unknowns in terms of other unknowns. You can't actually figure out exact values for any of the unknowns themselves. This tells you that a way to protect a secret is to accompany it with another $k-1$ pieces of sacrificial information that you don't care about, and then to distribute linear equations to participants. If k get together, and the equations have linear independence, then the group can solve for all the unknowns, including the secret. If there are fewer than k equations, you want it to be the case that you can't solve for any of the unknowns exactly. The sacrificial information protects the secret.

The role of polynomials here is simply to give us a structured way to get systems of linear equations that have nice properties.

[5] Note that this is one major reason we choose to work over finite fields rather than, say, over the real numbers, where the basic secret-sharing scheme would still work. Because there are only finitely many values in our field, we can quantify precisely how many remaining possibilities there are for the value of the secret, and show that this is the same as if the officials had no information at all. Another major reason is to keep the computations exact using integer arithmetic in a bounded range, rather than floating point operations over the reals that can suffer from numerical instability.

(Note that all divisions above are to be interpreted as multiplication by the corresponding inverse mod 7; e.g., in the first line for Δ_3, division by 2 is really multiplication by $2^{-1} = 4 \pmod 7$.) They then compute the polynomial over $GF(7)$: $P(x) = (1)\Delta_3(x) + (6)\Delta_4(x) + (3)\Delta_5(x) = 3x^2 + 5x + 1$. (Verify this computation!) Finally, they simply compute $P(0)$ and discover that the secret is 1.

Let's see what happens if two officials try to get together, say persons 1 and 5. They both know that the polynomial looks like $P(x) = a_2x^2 + a_1x + s$. They also know the following equations:

$$P(1) = a_2 + a_1 + s = 2$$
$$P(5) = 4a_2 + 5a_1 + s = 3$$

But that is all they have—two equations with three unknowns—and thus they cannot find out the secret. This is the case no matter which two officials get together. Notice that since we are working over $GF(7)$, the two people could have guessed the secret ($0 \leq s \leq 6$) and constructed a unique degree 2 polynomial (by Property 2). But the two people combined have the same chance of guessing what the secret is as they do individually. This is important, as it implies that two people have no more information about the secret than one person does.