1 Roots

Recall that a polynomial of degree $d$ has at most $d$ roots. In this problem, assume we are working with polynomials over $\mathbb{R}$.

(a) Suppose $p(x)$ and $q(x)$ are two different nonzero polynomials with degrees $d_1$ and $d_2$ respectively. What can you say about the maximum number of roots of $p(x) = q(x)$, in terms of $d_1$ and $d_2$? How about $p(x) \cdot q(x) = 0$?

(b) Consider the degree 2 polynomial $f(x) = x^2 + ax + b$. Show that if $f$ has exactly one root, then $a^2 = 4b$.

(c) What is the minimum number of real roots that a nonzero polynomial of degree $d$ can have? How does the answer depend on $d$?

(d) Consider $P(x) = x^3 - x^2 - x - 2$. Show that $(x - 2)|P(x)$ by using the long polynomial division method.

Solution:

(a) A solution of $p(x) = q(x)$ is a root of the polynomial $p(x) - q(x)$, which has degree at most $\max(d_1, d_2)$. Therefore, the number of solutions is also at most $\max(d_1, d_2)$.

A solution of $p(x) \cdot q(x) = 0$ is a root of the polynomial $p(x) \cdot q(x)$, which has degree $d_1 + d_2$. Therefore, the number of solutions is at most $d_1 + d_2$.

(b) If there is a root $c$, then the polynomial is divisible by $x - c$. Therefore it can be written as $f(x) = (x - c)g(x)$. But $g(x)$ is a degree one polynomial and by looking at coefficients it is obvious that its leading coefficient is 1. Therefore $g(x) = x - d$ for some $d$. But then $d$ is also a root, which means that $d = c$. So $f(x) = (x - c)^2$ which means that $a = -2c$ and $b = c^2$, so $a^2 = 4b$.

(c) If $d$ is even, the polynomial can have 0 roots (e.g., consider $x^d + 1$, which is always positive for all $x \in \mathbb{R}$). If $d$ is odd, the polynomial must have at least 1 root (a polynomial of odd degree takes on arbitrarily large positive and negative values, and thus must pass through 0 inbetween them at least once).

(d) The long polynomial division is as follows:
So we have

\[
P(x) = x^3 - x^2 - x - 2 = (x - 2)(x^2 + x + 1),
\]

where \((x - 2)\) divides \(P(x)\).

2 How Many Polynomials?

Let \(P(x)\) be a polynomial of degree at most 2 over \(GF(5)\). As we saw in lecture, we need \(d + 1\) distinct points to determine a unique \(d\)-degree polynomial, so knowing the values for say, \(P(0), P(1),\) and \(P(2)\) would be enough to recover \(P\). (For this problem, we consider two polynomials to be distinct if they return different values for any input.)

(a) Assume that we know \(P(0) = 1, \) and \(P(1) = 2.\) Now consider \(P(2)\). How many values can \(P(2)\) have? How many distinct possibilities for \(P\) do we have?

(b) Now assume that we only know \(P(0) = 1.\) We consider \(P(1)\) and \(P(2)\). How many different \((P(1), P(2))\) pairs are there? How many distinct possibilities for \(P\) do we have?

(c) Now, let \(P\) be a polynomial of degree at most \(d.\) Assume we only know \(P\) evaluated at \(k \leq d + 1\) different values. How many different possibilities do we have for \(P?\)

(d) A polynomial with integer coefficients that cannot be factored into polynomials of lower degree on a finite field, is called an irreducible or prime polynomial.

Show that \(P(x) = x^2 + x + 1\) is a prime polynomial on \(GF(5)\).

Solution:

(a) 5 polynomials, each for different values of \(P(2).\)

(b) Now there are \(5^2\) different polynomials.

(c) \(p^{d+1-k}\) different polynomials. For \(k = d + 1,\) there should only be 1 polynomial.
(d) We can try all possible inputs for $x$ and show that in each case $P(x) \equiv 0 \pmod{x}$, which means that $P(x)$ does not have any root on the finite field $GF(5)$.

$x = 0 \Rightarrow P(0) \equiv 1 \pmod{5}$
$x = 1 \Rightarrow P(1) \equiv 3 \pmod{5}$
$x = 2 \Rightarrow P(2) \equiv 2 \pmod{5}$
$x = 3 \Rightarrow P(3) \equiv 3 \pmod{5}$
$x = 4 \Rightarrow P(4) \equiv 1 \pmod{5}$

Hence $P(x)$ is a prime polynomial.

3 Secrets in the United Nations

A vault in the United Nations can be opened with a secret combination $s \in \mathbb{Z}$. In only two situations should this vault be opened: (i) all 193 member countries must agree, or (ii) at least 55 countries, plus the U.N. Secretary-General, must agree.

(a) Propose a scheme that gives private information to the Secretary-General and all 193 member countries so that the secret combination $s$ can only be recovered under either one of the two specified conditions.

(b) The General Assembly of the UN decides to add an extra level of security: each of the 193 member countries has a delegation of 12 representatives, all of whom must agree in order for that country to help open the vault. Propose a scheme that adds this new feature. The scheme should give private information to the Secretary-General and to each representative of each country.

Solution:

(a) Create a polynomial of degree 192 and give each country one point. Give the Secretary General 192 – 55 = 137 points, so that if she collaborates with 55 countries, they will have a total of 192 points and can reconstruct the polynomial. Without the Secretary-General, the polynomial can still be recovered if all 192 countries come together. (We do all our work in $GF(p)$ where $p \geq d + 1$).

Alternatively, we could have one scheme for condition (i) and another for (ii). The first condition is the secret-sharing setup we discussed in the notes, so a single polynomial of degree 192 suffices, with each country receiving one point, and evaluation at zero returning the combination $s$. For the second condition, create a polynomial $f$ of degree 1 with $f(0) = s$, and give $f(1)$ to the Secretary-General. Now create a second polynomial $g$ of degree 54, with $g(0) = f(2)$, and give one point of $g$ to each country. This way any 55 countries can recover $g(0) = f(2)$, and then can consult with the Secretary-General to recover $s = f(0)$ from $f(1)$ and $f(2)$.
(b) We’ll layer an *additional* round of secret-sharing onto the scheme from part (a). If $t_i$ is the key given to the $i$th country, produce a degree-11 polynomial $f_i$ so that $f_i(0) = t_i$, and give one point of $f_i$ to each of the 12 delegates. Do the same for each country (using different $f_i$ each time, of course).