1 Polynomial Short

(a) What is the minimum number of points necessary to uniquely determine a degree d polynomial?

(b) Let p be a degree 6 polynomial and q be a degree 4 polynomial. What is the maximum possible degree of $p+q$? What is the minimum possible degree? What about $p \cdot q$?

2 Roots

Let's make sure you're comfortable with roots of polynomials in the familiar real numbers $\mathbb{R}$. 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 number of solutions of $p(x) = q(x)$? 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?

3 Roots: The Next Generations

Now go back and do it all over in modular arithmetic...

Which of the facts from above stay true when $\mathbb{R}$ is replaced by GF(p) [i.e., integer arithmetic modulo the prime p]? Which change, and how? Which statements won't even make sense anymore?

4 How Many Polynomials?

Let $P(x)$ be a polynomial of degree 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial.

(a) Assume that we know $P(0) = 1$, and $P(1) = 2$. Now we consider $P(2)$. How many values can $P(2)$ have? How many distinct polynomials are there?

(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 different polynomials are there?

(c) How many different polynomials of degree d over $GF(p)$ are there if we only know k values, where $k \leq d$?

5 GCD of Polynomials

Let $A(x)$ and $B(x)$ be polynomials (with coefficients in $\mathbb{R}$). We say that $\gcd(A(x), B(x)) = D(x)$ if $D(x)$ divides $A(x)$ and $B(x)$, and if every polynomial $C(x)$ that divides both $A(x)$ and $B(x)$ also divides $D(x)$. For example, $\gcd((x-1)(x+1), (x-1)(x+2)) = x - 1$. Notice this is the exact same as the normal definition of GCD, just extended to polynomials.

Incidentally, $\gcd(A(x), B(x))$ is the highest degree polynomial that divides both $A(x)$ and $B(x)$. In the subproblems below, you may assume you already have a subroutine `divide(`$P(x), S(x)$`)` for dividing two polynomials, which returns a tuple $(Q(x), R(x))$ of the quotient and the remainder, respectively, of dividing $P(x)$ by $S(x)$.

(a) Write a recursive program to compute `gcd`$(A(x), B(x))$.

(b) Write a recursive program to compute `extended-gcd`$(A(x), B(x))$.