CCS Discrete Math I	Professor: Padraic Bartlett

Homework 12: Finite Fields

Due Friday, Week 7 — *UCSB 2014*

Do **three** of the **six** problems below!

1. Consider applying the Euclidean algorithm to polynomials, as follows:

   Algorithm. Take any two polynomials $p(x), q(x)$, where the degree of $p(x)$ is not smaller than the degree of $q(x)$.

   This algorithm will calculate the GCD of $p(x), q(x)$. That is, this process will create a polynomial $r(x)$ that divides both $p(x)$ and $q(x)$, such that $p(x)/r(x)$ and $q(x)/r(x)$ have no factors in common.

   To initialize our algorithm, set $r_1(x) = p(x), r_2(x) = q(x)$. Our algorithm will create a sequence of polynomials $r_1(x), r_2(x), r_3(x) \ldots r_k(x)$,, where this last value $r_k(x)$ will be the GCD of a, b.

   i. Suppose that we have defined our sequence up to $r_i(x), r_{i+1}(x)$, that the degree of $r_i(x)$ is greater than the degree of $r_{i+1}(x)$, and that $r_{i+1}(x) \neq 0$.

   ii. If the remainder of $r_i(x)$ when divided by $r_{i+1}(x)$ is 0, quit our algorithm: $r_{i+1}(x)$ is the GCD of $p(x), q(x)$.

   iii. Otherwise, to define $r_{i+2}(x)$, simply set it equal to the remainder of $r_i(x)$ when divided by $r_{i+1}(x)$. (Note that we are doing polynomial long division here! If you are unsure how to do this, check out Wikipedia for some background, or talk to me!)

      This always gives us a polynomial with degree smaller than $r_{i+1}(x)$, by definition.

   iv. Return to i. and repeat this process.

   Prove that this algorithm works. That is, prove that the output $r(x)$ of this algorithm has the following properties:

   - $r(x)$ is a factor of $p(x)$ and $q(x)$, and furthermore
   - $p(x)/r(x)$ and $q(x)/r(x)$ have no factors in common.

2. Prove that there is no finite field of order 12.

3. Consider the polynomial $1 + x + x^2 + x^3 + \ldots + x^n$ as a polynomial in $\mathbb{F}_2[x]$.

   (a) Show that if $n+1$ is not a prime number, then this polynomial is not irreducible.

   (b) Suppose that $n+1$ is a prime number. Find a value of n for which this polynomial is irreducible, and another value of n for which this polynomial is not irreducible.

4. Prove that the "**commutativity**(+)" property is redundant in the definition of a field, in the following sense: show that if $\langle \mathbb{F}, +, \cdot \rangle$ is a structure that you know satisfies all of the other properties of being a field other than **commutativity**(+), then **commutativity**(+) must also hold for $\langle \mathbb{F}, +, \cdot \rangle$

5. Prove that there is no finite field of order 10.

6. Prove or disprove the following claim:

   For any polynomial $f(x)$ with integer coefficients, there is some prime p such that $f(x)$ is an irreducible polynomial[1] within $\mathbb{F}_p[x]$.

[1]To interpret $f(x)$ as an element of $\mathbb{F}_p[x]$, simply take all of its coefficients mod p. That is, we would think of $x^2 - 5x + 3$ as just $x^2 + x + 1$ in $\mathbb{F}_2[x]$.