CCS Discrete Math I | Professor: Padraic Bartlett

# Homework 13: Yet More Finite Fields

*Due Friday, Week 7* | *UCSB 2014*

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

1. In class, we made the following claim:

   **Lemma.** Let $f(x)$ be a polynomial in $\mathbb{F}[x]$, for any field $\mathbb{F}$. Then, if $f(a) = 0$ for some $a \in \mathbb{F}$, we can write $f(x) = (x-a) \cdot g(x)$, for some other polynomial $g(x) \in \mathbb{F}[x]$.

   Prove this lemma!

   (Hint: when $a = 0$, can you prove this result? If you can, then when $a \neq 0$, try looking at the polynomial $h(x) = f(x-a)$. How can a factorization of $h(x)$ help you factor $f(x)$?

2. Make a finite field of order 16. (That is: use the constructions from class to create such a field! Give me all of its elements, along with its addition and multiplication tables.) From this field's group tables, explain why it satisfies all of the field axioms other than associativity and distributivity. (I omit those because they're more of a pain to check.)

3. In how many ways can you travel on a rectangular grid from $(0, 0)$ to $(40, 40)$, with each step consisting of either an increase in the $x$ or $y$ coordinate, so that our path avoids the two points $(10, 20)$ and $(20, 30)$?