CCS Discrete Math I — Professor: Padraic Bartlett

Homework 14: Review

Due Monday, Week 9 — *UCSB 2014*

This set is different from other sets. For one, it is due on **Monday**, week 9, instead of Friday, week 8! This is because of Thanksgiving. For another, this set isn't focused only on the material of the past week! Instead, it's designed to function as a **review** of the quarter so far. The idea here is to give you all a chance to practice some of the skills/problems that we worked on in earlier weeks, because (as you may have noticed!) they keep coming up in class!

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

1. Counting and cosets!

   (a) Show that $H = \{id, (12), (13), (23), (123), (132)\}$ is a subgroup of S_n for any $n \geq 3$.

   (b) How many elements are there in S_n, for $n = 24601$?

   (c) How many cosets of H are there in S_n, for $n = 24601$?

2. Catalan numbers and counting permutations!

   (a) Let C_n denote the collection of all of the orderings of the set $\{1, 2, \ldots n\}$ that do not have any 3-term increasing subsequences. For example, C_4 contains the following elements:

   $$1432, 2143, 2413, 2431, 3142, 3214, 3241,$$
   $$3412, 3421, 4132, 4213, 4231, 4312, 4321.$$

   Alternately, if it helps, the orderings of $\{1, 2, 3, 4\}$ that are **not** in the above list are the following, because they all have 3-term increasing subsequences. (Subsequences are highlighted in red below; where there were multiple such subsequences, I just picked one of the possible subsequences.)

   1234, 1243, 1324, 1342, 1423,
   2134, 2314, 2341, 3124, 4123.

   Show that C_n is counted by the Catalan numbers.

   (b) Using (a), determine the ratio of permutations of $\{1, 2, \ldots 50\}$ with no 3-term increasing subsequence to the total number of such permutations: that is, find the fraction

   $$\frac{\#(\text{permutations of } \{1, 2 \ldots 50\} \text{ with no 3-term increasing subsequence})}{\#(\text{permutations of } \{1, 2 \ldots 50\})}.$$

   What is this number, roughly? (I.e. give me its first few digits and order of magnitude.)

3. Righting wrongs! To answer this problem,

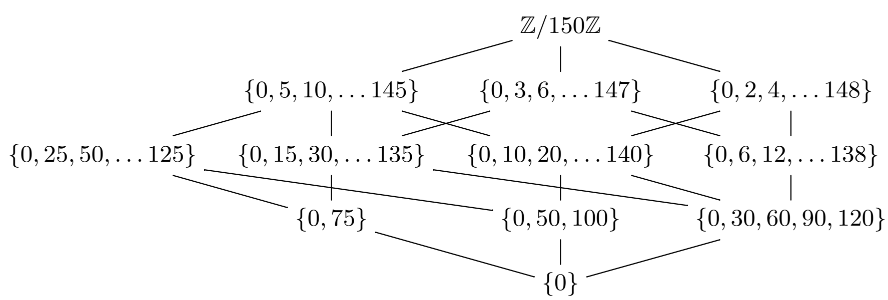
   (a) Go through your old HW and quizzes!
   (b) Find **one** problems that you attempted, but did not get full credit on. (I.e. 0 or .5 scores on attempted work.)
   (c) Attach your old work (you should have it still in LaTeX!)
   (d) Attach a paragraph explaining why your old attempt didn't work / your proof was flawed / etc.
   (e) Then, **fix** your problem by attaching a new and correct solution!

   You need all of the parts above to receive credit here.

4. Groups and games!

   (a) Given any group G and all of its subgroups, we can make a **lattice** out of these subgroups, as follows:
      - Draw one vertex on our paper for each subgroup that we have.
      - Draw a line from one subgroup H to another subgroup K if and only if the following happens:
        – H is a subgroup of K.
        – There is no third subgroup J such that $J \neq H, K$ and $H \subset J \subset K$.

      We draw an example for $G = \langle \mathbb{Z}/150\mathbb{Z}, + \rangle$ here:



      Create such a lattice for $G = \langle \mathbb{Z}/168\mathbb{Z}, + \rangle$.

   (b) Consider the following two-player game on this lattice:
      - Player 1 picks out a subgroup H on the lattice, and deletes it, along with any subgroups contained within H.
      - Player 2 then picks out a remaining subgroup H', and also deletes it along with any subgroups contained within H'.
      - The players repeat this process until there are no subgroups left. The player who chose the last subgroup loses.

      Find a winning strategy for either player 1 or player 2 on the lattice for $G = \langle \mathbb{Z}/84\mathbb{Z}, + \rangle$. (Helpful hint: you already made this lattice as a sublattice in your answer to (a)!)

5. Generating functions and groups!

   (a) Show that in $\mathbb{F}_p[x]$, for any n, there are precisely p^n many monic[1] polynomials of degree n.

   (b) Let A_n denote the number of monic polynomials of degree n that you calculated in (a), and set

$$A(x) = \sum_{n=0}^{\infty} A_n x^n.$$

   Let $M_n(p) = M_n$ denote the number of irreducible monic polynomials of degree n. Show[2] that

$$A(x) = \prod_{n=1}^{\infty} \left(1 + x^n + x^{2n} + \ldots +\right)^{M_n}.$$

   (Hint: show that the coefficients for both expressions are equal!)

6. Polynomial problems!

   (a) Take any polynomial $f(x) \in \mathbb{Z}[x]$ with degree at least 2. For any prime p, we can interpret $f(x)$ as a polynomial in $\mathbb{F}_p[x]$ by reducing all of its coefficients mod p. For example, if $f(x) = 4x^2 + 3x - 7$, we could interpret $f(x)$ in $\mathbb{F}_2[x]$ as $x + 1$. Conversely, if we interpreted $f(x)$ as an element of $\mathbb{F}_3[x]$, it would be $x^2 + 2$.

   For any such polynomial $f(x)$, show that there is some prime p and value n such that if we interpret $f(x)$ as a polynomial in $\mathbb{F}_p[x]$, then $f(n) = 0$.

   (b) Take any polynomial $f(x) \in \mathbb{Z}[x]$ with degree at least 2. Using (a), prove that there is some prime p such that $f(x)$ is **not** an irreducible polynomial when interpreted in $\mathbb{F}_p[x]$. (For example, $x^2 + x + 1$ is not irreducible in $\mathbb{F}_3[x]$, because we can write it as $(x + 2)(x + 2) = x^2 + 4x + 4 = x^2 + x + 1$.)

[1] If $f(x)$ is a degree-n monic polynomial, then the coefficient of x^n in $f(x)$ is just 1.

[2] If you keep going with this problem, you'll get an alternate proof that $M_n > 0$ for all n! Yay, generating functions.