Lecture 25

Enoch Cheung

November 21, 2013

Exam Review: The biggest thing for this exam (and most math exams) is to make sure they're familiar with their formal definitions. If they start off a proof by saying let $a \in \text{PreIm}(Y)$ their next line should be to translate what that means (i.e. $\exists b \in Y$ such that $f(a) = b$). Proofs on the test will rely mostly on definitions and some basic theorems (Euclid's Lemma, Fundamental Theorem of Airthmetic, GCD Theorem, MAL). The other thing to work on is that they know how to read symbolic statements and how to begin proofs of universal/existential statements, especially universal quantifiers in front of a conditional statement.

A good list of the definitions and theorems that you need to know is on the review sheet on Blackboard. The following is taken from it:

Number theory. The Division Algorithm, the definition of congruence modulo m, the modular arithmetic lemma, the definition of a gcd, the gcd theorem, Euclid's Lemma, the fundamental theorem of arithmetic, what the set $\mathbb{Z}/m\mathbb{Z}$ looks like, which elements of $\mathbb{Z}/m\mathbb{Z}$ have multiplicative inverses, how to solve linear diophantine equations or determine when there is no solution, and the Chinese Remainder Theorem.

Functions/Cardinality. Know: the definition of a function, image and preimage of a set under a function, how to prove/disprove injectivity, surjectivity and bijectivity, how to prove two functions are inverses, invertibile iff bijective, cardinality, CBS theorem, Cantor's Theorem, how to determine whether a set is countably or uncountably infinite, countable union of countable sets is countable, finite product of countable sets is countable, the real numbers are uncountable, and diagonalization arguments.

1. Find all solutions to $4x \equiv 8 \pmod{12}$.

   Lemma. If $d|m$ then

   $$xd \equiv yd \pmod{m} \iff x \equiv y \pmod{\frac{m}{d}}$$

   Proof: Certainly, if $x \equiv y \pmod{\frac{m}{d}}$, then $\frac{m}{d}|(x-y)$ so $m|(x-y)$. Now suppose $xd \equiv yd \pmod{m}$, then $m|(xd-yd)$ so $mk = (x-y)d$ for some $k \in \mathbb{N}$. Therefore, $\frac{m}{d}k = x - y$ so $\frac{m}{d}|(x-y)$. □

   Therefore, since $4|12$

   $$4x \equiv 8 \pmod{12} \iff x \equiv 2 \pmod{3}$$

   so the only solutions are $x \equiv 2 \pmod 3$, which in mod 12 are $x \equiv 2, 5, 8, 11 \pmod{12}$.

2. Find all solutions to $4x \equiv 6 \pmod{12}$.

   There are no solutions. Suppose x is such a solution, then $12|6-4x$, and $4|12$ so $4|6-4x$ so $4|6$ which is false.

3. Show that for all $a, b \in \mathbb{N}$, $d \in \mathbb{Z}$, $d|a$ and $d|b$ if and only if $d|\gcd(a,b)$.

   ($\Rightarrow$) Consider arbitrary $a, b \in \mathbb{N}$, $d \in \mathbb{Z}$ such that $d|a$ and $d|b$. By gcd theorem there are $x, y \in \mathbb{Z}$ such that $\gcd(a,b) = xa + yb$, so by MAL since $a \equiv b \equiv 0 \pmod d$, $\gcd(a,b) \equiv 0 \pmod d$. Therefore, $d|\gcd(a,b)$.

   ($\Leftarrow$) Consider arbitrary $a, b \in \mathbb{N}$, $d \in \mathbb{Z}$ such that $d|\gcd(a,b)$. By definition $\gcd(a,b)|a$ and $\gcd(a,b)|b$, so a, b are multiples of $\gcd(a,b)$, which itself is a multiple of d, so $d|a$ and $d|b$.

4. For any $a, b \in \mathbb{N}$, define a function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ as $f(x,y) = ax + by$. What is $\text{Im}_f(\mathbb{Z} \times \mathbb{Z})$?

   Let $d = \gcd(a,b)$. We know that there exists $x, y \in \mathbb{Z}$ such that $f(x,y) = ax + by = d$, so $d \in \text{Im}_f(\mathbb{Z} \times \mathbb{Z})$. Recall the previous theorem that in fact d is the least positve integer in $\text{Im}_f(\mathbb{Z} \times \mathbb{Z})$. Furthermore, we know that for any $k \in \mathbb{Z}$, $kd = a(kx) + b(ky) = f(kx, ky)$, so $kd \in \text{Im}_f(\mathbb{Z} \times \mathbb{Z})$.

   In fact, that is all of it, meaning that $\text{Im}_f(\mathbb{Z} \times \mathbb{Z}) = d\mathbb{Z}$. This is because given any $y \in \text{Im}_f(\mathbb{Z} \times \mathbb{Z})$, using division algorithm write $y = qd + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < d$. Then since we know that $qd \in \text{Im}_f(\mathbb{Z} \times \mathbb{Z})$ as well, you can check that $r = qd - y \in \text{Im}_f(\mathbb{Z} \times \mathbb{Z})$. However, we know that d is the least positive interger in $\text{Im}_f(\mathbb{Z} \times \mathbb{Z})$, so since $0 \leq r < d$, $r = 0$, so $y = qd \in d\mathbb{Z}$.

5. Show that the set $S = \{f : [n] \to \mathbb{N} \mid f \text{ is a function }, n \in \mathbb{N}\}$ which is the set of all finite sequences, is countable.

   Recall that we showed that $A \times B$ is countably finite for any countably infinite set A, B. Inductively, we can show that $\mathbb{N}^n = \underbrace{\mathbb{N} \times \cdots \times \mathbb{N}}_{n \text{ times}}$ for any $n \in \mathbb{N}$ is countably infinite.

   Base case: $\mathbb{N}^1 = \mathbb{N}$ is countably infinite.

   Inductive case: Assume for some $n \in \mathbb{N}$ that $\mathbb{N}^n$ is countably infinite, then $\mathbb{N}^{n+1} = \mathbb{N}^n \times \mathbb{N}$ is countably infinite because it is the product of two countably infintie sets.

   Therefore, $\mathbb{N}^n$ is countably infinite for each $n \in \mathbb{N}$. For each $n \in \mathbb{N}$, let $S_n = \{f : [n] \to \mathbb{N} \mid f \text{ is a function }\}$. It is easy to verify that for each $n \in \mathbb{N}$, the following is a bijection

$$\begin{aligned} s_n : S_n &\longrightarrow \mathbb{N}^n \\ f &\longmapsto (f(1), f(2), \ldots, f(n)) \end{aligned}$$

   Therefore, each S_n is countably infinite, and note that $S = \bigcup_{n \in \mathbb{N}} S_n$ so S is a countable union of countable sets so it is countably infinite.