FINAL REVIEW, MATH 215, SPRING 2019

Induction. Definition: Let P be some property about natural numbers. Suppose that the following hold:

(1) (base) $P(1)$ is true.
(2) (inductive) For all $n \geq 1$, $P(n) \to P(n+1)$.

Then for all $n \geq 1$, $P(n)$ holds.

Know how to do proofs by induction.

Functions. Definition of a function, one-to-one, onto, bijection, and how to prove that a function is one-to-one, onto, or a bijection.

Equivalence relations. Definition of an equivalence relation, an equivalence class, being able to prove that the equivalences classes form a partition, being able to prove that a relation is an equivalence relation.

Modular arithmetic

(1) Definition: $a \equiv b \bmod n$ iff $n|(b-a)$; the proof that this is an equivalence relation; the set of equivalence classes is $\mathbb{Z}_n := \{[0], [1], ..., [n-1]\}$.
(2) How to add and multiply mod n, e.g. be able to do the tables for addition and multiplication in $\mathbb{Z}_3, \mathbb{Z}_4$, etc.
(3) The proof that if $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$, then $a+b \equiv a'+b'$ mod n and $ab \equiv a'b' \bmod n$
(4) The proof that if a and n are relatively prime (i.e. $gcd(a,n) = 1$), then multiplication by a is a bijection from $\mathbb{Z}_n \to \mathbb{Z}_n$.
(5) The statement of the Chinese remainder theorem:
    Suppose that $\{n_1, ..., n_k\}$ are pairwise relatively prime natural numbers. Then for any choice of $a_1, ..., a_k$, the system:
    - $x = a_1 \bmod n_1$
    - $x = a_2 \bmod n_2$
    - ...
    - $x = a_k \bmod n_k$

    has a solution for x which is unique mod the product $n_1 \cdot n_2 .... n_k$.
(6) Solving systems of modular equations.

Sets and Cardinality

(1) Notation:
    $\mathbb{N} := \{0, 1, 2, ...\}$ is the natural numbers,
    $\mathbb{Z} := \{..., -2, -1, 0, 1, 2, ...\}$ is the integers,
    $\mathbb{Q} := \{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$ is the rational numbers,
    $\mathbb{R}$ denotes the reals, $\mathbb{C}$ denotes the complex numbers.

$|\mathbb{N}| = \aleph_0 = \omega$, $|\mathbb{R}| = c = 2^{\aleph_0}$. Here c stand for the continuum.
${}^A2$ is the set of all functions from A to $\{0,1\}$; i.e. ${}^A2 := \{f : A \to \{0,1\} \mid f \text{ is a function}\}$.

(2) The Pigeonhole principle.
(3) Comparing cardinalities of sets:
   (a) $|A| = |B|$ iff there is a bijection $f : A \to B$.
   (b) $|A| \leq |B|$ iff there is a one-to-one function $f : A \to B$ iff there is an onto function $g : B \to A$.
   (c) A is *countable* iff there is an onto function $f : \mathbb{N} \to A$. Note that this includes all finite sets. If an infinite set A is countable, then $|A| = \omega$.
   (d) Examples: $|\mathbb{Z}| = |\mathbb{Q}| = \omega$; the set of all polynomials with rational coefficients is countable; the reals are uncountable.
(4) The power set:
   (a) Definition: $\mathcal{P}(A) = \{B \mid B \subset A\}$;
   (b) if $|A| = n$, then $|\mathcal{P}(A)| = 2^n$, $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ (no proof)
   (c) the proof that $|\mathcal{P}(A)| = |{}^A2|$ for any set A.
   (d) the proof of Cantor's theorem that there is no onto function $f : A \to \mathcal{P}(A)$ and so $|A| < |\mathcal{P}(A)|$,
   (e) the proof that there is no largest cardinal.

Sample problems:

Problem 1. *Determine which of the following is an equivalence relation. Prove your answer.*

(1) $\leq$ *on the rational numbers* $\mathbb{Q}$.
(2) *The Vitali relation on* $\mathbb{R}$ *defined by* aE_vb *iff* $b - a \in \mathbb{Q}$
(3) *The relation* E *on* $\mathbb{Z}$ *given by* aEb *iff* $a + b$ *is even.*

Problem 2. *Let E be an equivalence relation on some set X. Prove that the equivalence classes form a partition on X.*

Problem 3. *Solve the following system of equations for x:*

- $x = 5$ *mod* 10
- $x = 0$ *mod* 9
- $x = 3$ *mod* 7.

Problem 4. *(a) Let A and B be sets. Show that if $|A| = |B|$, then $|\mathcal{P}(A)| = |\mathcal{P}(B)|$.*
(b) Show that $|\mathcal{P}(\mathbb{Q})| = c$ (where $c = |\mathbb{R}|$).

Problem 5. *Show that there is a bijection between $\mathcal{P}(A)$ and ${}^A2$, and so they have the same cardinality.*

Problem 6. *Prove Cantor's theorem: that for every set A, $|A| < |\mathcal{P}(A)|$.*

Problem 7. *Show that the set* $B = \{10k \mid k \in \mathbb{Z}\} = \{..., -20, -10, 0, 10, 20, ...\}$ *is countable.*

Problem 8. *(a) State the principle of induction.*
(b) Prove that for all n, $1 + 2 + ... + n = \frac{n(n+1)}{2}$.

Problem 9. *Show that* $\sqrt[3]{2}$ *is not a rational number.*

Problem 10. *Show that there is no greatest prime number.*