MAT 200 OUTLINE, PART 3

I'm preparing a lecture outline for the benefit of those who are unable to make it to class due to illness or other reasons. See the course textbook for additional details about most of these items. If a theorem is listed as $\boxed{\textbf{Theorem.}}$, this means that you should be familiar with the proof.

3/26

- Hierarchy of number systems: natural numbers $\mathbb{N}$, integers $\mathbb{Z}$, rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, complex numbers $\mathbb{C}$
- fraction: a formal expression a/b (where $a, b \in \mathbb{Z}$, $b \neq 0$), equivalent fractions, addition and multiplication of fractions
- rational number: an equivalence class of fractions, where $a/b = c/d$ if and only if $ad = bc$ (observe how operations/equality for fractions are **defined** in terms of addition, multiplication of integers, which is well-understood)
- $\boxed{\textbf{Theorem.}}$ There is no rational number whose square is 2. (The equation $x^2 = 2$ does not have a solution in the rationals.)
- infinite decimals, real numbers, equivalence of infinite decimals (e.g., $1.000\overline{0}$ and $.999\overline{9}$)

3/29

- Cardinality of infinite sets, equipotent sets ("have the same cardinality")
- denumerable, countable, uncountable sets, cardinality $\aleph_0$ (aleph-null) and the Continuum Hypothesis
- Dedekind's Theorem. A set X is infinite if and only if it is equipotent to a proper subset
- If A, B are denumerable, then so are $A \cup B$ and $A \times B$. Also, $\mathbb{Q}$ is countable.
- Comparison of cardinalities: $|X| \leq |Y|$, $|X| < |Y|$ for sets X, Y
- Cantor's Theorem. The set of real numbers $\mathbb{R}$ is uncountable. (the *diagonalization* argument)
- $\boxed{\textbf{Theorem.}}$ For any set X, $|X| < |\mathcal{P}(X)|$. (This is my favorite proof of the whole course: simple but genius.) One implication is that, by iterating the power set operation, one may create sets of arbitrary large cardinality.

4/7

- The division theorem. Let $a, b \in \mathbb{Z}$, with $b > 0$. There are unique integers q, r such that $a = bq + r$ and $0 \leq r < b$. Example: dividing 26 apples evenly among 7 people
- Application: Let $a \in \mathbb{Z}$. Prove that a is divisible by 3 if and only if a^2 is divisible by 3.

4/9

- The Euclidean algorithm to find the greatest common divisor (gcd) of two integers
- $\boxed{\textbf{Theorem.}}$ Let $a, b \in \mathbb{N}$. Suppose $a = bq + r$ for some $q, r \in \mathbb{Z}$. Then $\gcd(a, b) = \gcd(b, r)$.
- Example: find $\gcd(120, 48)$ using the Euclidean algorithm

4/12

- Integral linear combinations
- Theorem. Let $a, b \in \mathbb{N}$. There exist $m, n \in \mathbb{Z}$ such that $\gcd(a, b) = am + bn$.

4/14

- Diophantine equation: solutions are required to be integers
- Examples: $m^2 = 2n^2$ has only trivial solution (irrationality of $\sqrt{2}$); $x^2 + y^2 = z^2$ has certain integer solutions called Pythagorean triples (e.g., $(3, 4, 5)$, $(5, 12, 13)$); $x^n + y^n = z^n$ has no integer solutions if $n \geq 3$ (the so-called Fermat's Last Theorem, proved by Andrew Wiles in 1994)
- Theorem. For all $a, b, c \in \mathbb{N}$, there exist $m, n \in \mathbb{Z}$ such that $am + bn = c$ if and only if $\gcd(a, b)$ divides c.
- Use the corresponding *homogeneous* equation to find all solutions (m, n) of $am + bn = c$.
- Example: Determine whether $140m + 63n = 35$ has a solution. If so, find all solutions (m, n).

4/16

- Congruence: $a \equiv b \mod m$
- Definition of even/odd in terms of congruences
- Everyday examples: hours are counted modulo 12 or modulo 24; days are counted modulo 7
- Reflexive, symmetric, and transitive properties of congruences
- Modulur arithmetic: congruence respects the basic operations of addition, subtraction, multiplication. I.e., if $a_1 \equiv a_2 \mod m$ and $b_1 \equiv b_2 \mod m$, then $a_1 + b_1 \equiv a_2 + b_2 \mod m$ and $a_1 b_1 \equiv a_2 b_2 \mod m$.

4/19

- Modular arithmetic example: determining the day of the week of a given date
- Example: show $4|(3^n + 2n - 1)$ (recall Midterm 1)
- The set R_m of remainders modulo m; the remainder map $r_m \colon \mathbb{Z} \to R_m$
- Proposition. Two integers $a, b \in \mathbb{Z}$ are congruent modulo m if and only if $r_m(a) = r_m(b)$
- $\boxed{\textbf{Theorem.}}$ Suppose $a|m$. Then $ab_1 \equiv ab_2 \mod m$ if and only if $b_1 \equiv b_2 \mod (m/a)$
- $\boxed{\textbf{Theorem.}}$ Suppose $\gcd(a, m) = 1$. Then $ab_1 \equiv ab_2$ if and only if $b_1 \equiv b_2 \mod m$. (Why is it " $\mod (m/a)$" in the previous theorem and " $\mod m$" in this theorem?)
- Example: solve the congruence $6x \equiv 15 \mod 21$ (i.e., find all values $x \in \mathbb{N}$ satisfying the equation).

4/21

- Solving linear congruences $ax \equiv b \mod m$ in general
- Theorem. Let $a, b, m \in \mathbb{N}$. Then $ax \equiv b \mod m$ has a solution if and only if $\gcd(a, m)|b$. In this case, the number of solutions modulo m is $\gcd(a, m)$.

4/23

- Example: solve $255x \equiv 15 \mod 621$.
- Congruence class of a modulo m, denoted by $[a]_m$. The space $\mathbb{Z}_m$ of congruence classes modulo m
- Modular arithmetic from the point of view of congruence classes