151 Excellent Final Exam Review

soumilm, vchowdha

Final Exam

1 Things to Know

Refer to the previous three Excellent Review handouts for the other topics.

1.1 Countability

1.1.1 Countable Sets

- Basic Definitions:
  - A set S is **countable** if it is **finite** or if it is **countably infinite**.
  - A set S is **countably infinite** if $\exists f : \mathbb{N} \to S$ such that f is a bijection.
- Closure properties of countable sets
  - Let X be a set and C be a countable set.
    - If $\exists f : X \to C$ such that f is injective, then X is countable.
      Note: *Intuition: $|X| \leq |C|$ because there is an injection from X to C, and $|C| = |\mathbb{N}|$, so X is "smaller" than $\mathbb{N}$ and thus countable.*
    - If $\exists f : C \to X$ such that f is surjective, then X is countable.
      Note: *Similar to above, $|C| \geq |X|$*
  - The ***finite*** cartesian product of countable sets is countable
  - The ***countable union*** of countable sets is countable
    Note: *This doesn't have to be a partition!*
  - A subset of a countable set is countable
- Most commonly used countable sets: $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{N} \times \mathbb{N}$
- Encoding method of showing countability:
  - Define an alphabet Σ of symbols that you will use to describe each element in your set
  - Describe the process of encoding each element in your set with Σ
  - Show that this encoding is injective - i.e. each element in your set maps to exactly one encoding
  - Example: encode $\mathbb{Z}$ with $\Sigma = \{-, 0, 1, 2, 3, 4, ..., 9\}$ where each $x \in \mathbb{Z}$ is encoded via simply writing down the number in base 10, with a $-$ if it is negative. This is injective since if two numbers have the same encoding, they have the same sign and same base 10 representation and must therefore be the same.
- Tips for proving countability
  - Try to come up with a way to describe each element of your set with a finite amount of information (i.e. every periodic function has a finite number of elements in its image)

- Try to relate your set to known countable sets, or come up with a countable set to relate your set to (this could involve using subsets or unions or cartesian products)
- Remember that you don't have to make a bijection; an injection or surjection suffices, and in most cases, an injection is easiest

1.1.2 Uncountable Sets

- **Cantor's Theorem**: For any set X, $\nexists$ a surjection $X \to \mathcal{P}(X)$. (This implies that for any infinite set X, $\mathcal{P}(X)$ is uncountable)
  - Proof uses the idea of **diagonalization**, where you show a surjection $f : X \to \mathcal{P}(X)$ cannot exist by creating an element $Y \in \mathcal{P}(X)$ that cannot be mapped to by manipulating the elements along the diagonal so that Y is different from each $f(x)$ in at least one place.
- If U is an uncountable set and $\exists f : X \to U$ such that f is surjective, then X is uncountable
  Note: *Intuition:* $|X| \geq |U|$ *and* $|U| > |\mathbb{N}|$ *because* U *is uncountable, so* $|X| > |\mathbb{N}|$
- If U is an uncountable set and $\exists f : U \to X$ such that f is injective, then X is uncountable
- If $\exists U \subseteq X$ such that U is uncountable, then X is uncountable
- Commonly used uncountable sets: $\mathbb{R}, \mathcal{P}(\mathbb{N}), \{0,1\}^{\mathbb{N}}$

1.2 Probability

- Definitions
  - A **probability space** is a pair $(\Omega, \mathbb{P})$ such that $\mathbb{P} : \mathcal{P}(\Omega) \to [0,1]$ and satisfies these two properties:
    - $\mathbb{P}(\Omega) = 1$
    - $\mathbb{P}(\bigcup_i A_i) = \sum_i \mathbb{P}(A_i)$ where the A_i's form a partition of Ω
      - Alternatively, we can replace the second condition with: $\mathbb{P}(A) = \sum_{\omega \in A} \mathbb{P}(\{\omega\})$
  - Ω is called the **sample space**
  - Each $\omega \in \Omega$ is an **outcome**
  - Each $A \subseteq \Omega$ is an **event**
  - $\mathbb{P}$ is called the **probability measure**
  - Events A, B are **independent** if $\mathbb{P}(A \cap B) = \mathbb{P}(A)\mathbb{P}(B)$
    - This generalizes to more than one event; $A_1, ..., A_n$ are **mutually independent** if $\mathbb{P}(A_{i_1} \cap ... \cap A_{i_k}) = \mathbb{P}(A_{i_1})...\mathbb{P}(A_{i_k})$, with $2 \leq k \leq n$ and $i_1, ..., i_k$ being distinct elements in $[n]$
      Note: *In simpler terms, this says that a set of events is mutually independent if any subset of at least two them is also mutually independent*
    - Alternatively, if $P(B) \neq 0$, $\mathbb{P}(A|B) = \mathbb{P}(A)$
  - Events A and B are **mutually exclusive** if $A \cap B = \varnothing$
  - A **random variable** X is a function from Ω to $\mathbb{R}$
  - The **probability mass function** f of some random variable X is $f : X[\Omega] \to [0,1]$ such that $f(x) = \mathbb{P}(X = x)$
  - Two random variables X and Y are independent if the events $\{X = e\}$ and $\{Y = e'\}$ are independent for all $e, e' \in \mathbb{R}$
- Commonly used formulas
  - **Union**: Let $A, B \subseteq \Omega$. Then, $\mathbb{P}(A \cup B) = \mathbb{P}(A) + \mathbb{P}(B) - \mathbb{P}(A \cap B)$

- **Complement**: Let $A \subseteq \Omega$. Then, $\mathbb{P}(A^c) = 1 - \mathbb{P}(A)$
- **Conditional Probability**: Let $A, B \subseteq \Omega$ such that $\mathbb{P}(B) \neq 0$. Then $\mathbb{P}(A \mid B) = \frac{\mathbb{P}(A \cap B)}{\mathbb{P}(B)}$
- If $B_1, ..., B_n$ form a partition of Ω, then $\mathbb{P}(A) = \sum_{i=1}^{n} \mathbb{P}(A|B_i)\mathbb{P}(B_i)$
- **Bayes' Theorem:** $\mathbb{P}(A \mid B) = \frac{\mathbb{P}(B|A)\mathbb{P}(A)}{\mathbb{P}(B)}$

- Probability distributions
  - A random variable X has a **uniform distribution** if $f(e) = \frac{1}{n}$, where $n = |X[\Omega]|$; in other words, every value of X is equally likely
  - A random variable X has a **Bernoulli distribution with parameter** p if $f(1) = p$ and $f(0) = 1 - p$.

    Note: *Think of this as a variable that represents either a success or failure, with the probability of success being p*
  - A random variable X has a **binomial distribution with parameters** n, p if $f(k) = \binom{n}{k} p^k (1 - p)^{n-k}$

    Note: *Think of X as representing the number of successful trials in an experiment with n trials, where each trial has probability p of success*
  - A random variable X has a **geometric distribution with parameter** p if $f(k) = (1 - p)^{k-1} p$

    Note: *Think of X as representing the number of times you need to try something before you get a success, where the probability of success is p*

- Expected value
  - The **expected value** of a random variable X is $\mathbb{E}[X] = \sum_{e \in X[\Omega]} e \cdot \mathbb{P}(X = e)$
  - The expected value of a Bernoulli random variable with parameter p is p
  - The expected value of a geometric random variable with parameter p is $\frac{1}{p}$
  - The expected value of a binomial random variable with parameters n, p is np
  - **Linearity of expectation**: given random variables X and Y and constants $a, b \in \mathbb{R}$, $\mathbb{E}[aX + bY] = a\mathbb{E}[X] + b\mathbb{E}[Y]$
  - A common strategy for expected value problems is to define an **indicator random variable** X_i
    - X_i is either 1 or 0 depending on whether the event it represents happens or not
    - Usually you have another random variable Y which can be represented as the sum of all the X_i's
    - To find the $\mathbb{E}[Y]$, you apply linearity of expectation and add up the $\mathbb{E}[X_i]$'s
    - Note that $\mathbb{E}[X_i] = \mathbb{P}(X_i = 1)$
  - Be sure to review the coupon collector problem

2 Problems

We've put together a bunch of problems for you to use for review. Again, these problems are **not** necessarily representative of exam problems, but rather meant to test your conceptual understanding of a wide range of topics.

Difficulties of Problems: For each section, problems are ordered roughly from easiest to hardest (by my estimation, which is obviously subjective). In addition, some problems are challenge problems (marked with a $\star$) that are almost definitely more difficult than the problems you can expect on the exam. We've placed hints for these challenge problems in the next section, if you feel like you're stuck.

And, as always, good luck!

2.1 Sets and Functions

Problem 1 (Sullivan 3.11.14)**.** Say $S \subseteq T \subseteq \mathcal{P}(\mathbb{N})$. Show that $\bigcup_{X \in S} X \subseteq \bigcup_{X \in T} X$.

2.2 Induction

Problem 2. Show that $\forall n \in \mathbb{N}^+, \sum_{k=0}^{n-1} 2k + 1 = n^2$

Problem 3. Prove that for any $m \in \mathbb{N}^+$, if $a_1, a_2 ... a_n \in \mathbb{R}^+$, that $\frac{a_1 + a_2 + ... + a_n}{n} \geq \sqrt[n]{a_1 a_2 ... a_n}$, where $n = 2^m$. You can cite 2-variable AM-GM without proof, but not the generalized (n-variable) version.
(In other words, show that AM-GM holds when the number of a_i's is a power of 2.)

2.3 Number Theory

Note: *While I did not put any such problems on this review, you should also be familiar with computing powers and factorials in modular spaces. Also know how to apply the Chinese Remainder Theorem and solve linear Diophantine equations.*

Problem 4 (Clive 3.3.37)**.** Say $n \in \mathbb{N}$ is a composite number and $n \neq 4$. Show that $(n-1)! \equiv 0 \mod n$.

Problem 5. Let p be a prime. Find all integer solutions to the equation $2n^2 + n \equiv_p 0$

Problem 6. Find all $n \in \mathbb{N}$ with $\gcd(n^3 + 2n^2 + 4n + 8, n + 1) = 5$.

Problem 7 (D'Angelo, West 7.31)**.** Say $m \in \mathbb{N}$ is an arbitrary natural and $n = m^2 + 1$. Call a number k a square modulo n if $\exists j \in \mathbb{N}$ s.t. $k \equiv_n j^2$. Show that if k is a square modulo n, so is $-k$.

Problem 8. ($\star$) Let p be a prime such that $p \equiv 1 \mod 4$. Furthermore, suppose there is some $a \in \mathbb{Z}$ such that $\forall k$ with $0 < k < p - 1, a^k \not\equiv_p 0, 1$. Then, show that $\exists n \in \mathbb{N}$ s.t. $n^2 \equiv -1 \mod p$.

Note: *I'm not entirely convinced this is a challenge problem to be honest.*

2.4 Relations

Problem 9. Define a relation R over $\mathbb{Z}$ defined by $(a, b) \in R \iff 2a + 5b \equiv 0 \mod 7$. Show that R is an equivalence relation.

Note: *This is more of an exercise in number theory than relations.*

Problem 10. Suppose R, S are two equivalence relations on some set X. Also, call P_R the set of equivalence classes of R, and P_S the set of equivalence classes of S. Show that $P_R = P_S \implies R = S$ (note: P_R, P_S are sets of sets)

Problem 11. Suppose $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ is a surjective function satisfying the following property:

$$\forall X, Y \subseteq \mathbb{N}, f(X \cup Y) = f(X) \cup f(Y)$$

Define a relation R on $\mathbb{N}$ by $(x, y) \in R \iff \exists X \subseteq \mathbb{N}$ s.t. $x \in X$ and $y \in f(X)$.

Show that R is an equivalence relation, and furthermore that there is only one equivalence class.

Problem 12. Say $\sim_1, \sim_2$ are equivalence relations on some set X satisfying the following property:

$$\forall x \neq y \in X, x \sim_1 y \vee x \sim_2 y \textit{ but not both}$$

In other words, any two distinct elements of X are related by exactly one of the two equivalence relations. Show that one of the two relations is the equality relation (i.e. $\exists i \in \{1, 2\}$ s.t. $x \sim_i y \iff x = y$).

Note: *This was a actually homework problem last year.*

2.5 Finiteness

Problem 13. Let $A \subseteq \mathbb{Z}$ be non-empty. Show that A is finite $\iff$ it has a maximum *and* a minimum element.

Note: *Recall that any non-empty $A \subseteq \mathbb{N}$ is finite $\iff$ it has a maximum element. This fact may be useful in proving the above statement.*

Problem 14 (Clive 6.E.2)**.** Show that $|\mathbb{Z}/n\mathbb{Z}| = n$.

2.6 Counting

Note: *You have a lot of counting practice available so I was a little lazy with this section. Sorry about that :(*

Problem 15. Let $n \in \mathbb{N}$. Show that

$$\sum_{k=1}^{n} k^2 = \binom{n+1}{2} + 2\binom{n+1}{3}$$

Problem 16. Find the number of functions $f : [6] \to [6]$ such that $f(f(f(x))) = x$.

2.7 Inequalities

Problem 17. Use Cauchy-Schwarz to show that $\forall a, b \geq 0, \frac{a+b}{2} \geq \sqrt{ab}$.

Problem 18. Let $a, b \geq 0$ be reals such that $a + b = 4$. Find the minimum value of $a^3 + b^3$.

Problem 19. (⋆) Say $P(x)$ is a polynomial with positive coefficients, and $P(1) \geq \frac{1}{P(1)}$. Show that $\forall x > 0$ that $P(1/x) \geq \frac{1}{P(x)}$.

Problem 20. (⋆) Let $a, b, c \geq 0$. Show that $a^3 + b^3 + c^3 \geq a^2b + b^2c + c^2a$.

Note: *This problem appeared on an excel review sheet before Midterm 3 and nobody really knew how to do it so I've put the problem here in case you want to try it again or see a solution.*

2.8 Countability

Problem 21. Show that the set of relations (not necessarily equivalence relations) on $\mathbb{N}$ is uncountable.

Problem 22. Show that the set of *equivalence* relations on $\mathbb{N}$ is uncountable.

Problem 23. Show that the set of bijections $\mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ is uncountable.

Problem 24. Call a function $f : \mathbb{N} \to \mathbb{N}$ "almost zero" if $\{n \in \mathbb{N} : f(n) \neq 0\}$ is finite (in particular, only a finite number of naturals don't map to 0). Show that the set of almost zero functions is countable.

Problem 25. Let $X \subseteq \mathcal{P}(\mathbb{Q})$ be the set of all subsets of $\mathbb{Q}$ that have no maximum element. (For example, $\{x \in \mathbb{Q} : x^2 \leq 2\} \in X$, but $\{x \in \mathbb{Q} : x^2 \leq 4\} \notin X$, since it has maximum element 2.)
Show that X is uncountable. You may cite without proof that there exists a rational and an irrational between any two distinct reals.

Problem 26. (⋆) We call a real number algebraic if it is the root of some polynomial $p(x)$ that has integer coefficients. So for example, $2/3$ is algebraic ($p(x) = 3x - 2$), as is $\sqrt{2}$ ($p(x) = x^2 - 2$). However, it has been proven that π and e are not algebraic.
Show that the set of algebraic numbers is countable.

2.9 Probability

Problem 27. Ten balls numbered 1 to 6 are placed in a jar. Alice reaches into the jar and removes 2 balls (without replacement). What is the probability that the sum of the numbers on the two balls is even?

Problem 28. Suppose a hundred people line up to board a plane. The first person to board the plan takes a random seat. After that, each person takes their assigned seat if it is unoccupied, or a random seat otherwise. What is the probability that the last person to board the plane gets their assigned seat?

Problem 29. Consider a tournament with 64 teams and 6 rounds. You attempt to predict the winners for all 63 games and get the following points for each correct prediction: 32 for the final winner, 16 for each finalist, and so on, until 1 point for each winner in the first round. How many points can you expect to score if you decide to flip a fair coin for each of the 63 bets?

Problem 30 (AIME 2007)**.** Let P be $\mathcal{P}([4])$ and consider two subsets A, B of $[4]$ that are chosen independently at random from P. What is the probability that B is a subset of at least one of A and $[4] \setminus A$?

Problem 31. Three fair 6-sided dice are rolled. What is the probability that the sum of the three dice is 10, given that the three dice have different values?

Problem 32. Mackey only gives two types of exams: hard or impossible. You will get an impossible exam with probability 0.8. The first question will be marked as difficult with probability 0.9 if the exam is impossible and probability 0.15 otherwise. What is your probability that your exam is impossible given that the first question is marked as difficult?

Problem 33. You distribute 25 apples over 10 boxes randomly. What is the expected number of boxes that will contain exactly 10 apples?

Problem 34. Charlie has a fair 100-sided die and has nothing to do, so he decides to roll the die until he's seen all the numbers at least once. What is the expected number of times Charlie will have to roll the die?

3 Hints

Problem 8. First see if you can find some $m \in \mathbb{N}$ s.t. $m^2 \equiv 1 \bmod p$ and $m \equiv -1 \bmod p$, for any arbitrary odd prime p. Then see if you can use the fact that $p \equiv 1 \bmod 4$ to find a desired n from m.

Problem 19. Let $P(x) = a_n x^n + ... + a_0 x^0$, with $a_0, ...a_n > 0$. Then consider bounding the value of $P(1/x) \cdot P(x)$.

Problem 20. The hint provided by Excel was "Apply AM-GM in a creative way". If that's too vague for you, by hint is to consider the term $a^3 + a^3 + b^3$ and place bounds on it somehow.

Problem 25. First see if you can show that the set of polynomials with integer coefficients is countable.

4 Solutions

Note: *These are the complete solutions to the problems. Once again, we don't expect this much detail on the exam.*

4.1 Sets and Functions

Problem 1 (Sullivan 3.11.14)**.** Say $S \subseteq T \subseteq \mathcal{P}(\mathbb{N})$. Show that $\bigcup_{X \in S} X \subseteq \bigcup_{X \in T} X$.

Solution:

Let $n \in \bigcup_{X \in S} X$. We want to show $n \in \bigcup_{X \in T} X$.

By the definition of $\bigcup$, $\exists S' \in S$ with $n \in S'$. But since $S \subseteq T, S' \in T$. Then $n \in S' \subseteq \bigcup_{X \in T} X$.

Then we are done. ■

4.2 Induction

Problem 2. Show that $\forall n \in \mathbb{N}^+, \sum_{k=0}^{n-1} 2k+1 = n^2$

Solution:

We do this (obviously) by induction.

Let $P(n) =$ "$\sum_{k=0}^{n-1} 2k+1 = n^2$" for $n \geq 1$.

Base Case: $P(1)$.

The left side is $\sum_{k=0}^{0} 2k+1 = 2 \cdot 0 + 1 = 1$. The right side is $1^1 = 1$. Clearly they are equal. Hence $P(1)$ holds.

Inductive Hypothesis: Suppose $\forall i \leq n, P(i)$ is true.

Induction Step: We want to show $P(n+1)$ is true. In other words, we want to show $\sum_{k=0}^{n} 2k+1 = (n+1)^2$.

$$\begin{aligned} \sum_{k=0}^{n} 2k+1 &= \left(\sum_{k=0}^{n-1} 2k+1 \right) + (2n+1) \\ &= n^2 + 2n + 1 && \text{(by IH)} \\ &= (n+1)^2 \end{aligned}$$

Then, by the strong principle of mathematical induction, $P(n)$ is true $\forall n \geq 1$. ■

Note: *While we could have done this with weak induction, it does not harm to use strong induction. It still proves the result we want, and when starting a problem you will often not know whether you need strong or weak induction so using strong induction is a safe bet.*

Problem 3. Prove that for any $m \in \mathbb{N}^+$, if $a_1, a_2 ... a_n \in \mathbb{R}^+$, that $\frac{a_1+a_2+...+a_n}{n} \geq \sqrt[n]{a_1 a_2 ... a_n}$, where $n = 2^m$.
You can cite 2-variable AM-GM without proof, but not the generalized (n-variable) version.
(In other words, show that AM-GM holds when the number of a_i's is a power of 2.)

Solution:

We do this by induction on m.

Let $P(m) =$ "$\forall a_1, ...a_n \in \mathbb{R}^+, \frac{a_1+...+a_n}{n} \geq \sqrt[n]{a_1 ... a_n}$, where $n = 2^m$" for $m \geq 1$.

Base Case: $P(1)$. In this case $n = 2$, so we wish to show $\forall a_1, a_2 \in \mathbb{R}^+, \frac{a_1+a_2}{2} \geq \sqrt{a_1 a_2}$. Since this is simply AM-GM in 2 variables, we can cite this without proof.

Inductive Hypothesis: Suppose that $\forall i \leq m, P(i)$ holds.

Induction Step: We want to show $P(m+1)$ holds.

Let $n = 2^m$. Then $2n = 2^{m+1}$. We then want to show that $\forall a_1, ...a_{2n} \in \mathbb{R}^+, \frac{a_1+...+a_{2n}}{2n} \geq \sqrt[2n]{a_1...a_{2n}}$.

We know $\frac{a_1+...+a_{2n}}{2n} = \frac{1}{2}\left(\frac{a_1+...+a_n}{n} + \frac{a_{n+1}+...+a_{2n}}{n}\right)$.

By n-variable AM-GM (which we assumed to be true in our IH, since $n = 2^m$), we have that $\frac{a_1+...+a_n}{n} \geq \sqrt[n]{a_1...a_n}$ and $\frac{a_{n+1}+...+a_{2n}}{n} \geq \sqrt[n]{a_{n+1}+...+a_{2n}}$. Then:

$$\begin{aligned}
\frac{a_1+...+a_{2n}}{2n} &= \frac{1}{2}\left(\frac{a_1+...+a_n}{n} + \frac{a_{n+1}+...+a_{2n}}{n}\right) \\
&\geq \frac{1}{2}\left(\sqrt[n]{a_1...a_n} + \sqrt[n]{a_{n+1}...a_{2n}}\right) && \text{(as explained above)} \\
&\geq \sqrt{\sqrt[n]{a_1...a_n} \cdot \sqrt[n]{a_{n+1}...a_{2n}}} && \text{(by 2-variable AM-GM)} \\
&= \sqrt{\sqrt[n]{a_1...a_n a_{n+1}...a_{2n}}} \\
&= \left(\sqrt[n]{a_1...a_{2n}}\right)^{1/2} \\
&= \left((a_1...a_{2n})^{1/n}\right)^{1/2} \\
&= (a_1...a_{2n})^{1/2n} \\
&= \sqrt[2n]{a_1...a_{2n}}
\end{aligned}$$

This is our desired result. Then, we are done. ■

Note: *Historically, AM-GM was actually proved using induction, but a different variant than what was taught in class. If we let $P(n)$ denote n-variable AM-GM, it was proven that $P(n) \implies P(2n)$ (which was essentially proven above) and $P(n) \implies P(n-1)$. Although this seems strange, using a base case of $P(2)$, this actually implies $\forall n \geq 2, P(n)$. For example, if we wanted to show that $P(13)$ held, we'd note that $P(2) \implies P(4) \implies P(8) \implies P(16) \implies P(15) \implies P(14) \implies P(13)$. You should see how this generalizes to any natural.*

4.3 Number Theory

Problem 4 (Clive 5.3.37)**.** Say $n \in \mathbb{N}$ is a composite number and $n \neq 4$. Show that $(n-1)! \equiv 0 \bmod n$.

Solution:

Say n is a composite number. There are two cases:

Case 1: $n = p^2$ for some prime p with $2 < p < n$

First, note that $p > 2$, so $2p < p^2 = n$. Then $p < 2p < n$ (this implies $p \leq 2p-1$ and $2p \leq n-1$). In particular, $p! \mid (2p-1)!$, so $p \mid (2p-1)!$. Then $p(2p) \mid (2p)!$ and $(2p)! \mid (n-1)!$. Then $2p^2 \mid (n-1)!$ and so $p^2 \mid (n-1)!$. But $p^2 = n$, so $n \mid (n-1)!$.

Case 2: $n = pq$, with $1 < p, q < n$ and $p \neq q$. (Note: If $n \neq p^2$ for any prime p, we can necessarily find two distinct numbers p, q that have product n. For example, we could take p to be a prime factor of n, and let $q = n/p \neq p$).

WLOG say $p < q$.

Then note that $p \mid p!$ and $p! \mid (q-1)!$ (since $q-1 \geq p$). Then $p \mid (q-1)!$. This implies $pq \mid q!$. Then, we have that $n \mid q!$. But $q < n \implies q! \mid (n-1)!$, so $n \mid (n-1)!$.

Since $n \mid (n-1)!$ in both cases, we have that $(n-1)! \equiv 0 \bmod n$. ■

Note: *The first case is necessary here because the second case assumes that you can find two nontrivial distinct prime factors for n, but if n is a prime number squared that is not true. Without the first case, when you WLOG that $p < q$, you actually are losing generality.*

Problem 5. Let p be a prime. Find all integer solutions to the equation $2n^2 + n \equiv_p 0$

Solution:

We claim that if $p = 2$, then $2n^2+n \equiv_p 0 \iff n \equiv_2 0$ and if $p > 2$, then $2n^2+n \equiv_p 0 \iff n \equiv_p 0 \vee n \equiv_p \frac{p-1}{2}$ (note $p > 2 \implies p$ odd, so $\frac{p-1}{2}$ is an integer).

We now prove this:

$\underline{p = 2}$: Since $\forall n \in \mathbb{Z}, 2n^2 \equiv_2 0$, we have that $2n^2 + n \equiv_2 0 \iff n \equiv_2 0$.

$\underline{p > 2}$: This is unfortunately more involved. It's not *that* bad though.

$$\begin{aligned}
& 2n^2 + n \equiv_p 0 \\
\iff & p \mid 2n^2 + n \\
\iff & p \mid n(2n+1) \\
\iff & p \mid n \vee p \mid 2n+1 \\
\iff & n \equiv_p 0 \vee 2n+1 \equiv_p 0 \\
\iff & n \equiv_p 0 \vee 2n \equiv_p -1 \equiv p-1 \\
\iff & n \equiv_p 0 \vee n \equiv_p 2^{-1}(p-1)
\end{aligned}$$

Now, note that $p-1$ is even, so $\frac{p-1}{2}$ is an integer. Furthermore, $\frac{p-1}{2} \cdot 2 = p-1$. Then $\frac{p-1}{2} \equiv_p 2^{-1}(p-1)$.

Then $2n^2 + n \equiv_p 0 \iff n \equiv_p 0 \vee n \equiv_p \frac{p-1}{2}$.

This proves our claim. ■

Problem 6. Find all $n \in \mathbb{N}$ with $\gcd(n^3 + 2n^2 + 4n + 8, n+1) = 5$.

Solution:

We do the Euclidean Algorithm

$$\begin{aligned}
& \gcd(n^3 + 2n^2 + 4n + 8, n+1) \\
= & \gcd(n^3 + 2n^2 + 4n + 8 - n^2(n+1), n+1) \\
= & \gcd(n^2 + 4n + 8, n+1) \\
= & \gcd(n^2 + 4n + 8 - n(n+1), n+1) \\
= & \gcd(3n + 8, n+1) \\
= & \gcd(3n + 8 - 3(n+1), n+1) \\
= & \gcd(5, n+1)
\end{aligned}$$

So, $\gcd(n^3 + 2n^2 + 4n + 8, n+1) = 5$ exactly when $\gcd(5, n+1) = 5$. But when does $\gcd(5, n+1) = 5$? We know that $\gcd(5, n+1) \in \{1, 5\}$ since it is a factor of 5. So we need simply make sure 5 is a factor of $n+1$. 5 being a common factor of 5 and $n+1$ will automatically imply it is the greatest common factor.

Note that 5 is a factor of $n+1 \iff n \equiv 4 \bmod 5$.

Then $\gcd(n^3 + 2n^2 + 4n + 8, n + 1) = 5 \iff n \equiv 4 \bmod 5$. ■

Note: *It is a common misconception that that* $\gcd(a, b) = \gcd(b, r)$ *if* r *is the remainder when dividing* a *by* b *(i.e.* $a = qb + r, 0 \leq r < b$*). But this is not actually true - in the above example, without knowing what* n *is, we don't quite know whether our remainders satisfy that inequality. However, we don't need this to hold. We simply have that* $\gcd(qb + r, b) = \gcd(b, r)$*. More simply,* $\forall q \in \mathbb{Z}, \gcd(a, b) = \gcd(b, a - qb)$*. We can subtract any multiple of* b *from* a *and the equality still holds.*

Problem 7 (D'Angelo, West 7.31)**.** Say $m \in \mathbb{N}$ is an arbitrary natural and $n = m^2 + 1$. Call a number k a square modulo n if $\exists j \in \mathbb{N}$ s.t. $k \equiv_n j^2$. Show that if k is a square modulo n, so is $-k$.

Solution:

Suppose k is a square modulo n. Note that $n = m^2 + 1$, so $m^2 \equiv_n -1$

Then $\exists j \in \mathbb{N}$ s.t. $j^2 \equiv_n k$. Then, consider $(jm)^2$ in $\mathbb{Z}/n\mathbb{Z}$.

$(jm)^2 \equiv_n j^2m^2 \equiv_n km^2 \equiv_n k(-1) \equiv_n -k$ Then $(jm)^2 \equiv_n -k$, and so $-k$ is a square modulo n ■

Problem 8. (⋆) Let p be a prime such that $p \equiv 1 \bmod 4$. Furthermore, suppose there is some $a \in \mathbb{Z}$ such that $\forall k$ with $0 < k < p - 1, a^k \not\equiv_p 0, 1$. Then, show that $\exists n \in \mathbb{N}$ s.t. $n^2 \equiv -1 \bmod p$.

Solution:

Let $m = \frac{p-1}{4}$. Note that this is an integer since $p \equiv_4 1$. Then, we claim that a^m is our desired n. Now we prove this.

First, consider this lemma: $\forall x \in \mathbb{Z}, x^2 \equiv_p 1 \iff x \equiv_p \pm 1$. (Note that this was on your homework).

Now, we use this to show our desired claim. We have that $a^{p-1} \equiv_p 1$ by FLT (note: $p \nmid a$, since $a^1 \neq 0$).

Also, $n^4 \equiv_p (a^{\frac{p-1}{4}})^4 \equiv_p a^{p-1} \equiv_p 1$.

Then, we have that $n^2 \equiv_p \pm 1$. But, $n^2 \equiv a^{\frac{p-1}{2}} \not\equiv 1$ by the assumption in the problem. Then $n^2 \equiv -1$.

Then we are done. ■

4.4 Relations

Problem 9. Define a relation R over $\mathbb{Z}$ defined by $(a, b) \in R \iff 2a + 5b \equiv 0 \bmod 7$. Show that R is an equivalence relation.

Solution:

Note that for any $a, b \in \mathbb{Z}$, $2a + 5b \equiv_7 0 \iff 2a \equiv_7 -5b \iff 2a \equiv_7 2b \iff 4 \cdot 2a \equiv_7 4 \cdot 2b \iff 8a \equiv_7 8b \iff a \equiv_7 b$.

So, the relation defined in the problem is just congruence $\bmod 7$. We know this to be an equivalence relation.
Note: *It may be helpful to make sure you can reproduce the proof from definitions of mods.* ■

Problem 10. Suppose R, S are two equivalence relations on some set X. Also, call P_R the set of equivalence classes of R, and P_S the set of equivalence classes of S. Show that $P_R = P_S \implies R = S$ (note: P_R, P_S are sets of sets)

Solution:

Let $x, y \in X$. We want to show $(x, y) \in R \iff (x, y) \in S$ (i.e. double containment). We will show one direction, and noting that the other direction is symmetric, this proves that $R = S$.

Suppose $(x, y) \in R$. Since P_R is a partition of X, we have that $\exists X' \in P_R$ s.t. $x \in X'$. But since P_R is a set

of equivalence classes and $(x, y) \in R$, we have that $y \in X'$. But $P_R = P_S$, so $X' \in P_S$. Then, x and y are in the same equivalence classes of S. Then $(x, y) \in S$. ■

Note: *On Excellent Review 2, we have you prove that given a partition of a set X, you could construct an equivalence relation $\sim$ over X such that the partition formed the equivalence classes of $\sim$. This problem shows that given two equivalence relations $\sim_1, \sim_2$ over some set X, if they share the same equivalence classes, they must be the same. Putting these together, we can see that given a partition of some set X, there exists a unique equivalence relation whose equivalence classes form the given partition.*

Problem 11. Suppose $f : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ is a surjective function satisfying the following property:

$$\forall X, Y \subseteq \mathbb{N}, f(X \cup Y) = f(X) \cup f(Y)$$

Define a relation R on $\mathbb{N}$ by $(x, y) \in R \iff \exists X \subseteq \mathbb{N}$ s.t. $x \in X$ and $y \in f(X)$.

Show that R is an equivalence relation, and furthermore that there is only one equivalence class.

Solution:

We do this by showing that $\forall m, n \in \mathbb{N}, (m, n) \in R$. This proves all three properties required for a relation to be an equivalence relation, and also proves that there is only one equivalence class.

Let $m, n \in \mathbb{N}$. We have that f is surjective, so $\exists X \subseteq \mathbb{N}$ with $f(X) = \{n\}$. Then define $X' = \{m\} \cup X$. We have that $f(X') = f(\{m\}) \cup f(X) = f(\{m\}) \cup \{n\}$. Then $m \in X'$ and $n \in f(X')$. Hence $(m, n) \in R$.

Then, since everything is related to everything else, R is an equivalence relation with only one equivalence class. ■

Problem 12. Say $\sim_1, \sim_2$ are equivalence relations on some set X satisfying the following property:

$$\forall x \neq y \in X, x \sim_1 y \vee x \sim_2 y \textit{ but not both}$$

In other words, any two distinct elements of X are related by exactly one of the two equivalence relations. Show that one of the two relations is the equality relation (i.e. $\exists i \in \{1, 2\}$ s.t. $x \sim_i y \iff x = y$).

Solution:

We first prove a lemma that does most of the heavy lifting for this problem:

Given distinct $x, y, z \in X$, either all three are related by $\sim_1$, or all three are related by $\sim_2$, but it is not possible for both relations to relate elements within $\{x, y, z\}$.

Suppose $x \sim_1 y$. Then we have two cases:

1. $x \sim_1 z$ or $y \sim_1 z$. If either is true, we have by transitivity (and possibly symmetry) $x \sim_1 y, x \sim_1 z, y \sim_1 z$, and none of these are related by $\sim_2$.
2. $x \not\sim_1 z$ and $y \not\sim_1 z$. Then $x \sim_2 z$ and $y \sim_2 z$ by the statement in the problem. Then by transitivity and symmetry, we have that $x \sim_2 y$. But this is a contradiction since $x \sim_1 y$. Hence this case is impossible.

If $x \sim_2 y$, we have a similar proof. In either case, our lemma holds.

Now, pick two distinct elements $x, y \in X$ (if no two exist, $|X| = 1$, and so $\sim_1, \sim_2$ are both the equality relation). WLOG $x \sim_1 y$ (the $\sim_2$ case is identical). Then $\forall z, x \sim_1 z, y \sim_1 z$ by the lemma. Then by transitivity, we have that any two elements in X are related by $\sim_1$. Then no two distinct elements are related by $\sim_2$, and so $\sim_2$ is the equality relation.

Then, we are done.

■

4.5 Finiteness

Problem 13. Let $A \subseteq \mathbb{Z}$ be non-empty. Show that A is finite $\iff$ it has a maximum *and* a minimum element.

Solution:

$(\Rightarrow)$:

Suppose A is finite. Let $A^+ = \{z \in \mathbb{Z} : z \geq 0\}$ and $A^- = \{z \in \mathbb{Z} : z \leq 0\}$. Let $B = \{-z : z \in A^-\}$. (Note that all these sets could contain 0, the $+$'s and $-$'s can be misleading.)

Note that $A = A^+ \cup A^-$. Then A^+, A^- are both finite. Since we can biject between A^- and B (by the map $f(z) = -z$), we have that B is finite.

But A^+, B contain only non-negative numbers, and hence are both finite subsets of $\mathbb{N}$. They both then have maximum elements. Call these a and b respectively. Then, a is a maximum of A (since $a \in A$, every element of A^+ is smaller than a by definition of maximum, and $a \geq 0$ and every element in A^- is non-positive). Also, $-b$ is the minimum of A^- and hence of A.

Then A has a minimum and a maximum.

$(\Leftarrow)$:

Suppose a is the maximum of A and b is the minimum. Then $A \subseteq \{z \in \mathbb{Z} : b \leq z \leq a\}$. But this is a set of size $a - b + 1$ (we can biject to $[a - b + 1]$ via $f(z) = z - b + 1$). Then A is finite and has size at most $a - b + 1$. ■

Problem 14 (Clive 6.E.2)**.** Show that $|\mathbb{Z}/n\mathbb{Z}| = n$.

Solution:

We show this by bijecting from $[n]$ to $\mathbb{Z}/n\mathbb{Z}$.

Define $f(m) = [m]_n$. In other words, map m to its equivalence class in $\mathbb{Z}/n\mathbb{Z}$. Totality and uniqueness of this function are clear. Existence follows from the definition of $\mathbb{Z}/n\mathbb{Z}$

Surjectivity: Let $a \in \mathbb{Z}$. We want to show $[a]_n$ is mapped to. By the division algorithm, find r with $a = qn + r$ and $0 \leq r < n$. If $r = 0$, replace it with n, so that $r \in [n]$. Then $f(r) = [a]_n$. To do this, it suffices to show $a \equiv_n r$. Ir $r \neq 0$, we have that $a = qn + r \equiv_n r$. If $r = n$, then $a = qn + 0 \equiv_n 0$ and $r \equiv_n 0$. In either case $a \equiv_n r$. Hence, $f(r) = [a]_n$, and we are done.

Injectivity: Let $a, b \in [n]$ with $f(a) = f(b)$. Then $[a]_n = [b]_n$, and in particular, $a \in [b]_n$. Then $a \equiv_n b$, and so $n \mid a - b$. But $|a - b| < n$ since $a, b \in [n]$. Then $a - b = 0$, so $a = b$. Then we are done.

Hence, this function is bijective, and so $|\mathbb{Z}/n\mathbb{Z}| = n$. ■

4.6 Counting

Problem 15. Let $n \in \mathbb{N}$. Show that

$$\sum_{k=1}^{n} k^2 = \binom{n+1}{2} + 2\binom{n+1}{3}$$

Solution:

Let $S = \{(i, j, k) \mid 0 \leq i, j < k \leq n\}$.

LHS:

We partition on k. Since $k > 0$, $k \geq 1$. Similarly, $k \leq n$ from the definition of S. Then, for each k we pick i and j. There are k choices as i and j are between 0 and $k-1$ inclusive. So by IMP, there are k^2 choices for each case. The cases are disjoint since the largest element in the tuple must be different for different k, so there's no overlap between the cases.

RHS:

We case on whether $i = j$ or not.

Case 1: If $i = j$:

Then we pick 2 elements out of the $n+1$. There are $\binom{n+1}{2}$ ways to do so. We assign the larger one to be k and the smaller one to be i and j.

Case 2: If $i \neq j$:

Then we pick 3 elements out of the $n+1$. There are $\binom{n+1}{2}$ ways to do so. We assign the largest one to be k and pick one of the remaining 2 to be j (the last one is assigned to i). Since there are 2 choices for j, by IMP we have that there are $2\binom{n+1}{3}$ possible tuples total.

Since these cases are disjoint (it's impossible to have $i = j$ and $i \neq j$) and exhaustive (as one of these cases must occur for every tuple in S by Law of Excluded Middle), by the addition principle, $|S| = \binom{n+1}{2} + 2\binom{n+1}{3}$. ■

Problem 16. Find the number of functions $f : [6] \to [6]$ such that $f(f(f(x))) = x$.

Solution:

We note that for f to satisfy this property, it must do one of two things to every element:

- Map x to itself (so $f(x) = x$)
- Map x to some distinct y and map y to some $z \neq x$, but map z to x (so $f(x) = y, f(y) = z, f(z) = x$

In other words, if we were to chain f on some element of [6], we should get either a cycle of three elements, or stay at a single element forever.

We partition based on the number of such cycles it has.

- No cycles: Then $\forall x \in [6], f(x) = x$. There is only one such function.
- 1 cycle: We create a function of this form using a multi-step process:
  (i) We pick 3 elements to not be in the cycle. There are $\binom{6}{3}$ ways to do this.
  (ii) Given the 3 remaining elements, we form a cycle. We do this by taking the lowest of the three, and picking which of the other two to map it to. This uniquely determines the cycle. There are 2 ways to do this.

  By the dependent multiplication principle, there are $2\binom{6}{3}$ ways to do this.
- 2 cycles: In this case every number is in a cycle. We form our two cycles using the following multi-step process:
  (i) Pick two elements to be in the same cycle as 1. There are $\binom{5}{2}$ ways to do this. Note: *Just picking 3 elements to be in a cycle overcounts: for example you could pick $\{2, 4, 5\}$ to be a cycle, or $\{1, 3, 6\}$, but those correspond to the same two sets of cycles*
  (ii) Pick what element 1 maps to. This uniquely identifies the entirely cycle that 1 is in. There are 2 ways to do this.
  (iii) Given the 3 remaining elements, take the lowest of the three, and pick which of the other two to map it to. This uniquely determines the other cycle. There are 2 ways to do this.

By the dependent multiplication principle, there are $2^2\binom{5}{2}$ ways to do this.

These are mutually exclusive because there is a unique number of cycles in this function. It is exhaustive because there are 6 elements, which can form at most 2 disjoint cycles, so these are the only possibilities.

Then, we use the addition principle. This gives us that the total number of such functions is

$$1 + 2\binom{6}{3} + 2^2\binom{5}{2} = 81$$

■

4.7 Inequalities

Problem 17. Use Cauchy-Schwarz to show that $\forall a, b \geq 0$, $\frac{a+b}{2} \geq \sqrt{ab}$.

Solution:

Consider $\vec{v} = (\sqrt{a}, \sqrt{b})$ and $\vec{w} = (\sqrt{b}, \sqrt{a})$. By Cauchy-Schwarz, we have that $|\vec{v} \cdot \vec{w}|^2 \leq ||\vec{v}||^2 \cdot ||\vec{w}||^2$.

Now $\vec{v} \cdot \vec{w} = \sqrt{a}\sqrt{b} + \sqrt{b}\sqrt{a} = 2\sqrt{ab}$. Also, $||\vec{v}|| = ||\vec{w}|| = \sqrt{\sqrt{a}^2 + \sqrt{b}^2} = \sqrt{a+b}$.

Then, by Cauchy-Schwarz, we have that $2\sqrt{ab} \leq a + b$. Dividing by 2, we get $\frac{a+b}{2} \geq \sqrt{ab}$ ■

Note: *Please remember how to spell the name "Schwarz" - you'd be surprised how some of you spelled it on the last midterm.*

Problem 18. Let $a, b \geq 0$ be reals such that $a + b = 4$. Find the minimum value of $a^3 + b^3$.

Solution:

The minimum value is 16.

First, note that $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3 + 3ab(a+b)$. Substituting for $a+b$, we have that: $64 = a^3 + b^3 + 12ab$. Now, we have from AM-GM that $\frac{a+b}{2} \geq \sqrt{ab} \implies 2 \geq \sqrt{ab} \implies ab \leq 4$. Then, $64 = a^3 + b^3 + 12ab \leq a^3 + b^3 + 12 \cdot 4$.

From this, we get that $a^3 + b^3 \geq 16$. Now we need to show that there are values for a, b where $a^3 + b^3 = 16$.

But take $a = b = 2$. Clearly $a + b = 4$ and $a^3 + b^3 = 16$.

Then 16 is the minimum value of $a^3 + b^3$. ■

Note: *When asked to find the minimum (or maximum) value of some expression - you have to: state a value you claim to be the minimum (maximum), show that the given expression is always at least (at most) your value and show that the given expression is exactly equal to your value at some point.*
For example, if I asked you to find the minimum value of x^2 over the reals, you could not say that the minimum is -1000. While it is certainly true that -1000 is a lower bound for x^2, it's a very loose bound - the real minimum of x^2 is 0.
However, if asked simply to prove an inequality (say the problem above was to simply prove that $a^3+b^3 \geq 16$), you need not show that equality is attained - indeed sometimes it may not be true that equality is attained. Also note that equality is usually attained when all the terms are equal to each other.

Problem 19. (⋆) Say $P(x)$ is a polynomial with positive coefficients, and $P(1) \geq \frac{1}{P(1)}$. Show that $\forall x > 0$ that $P(1/x) \geq \frac{1}{P(x)}$.

Solution:

Say $P(x) = a_n x^n + ... + a_1 x + a_0$. Note that $P(1) = a_n + ... + a_0$. We have that $P(1) \geq \frac{1}{P(1)}$, and since $P(1) > 0$ (the coefficients are positive), we have that $[P(1)]^2 \geq 1$.

Then, let $x > 0$, consider $P(1/x)P(x)$. This is exactly

$(a_n \frac{1}{x^n} + ... + a_1 \frac{1}{x} + a_0)(a_n x^n + ... + a_0)$

We now use Cauchy-Schwarz to bound this quantity:

Take $\vec{v} = \left(\frac{\sqrt{a_n}}{x^{n/2}} \quad \frac{\sqrt{a_{n-1}}}{x^{(n-1)/2}} \quad \dots \quad \frac{\sqrt{a_1}}{x^{1/2}} \quad \sqrt{a_0}\right)$ and $\vec{w} = \left(\sqrt{a_n}x^{n/2} \quad \dots \quad \sqrt{a_1}x^{1/2} \quad \sqrt{a_0}\right)$

Then $||\vec{v}||^2 = P(1/x)$ and $||\vec{w}||^2 = P(x)$. Also note that $\vec{v} \cdot \vec{w} = a_n + ... + a_0 = P(1)$.

Then by Cauchy-Schwarz, we have that $||\vec{v}||^2||\vec{w}||^2 \geq (\vec{v}\vec{w})^2$. Substituting, we have $P(1/x)P(x) \geq [P(1)]^2$.

But $[P(1)]^2 \geq 1$.

Then we are done. ■

Problem 20. (⋆) Let $a, b, c \geq 0$. Show that $a^3 + b^3 + c^3 \geq a^2b + b^2c + c^2a$.

Solution:

Note that by AM-GM, we have that $\frac{a^3+a^3+b^3}{3} \geq \sqrt[3]{a^6b^3} = a^2b$.

Similarly, $\frac{b^3+b^3+c^2}{3} \geq b^2c$ and $\frac{c^2+c^2+a^2}{3} \geq c^2a$.

Adding these three inequalities together, we get

$\frac{(a^3+a^3+b^3)+(b^3+b^3+c^3)+(c^3+c^3+a^3)}{3} \geq a^2b + b^2c + c^2a$. But the left side is simply $a^3 + b^3 + c^3$.

Then, we have proven the desired inequality. ■

4.8 Countability

Problem 21. Show that the set of relations (not necessarily equivalence relations) on $\mathbb{N}$ is uncountable.

Solution:

We note that there exists a natural bijection from the set of relations on $\mathbb{N}$ to the $\mathcal{P}(\mathbb{N} \times \mathbb{N})$ defined by the function that maps a relation to its graph. Then, we need simply show $\mathcal{P}(\mathbb{N} \times \mathbb{N})$ is uncountable.

But we know that $\mathbb{N} \times \mathbb{N}$ is countably infinite, and by Cantor's theorem, there is no surjection $\mathbb{N} \times \mathbb{N} \to \mathcal{P}(\mathbb{N} \times \mathbb{N})$. If $\mathcal{P}(\mathbb{N} \times \mathbb{N})$ were countable (it would have to then be countable infinite), we could biject it to the naturals, which can be bijected to $\mathbb{N} \times \mathbb{N}$, giving us a bijection between $\mathbb{N} \times \mathbb{N}$ and its powerset. Since this is impossible, $\mathcal{P}(\mathbb{N} \times \mathbb{N})$ must be uncountable. ■

Problem 22. Show that the set of *equivalence* relations on $\mathbb{N}$ is uncountable.

Solution:

We shall show that the set of equivalence relations on $\mathbb{N}$ is uncountable by injecting an uncountable set (namely, $\mathcal{P}(\mathbb{N} \setminus \{0\})$) onto it. Let X be the set of equivalence relations on $\mathbb{N}$.

Then, define the following function:

$f(A) = R_A$, where R_A is defined as the following:

$(x, y) \in R_A \iff x, y \in A \cup \{0\}$ or $x, y \notin A \cup \{0\}$

In other words, we map A to the equivalence relation that has two equivalence classes: one containing all of A and 0, and one containing everything else.

This function is well-defined since we defined a partition of $\mathbb{N}$ ($\{A \cup \{0\}, \mathbb{N} \setminus \{A \cup \{0\}\}$) and we know from a

previous Excellent Review that you this definition of a relation based on a partition defines an equivalence relation.

Now, we show injectivity via the contrapositive. Suppose $A \neq A' \subseteq \mathbb{N} \setminus \{0\}$. Then there is some $a \in A \setminus A'$ or $A' \setminus A$. WLOG say $a \in A \setminus A'$. Then $(0, a) \in R_A$ but $(0, a) \notin R_{A'}$. Hence $f(A) \neq f(A')$.

Then, this function is injective.

Then we are done. ■

Note: *The intuition behind this proof is given a set A, we can define an equivalence relation based on the partition $\{A, \mathbb{N} \setminus A\}$. This ends up not quite working though, because then A and $\mathbb{N} \setminus A$ map to the same equivalence relation. So we break the symmetry by adding a 0 to one of the two sides. Once you get the idea, most of this is formalizing it, but the formalisms are typically not the hard parts of such problems.*

Problem 23. Show that the set of bijections $\mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ is uncountable.

Solution:

We inject $\mathcal{P}(\mathbb{N})$ onto the set of bijections (which we call X).

Define a function $f(A) = g_A$, where $g_A : \mathcal{P}(\mathbb{N}) \to \mathcal{P}(\mathbb{N})$ is defined by $g_A(B) = B \triangle A$ (where $\triangle$ is the symmetric difference: $C \triangle C' = (C \setminus C') \cup (C' \setminus C)$). Since g_A is its own inverse, it is clearly bijective.

Now, we wish to show f is injective. Suppose $f(A) = f(A')$. Then $g_A = g_{A'}$ and so $g_A(\varnothing) = g_{A'}(\varnothing)$. But $g_A(\varnothing) = A$ and $g_{A'}(\varnothing) = A'$, so $A = A'$.

Then we are done. ■

Problem 24. Call a function $f : \mathbb{N} \to \mathbb{N}$ "almost zero" if $\{n \in \mathbb{N} : f(n) \neq 0\}$ is finite (in particular, only a finite number of naturals don't map to 0). Show that the set of almost zero functions is countable.

Solution:

First, note that the set of *finite* subsets of $\mathbb{N} \times \mathbb{N}$ is countable. Call this set X. We shall first prove X is countable.

We partition X into $\bigcup_{k \in \mathbb{N}} X_k$, where $X_k = \{X' \in X : |X'| = k\}$ is the set of elements of X that have size k. We can inject $X_k \to (\mathbb{N} \times \mathbb{N})^k$ by the following:

$f(\{(x_1, y_1), (x_2, y_2), ...(x_k, y_k)\} = ((x_1, y_1), (x_2, y_2), ...(x_k, y_k))$, where we order the (x_i, y_i)'s in increasing order of the first coordinate, breaking ties with the second coordinate. Then, this function is well-defined, and injective, since if two sets X_1, X_2 both map to the same tuple, then X_1 and X_2 are both the set of elements in the tuple, and so $X_1 = X_2$.

Since $(\mathbb{N} \times \mathbb{N})$ is countable, so is $(\mathbb{N} \times \mathbb{N})^k$, and so X_k is countable. Since X is a countable union of X_k's, each of which is countable, X is countable.

Now, we show that set of "almost zero" functions is countable. Let Z denote this set. We will inject Z onto X in the following manner:

$f(g) = \{(n, g(n)) : g(n) \neq 0\}$. This is finite since there are only finitely many n such that $g(n) \neq 0$ (since g is almost zero). Also, f is an injection:

Say $f(g_1) = f(g_2)$. Then $\forall (m, n) \in f(g_1) = f(g_2)$, we have that $g_1(m) = g_2(m) = n$. Furthermore, for every natural that is not the first element of a tuple in $f(g_1)$, it must map to 0 under both g_1 and g_2. Then g_1 and g_2 agree on all points, and so $g_1 = g_2$.

Since we injected Z onto X, we have that Z is countable. ■

Problem 25. Let $X \subseteq \mathcal{P}(\mathbb{Q})$ be the set of all subsets of $\mathbb{Q}$ that have no maximum element. (For example, $\{x \in \mathbb{Q} : x^2 \leq 2\} \in X$, but $\{x \in \mathbb{Q} : x^2 \leq 4\} \notin X$, since it has maximum element 2.)
Show that X is uncountable. You may cite without proof that there exists a rational and an irrational

between any two distinct reals.

Solution:

We inject the reals onto X. In particular, let $f : \mathbb{R} \to X$ be defined via $f(r) = \{q \in \mathbb{Q} : q < r\}$. First, we claim that this function is well-defined. Totality and uniqueness are clear, so let's simply prove existence.

We wish to show that $\forall r \in \mathbb{R}, \{q \in \mathbb{Q} : q < r\}$ has no maximal element. We do this by contradiction. Suppose a was the maximum element of $\{q \in \mathbb{Q} : q < r\}$. Then $a < r$. But then we can find some other rational a' between a and r, and so a is not a maximum. Hence, the function is well defined.

We now wish to show it is injective. We do this by contrapositive. Suppose $r \neq s$ (WLOG $r > s$). We wish to show $f(r) \neq f(s)$. To do this, pick any q between s and r. Since $s < q < r$, we have that $q \in f(r)$ but $q \notin f(s)$. Hence $f(r) \neq f(s)$.

Then our function is injective, so C is uncountable. ■

Problem 26. (⋆) We call a real number algebraic if it is the root of some polynomial $p(x)$ that has integer coefficients. So for example, $2/3$ is algebraic ($p(x) = 3x - 2$), as is $\sqrt{2}$ ($p(x) = x^2 - 2$). However, it has been proven that π and e are not algebraic.
Show that the set of algebraic numbers is countable.

Solution:

We first show that the set of polynomials over the integers is countable. Call this set P

We partition the polynomials by their degree. Let P_d be the set of polynomials over the integers that have degree at most d. We can then inject P_d onto $\mathbb{Z}^{d+1}$ by mapping $a_d x^d + ... + a_0$ to $(a_d, ...a_0)$. This is clearly an injection, since if all the a_i's are the same, the polynomial must be the same.

Note: *This function is actually a bijection, but if you don't need to show surjectivity, don't! Save your effort for things you actually need in the proof.*

Then P_d is countable and $P = \bigcup_{d \in \mathbb{N}} P_d$, so P is countable (countable union of countable sets is countable).

Now, we show that the set of algebraic numbers (call it A) is countable.

In particular, define $f : A \to P \times \mathbb{N}$ by mapping an algebraic number α to (p_α, i), where p_α is a polynomial with α as a root (such a polynomial exists since α is algebraic), and α is the i-th smallest root of p_α.

This is injective since if $f(\alpha) = f(\beta) = (p, i)$ then α, β are both the i-th smallest root of p, and hence must be the same. ■

Note: *It is tempting to map each algebraic number α to just a polynomial with α as a root, but since polynomials have several roots this might not be injective. Hence we need the extra parameter that tells us which root it is.*

4.9 Probability

Problem 27. Ten balls numbered 1 to 6 are placed in a jar. Alice reaches into the jar and removes 2 balls (without replacement). What is the probability that the sum of the numbers on the two balls is even?

Solution:

There are 6 ways to have the sum be even: $\{1, 3\}, \{1, 5\}, \{2, 4\}, \{2, 6\}, \{3, 5\}$. Since of each of these can occur in two ways, there are 12 total ways to have the sum be even. There are $6 \cdot 5 = 30$ ways to draw 2 balls without replacement. So, the total probability is $\frac{12}{30} = \frac{2}{5}$. ■

Problem 28. Suppose a hundred people line up to board a plane. The first person to board the plan takes a random seat. After that, each person takes their assigned seat if it is unoccupied, or a random seat otherwise. What is the probability that the last person to board the plane gets their assigned seat?

Solution:

The probability is $\frac{1}{2}$. This is because when the last person boards, the only seats available are the first person's seat or their own seat. This is because if there was some other seat j available when the last person boarded, then person j would've taken that seat because it must have been available when they boarded. So, the probability that the last person takes their seat is the same as the probability that someone else takes the first person's seat. That is the same as the probability that the first person does not take their seat. ■

Problem 29. Consider a tournament with 64 teams and 6 rounds. You attempt to predict the winners for all 63 games and get the following points for each correct prediction: 32 for the final winner, 16 for each finalist, and so on, until 1 point for each winner in the first round. How many points can you expect to score if you decide to flip a fair coin for each of the 63 bets?

Solution:

Let X be the number of points you score. Let X_i be the number of points we get from a game at round i. There are 2^{5-i} games at round i and you can get 2^i points for correctly predicting the winner, where i ranges from 0 to 5. A team that plays a game at round i has played i games previously and is playing one now.

So, the probability that you predict this team's outcome correctly is $(\frac{1}{2})^{i+1}$ since the probability that you predict each game correctly is $\frac{1}{2}$. Thus, $\mathbb{E}[X_i] = \frac{2^i}{2^{i+1}} = \frac{1}{2}$ and you can expect to win $\frac{2^{5-i}}{2}$ points overall on round i. Therefore, $\mathbb{E}[X] = \sum_{i=0}^{5} 2^{5-i} * \frac{1}{2} = \frac{1}{2}\sum_{i=0}^{5} 2^i = \frac{2^6-1}{2} = \frac{63}{2}$. ■

Problem 30 (AIME 2007)**.** Let P be $\mathcal{P}([4])$ and consider two subsets A, B of $[4]$ that are chosen independently at random from P. What is the probability that B is a subset of at least one of A and $[4] \setminus A$?

Solution:

If B is a subset of at least one of A and $[4] \setminus A$, then B is either a subset of A or disjoint from A. Let E_1 be the event that $B \subseteq A$ and E_2 be the event that $B \cap A = \varnothing$. To compute $\mathbb{P}(E_1 \cup E_2)$, we will use the Principle of Inclusion-Exclusion.

Computing $\mathbb{P}(E_1)$:

We compute the number of ways that B is a subset of A by partitioning based on the size of A. For each size k from 0 to 4, there are $\binom{4}{k}$ possible ways to pick A. For each of these sizes, there are 2^k possible ways to pick B. So the total number of ways to pick A and B such that B is a subset of A is $\sum_{k=0}^{4}\binom{4}{k}2^k$. Using the binomial Theorem, this is $(2+1)^4 = 81$. There are $2^8 = 256$ possible pairs of subsets of $[4]$, so $\mathbb{P}(E_1) = \frac{81}{256}$

Computing $\mathbb{P}(E_2)$:

Similar to above, we again partition based on the size of A. After we pick the size-k subset to be A, we choose a subset of the remaining elements in $[4]$ to be B. There are 2^{4-k} such ways to do so. So, the total number of ways to pick B such that A and B are disjoint is $\sum_{k=0}^{4}\binom{4}{k}2^{4-k} = (2+1)^4 = 81$ by the Binomial Theorem and thus $\mathbb{P}(E_2) = \frac{81}{256}$

Computing $\mathbb{P}(E_1 \cap E_2)$:

The only way for A and B to be disjoint while $B \subseteq A$ is if $B = \varnothing$. In this case, there are 2^4 possibilities for A, so the $\mathbb{P}(E_1 \cap E_2) = \frac{16}{256}$.

Thus, $\mathbb{P}(E_1 \cup E_2) = \mathbb{P}(E_1) + \mathbb{P}(E_2) - \mathbb{P}(E_1 \cap E_2) = \frac{81+81-16}{256} = \frac{146}{256}$. ■

Problem 31. Three fair 6-sided dice are rolled. What is the probability that the sum of the three dice is 10, given that the three dice have different values?

Solution:

Let S be the event that the sum of the three dice is 10 and D be the event that the three dice have different

values. To compute $\mathbb{P}(S \mid D)$, we use the formula for conditional probability and compute $\frac{\mathbb{P}(S \cap D)}{\mathbb{P}(D)}$.

First, we compute $\mathbb{P}(D)$. There are $6^3 = 216$ possible outcomes for the values of the three dice and $\binom{6}{3}3! = 6 * 5 * 4 = 120$ possible outcomes where the three dice have different values. So, $\mathbb{P}(D) = \frac{120}{216}$

Then, we compute $\mathbb{P}(S \cap D)$. There are 3 possible sets of values of the three dice that result in a sum of 10 where the values are all different: $\{1, 3, 6\}, \{1, 4, 5\}$, and $\{2, 3, 5\}$. Each of these has 3! orderings. So, there are $3 * 3!$ outcomes where the sum of the dice is 10 and they have different values; thus, $\mathbb{P}(S \cap D) = \frac{18}{216}$ and $\mathbb{P}(S \mid D) = \frac{18}{210}$.

■

Problem 32. Mackey only gives two types of exams: hard or impossible. You will get an impossible exam with probability 0.8. The first question will be marked as difficult with probability 0.9 if the exam is impossible and probability 0.15 otherwise. What is your probability that your exam is impossible given that the first question is marked as difficult?

Solution:

Let D be the event that the first question is marked difficult, H be the event that the exam is hard, and I be the event that the exam is impossible. We want to find $\mathbb{P}(I \mid D)$.

We know that $\mathbb{P}(I) = 0.8$, $\mathbb{P}(D \mid I) = 0.9$ and $\mathbb{P}(D \mid H) = 0.15$. Since $\mathbb{P}(I) = 0.8$ and there are only two types of exams, $\mathbb{P}(H) = 0.2$.

Using Bayes' Theorem:

$$\begin{aligned}
\mathbb{P}(I \mid D) &= \frac{\mathbb{P}(D \mid I)\mathbb{P}(I)}{\mathbb{P}(D)} \\
&= \frac{\mathbb{P}(D \mid I)\mathbb{P}(I)}{\mathbb{P}(D \mid I)\mathbb{P}(I) + \mathbb{P}(D \mid H)\mathbb{P}(H)} \\
&= \frac{0.9 * 0.8}{0.9 * 0.8 + 0.15 * 0.2} \\
&= 0.96
\end{aligned}$$

So, the probability that the exam is impossible given that the first question is marked difficult is 0.96. Big RIP. ■

Problem 33. You distribute 25 apples over 10 boxes randomly. What is the expected number of boxes that will contain exactly 10 apples?

Solution:

Let X_k be 1 if the kth box has exactly 10 apples and 0 otherwise and let X be the number of boxes that contain exactly 10 apples. Then, $X = \sum_{k=1}^{10} X_k$.

The $\mathbb{E}[X_k] = \mathbb{P}(X_k = 1)$. We can think of X_k as a binomial variable with 25 trials (one for each apple) and the probability of success being $\frac{1}{10}$ (representing the apple going into the kth box). So $\mathbb{P}(X_k = 1) = \binom{25}{10}(\frac{1}{10})^{10}(\frac{9}{10})^{15}$.

So, $\mathbb{E}[X] = \sum_{i=1}^{10} \mathbb{E}[X_i] = 10\binom{25}{10}(\frac{1}{10})^{10}(\frac{9}{10})^{15}$.

■

Problem 34. Charlie has a fair 100-sided die and has nothing to do, so he decides to roll the die until he's seen all the numbers at least once. What is the expected number of times Charlie will have to roll the die?

Solution:

Let X be the total number of rolls to see each number at least once. Let X_n be the number of times Charlie has to roll the die after seeing $n-1$ distinct numbers in order to see the n-th new number.

Then, $X = \sum_{i=1}^{100} X_i$, so $\mathbb{E}[X] = \sum_{i=1}^{100} \mathbb{E}[X_i]$ by the linearity of expectation.

After $i-1$ numbers have been seen, there are $100-(i-1) = 101-i$ numbers left to be seen, each with an equal probability of showing up since the die is fair. So, X_i is a geometric random variable with probability of success $\frac{101-i}{100}$. Thus, $\mathbb{E}[X_i] = \frac{100}{101-i}$.

So, $\mathbb{E}[X] = \sum_{i=1}^{100} \frac{100}{101-i} = 100 \sum_{i=1}^{100} \frac{1}{i} \approx 519$. ■

Note: *This is a very straightforward variation of the coupon collector problem! If you had trouble with this problem, be sure to review that again.*