CS 70 Discrete Mathematics and Probability Theory
Spring 2026 Sinclair, Song

DIS 7A

Preparing For The Midterm

The midterm is soon! The goal of today is to allow you to practice the style of questions that will be asked on the midterm. The questions on this worksheet are most similar to the long-answer questions on the midterm. On the midterm, there will also be multiple choice and true/false questions.

Please refer to our post on Ed for all the midterm logistics.

And remember, it's important to come to the exam well rested. Make sure to get some sleep and relax before the midterm. Alongside this discussion, we're also offering support in office hours if you have any questions or concepts you'd like to clarify.

Best of luck! You've got this.

1 Induction

Note 3

Prove that $\forall n \in \mathbb{N}$, we have $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

Hint: You may use the fact that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. *You should not need to expand* $(n+1)^3$.

Solution: Base Case: For $n = 1$, $1^3 = 1 = (1)^2$
Induction Hypothesis: for an arbitrary k in $\mathbb{N}$, assume $\sum_{i=1}^{k} i^3 = (\frac{k(k+1)}{2})^2$ (using hint.)

Induction Step: Prove $\sum_{i=1}^{k+1} i^3 = (\frac{(k+1)(k+2)}{2})^2$ (again, using hint.)

$$\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 \\
&= \left(\sum_{i=1}^{k} i\right)^2 + (k+1)^3 \\
&= \left(\frac{k(k+1)}{2}\right)^2 + \frac{4(k+1)^3}{4} \\
&= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\
&= \frac{(k+1)^2(k^2 + (4(k+1)))}{4} \\
&= \frac{(k+1)^2(k+2)^2}{4} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2 \\
&= \left(\sum_{i=1}^{k+1} i\right)^2
\end{aligned}$$

2 Graph Proof

Note 5

Let $G = (V, E)$ be a disconnected graph with no self-loops. Prove that its complement $\overline{G} = (V, \overline{E})$ is connected. (Recall that the complement of a graph is defined such that for $u, v \in V$: $(u, v) \in E$ if and only if $(u, v) \notin \overline{E}$.)

Solution: Given distinct vertices $u, v \in \overline{G}$, we argue there is a path between u and v as follows.

- Case 1: If (u, v) is not an edge in G, then the vertices u, v are connected by an edge in $\overline{G}$.
- Case 2: If the vertices u, v are connected by an edge in G, then (u, v) lies in the same connected component. Pick another vertex w in another component which must exist as G is disconnected. Since the edges $(u, w), (w, v)$ are not in G, $(u, w), (w, v)$ are edges in $\overline{G}$, so there exists a path $u \to w \to v$.

Note: A common mistake is to assume that because G is disconnected, there is a vertex with 0 edges. This is not true—G being disconnected just means that there exists some vertices u, v that don't have a path between them. An example could be two copies of K_5.

3 Modular Arithmetic

Note 6

(a) Consider the equation $47a + 49b = 1$ for integers a and b. Find one solution (a, b).

(b) What is $2^{70} \pmod{67}$?

(c) Let p, q be distinct primes.

(i) Simplify $q^p \pmod{pq}$. *Hint: Use the Chinese Remainder Theorem.*

(ii) There are $pq - (_____)$ elements of $\{0, \ldots, pq-1\}$ that have inverses under arithmetic modulo pq.

Solution:

(a) One solution is $(a = 24, b = -23)$. One can run Extended Euclid's algorithm as follows:

$$49 = 1 \times \mathbf{49} + 0 \times \mathbf{47} \qquad (E_1)$$
$$47 = 0 \times \mathbf{49} + 1 \times \mathbf{47} \qquad (E_2)$$
$$2 = 1 \times \mathbf{49} + (-1) \times \mathbf{47} \qquad (E_3 = E_1 - 1 \times E_2)$$
$$1 = (-23) \times \mathbf{49} + (24) \times \mathbf{17} \qquad (E_4 = E_2 - 23 \times E_3)$$

Alternatively, notice that $(47 - 49) = -2$, so $23(47 - 49) = -46$. Thus, we add one more 47 to get 1.

(b) $16 \pmod{67}$. From FLT, $2^{70} = 2^{66} \cdot 2^4 = 1 \cdot 16 = 16 \pmod{67}$.

(c) (i) q. Using FLT, $q^p \equiv q \pmod{p}$ and because $q \equiv 0 \pmod{q}$, $q^p \equiv 0 \pmod{q}$. Thus, using CRT, we know there is one solution to this system (mod pq). Therefore, $q^p \equiv q \pmod{pq}$.

(ii) $(p + q) - 1$. We know that numbers that are not relatively prime to a mod p do not have an inverse $\pmod{p}$. Under (mod pq), since p and q are primes, we can see that multiples of p and q are not relatively prime to pq. Therefore, from the pq numbers in $0 \ldots pq - 1$, subtract the ones divisible by p or q. There are q multiples of p $(0, p, 2p, \ldots (q-1)p)$ and p multiples of q $(0, q, 2q, \ldots (p-1)q)$. Notice that because p and q are primes, their nonzero multiples do not overlap under pq. However, we need to add back 1 since 0 is divisible by both p and q and we overcounted by 1.

4 Polynomials

Note 8

(a) Working under GF(5), the degree 2 polynomial that passes through the points $(0,1)$, $(1,2)$, and $(2,0)$ can be written in the form ax^2+bx+c for some coefficients a, b, and c. What are the coefficients of this polynomial? (Hint: this might be easier with linear equations rather than Lagrange.)

(b) Suppose we have a degree 1 polynomial $P(x)$ in GF(5). The points $(0,1)$, $(1,3)$, $(2,1)$, and $(3,2)$ are received from a communication channel that has at most 1 corruption.

(i) What is $P(x)$?

(ii) What is the error polynomial, $E(x)$?

Solution:

(a) $x^2+1 \pmod 5$. Since the polynomial passes through $(0,1)$, we know that $c=1$. The other two equations give $a+b+1 \equiv 2 \pmod 5$ and $4a+2b+1 \equiv 0 \pmod 5$. Solving these equations, we have that $a=1$ and $b=0$.

(b) (i) $2x+1 \pmod 5$. We need to find a degree 1 polynomial passing through at least 3 out of the 4 points. Trying out a few subsets of points gives a solution of $2x+1 \pmod 5$, which passes through the first, second, and fourth points.

(ii) $x-2 \pmod 5$. The point $(2,1)$ is an error, and it corresponds to $x=2$. The correct point is $(2,5)$.

5 Secret Sharing

Note 8

The planning committee for The International Conference on Hackathon Organization has designed the following secret sharing scheme:

- 70 points of a 49-degree shared polynomial have each been assigned to the 70 delegations, one point per delegation.
- Each delegation contains 10 delegates.
- They each receive a point of a degree 5 delegation-specific polynomial.
- Delegates can come together to recover their delegation's point on the shared polynomial using the delegation-specific polynomial.

A *rogue delegate* is an all-powerful delegate: they know all of the polynomials and have control over which delegation that they are placed in. The rogue delegates purposely manipulate their point on their delegation-specific polynomial to mess up the conference.

The planning committee will use the Berlekamp-Welch algorithm on the delegation-specific polynomials and on the shared polynomial to attempt to recover the (stable) correct secret. What is the largest number of rogue delegates that can attend the conference such that the committee is guaranteed to recover the correct secret? Justify your answer.

Solution:

32 delegates.

For a degree 49 polynomial, 50 points must be received correctly, and thus 10 errors out of a total of 70 points can be tolerated (with k general errors, we need to send $n+2k$ points. $70 = 50+2*(10)$). Thus, the rogue delegates must create 11 corruptions on the shared polynomial in order to corrupt the secret.

For each delegation, 6 correct points are required, and thus 8 points need to be sent to counter 2 errors out of 10 points. Thus, only 3 rogue delegates are necessary to corrupt the secret.

Then, $3 \cdot 11 = 33$ rogue delegates are sufficient to corrupt the secret of the shared polynomial. Accordingly, the maximum number of rogue delegates that the committee can guard against is 32.