CS 70 Discrete Mathematics and Probability Theory
Fall 2025 Sabin, Hug

DIS 7A

Preparing For The Midterm

The midterm is tomorrow! The goal of today is to allow you to practise 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 tomorrow's 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 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 $(2,5)$.

3 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 u,v is connected by an edge in $\overline{G}$.
- Case 2: If u,v is 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 uw,wv are not in G, uw,wv 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.

4 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.

5 How Many Solutions?

Note 6

Consider the equation $ax \equiv b \pmod{p}$ for prime p. In the below three parts, all values a, b, x are defined as values in the range $\{0, 1, \ldots p-1\}$. In addition, include justification for your answers to all the subparts of this problem.

(a) For how many pairs (a, b) does the equation have a unique solution?

(b) For how many pairs (a, b) does the equation have no solution?

(c) For how many pairs (a, b) does the equation have p solutions?

Now, consider the equation $ax \equiv b \pmod{pq}$ for distinct primes p, q. In the below three parts, all values a, b, x are defined as values in in the range $\{0, 1, \ldots pq-1\}$.

(d) If $\gcd(a, pq) = p$, show that there exists a solution if and only if $b = 0 \pmod{p}$. (Hint: Try to relate modular equations to their corresponding algebraic equations, and vice versa.)

(e) If $\gcd(a, pq) = p$ and there is a solution x, show that there are exactly p solutions. (Hint: consider how you can generate another solution $x +$ ___)

(f) For how many pairs (a, b) are there exactly p solutions?

Solution:

(a) As long as a and p are coprime, then there is a unique solution $x = a^{-1}b \pmod{p}$. All $p-1$ values of a besides $a = 0$ are coprime to p, and any values of b will suffice. Thus, there are $(p-1)p$ pairs of values.

(b) If $a = 0$ but $b \neq 0$, then there are no solutions. There are $p-1$ such pairs.

(c) If $a = 0, b = 0$, then any value of x is a solution. Note that the previous two parts already used up $(p-1)p + (p-1) = p^2 - 1$ pairs, so there is only 1 pair left.

(d) First, note that $\gcd(a, pq) = p$ means that a is a nonzero multiple of p in $\pmod{pq}$.

Only if direction: The original equation tells us that $ax = b + kpq$, and we assume there is a solution x. If a is a multiple of p, then so is ax, and thus $b + kpq$ must be as well. In order for this to be true, b must therefore also be a multiple of p, and thus $b \mod p = 0$.

If direction: Assuming that both a, b are multiples of p, then we have the equation $\frac{a}{p}x = \frac{b}{p} + kq$. Looking at this equation in $\bmod q$ tells us that $\frac{a}{p}x \equiv \frac{b}{p} \pmod{q}$ which has a unique solution x as long as $\frac{a}{p}$ is coprime to q. We know this is satisfied, because $\frac{a}{p}$ can neither be 0 nor q, due to $a \neq 0 \pmod{pq}$.

(e) Note that any number of the form $x + iq \pmod{pq}$ for $i \in \{0, 1, \ldots, p-1\}$ will generate a different, valid solution. This is because $a(x+iq) = ax + aiq = ax + kipq = ax = b \pmod{pq}$. There are p possible values for i that give us unique numbers in $\pmod{pq}$.

Now, we will show that any other number cannot be a valid solution. If we consider other numbers of the form $x + z$ where $z \neq iq \pmod{pq}$, then notice that z is not a multiple of q, and a is also not a multiple of q, so az cannot be a multiple of q and therefore neither is a multiple of pq, and thus $az \neq 0 \pmod{pq}$. Then, $a(x+z) = ax + az = b + az \neq b \pmod{pq}$.

(f) Let's consider the cases. If a is a nonzero multiple of p (for which there are $q-1$ values), then the previous parts tell us that there are exactly p solutions iff $b = 0 \pmod{p}$ (for which there are q values). There are thus $q(q-1)$ pairs in this case.

If a is a nonzero multiple of q, then analogous reasoning tells us that there is a solution iff $b = 0 \pmod{q}$, and there will be q solutions, not p.

The only remaining case is that $a = 0$ (which is equivalent to saying that a is a multiple of both p and q). Then, if $b = 0$ then any value of x is a solution, and if $b \neq 0$ then there are no solutions.

Thus, only the first case yields any solutions, for which there are $q(q-1)$ such pairs.