Final Review: Practice Problems

Number Theory

Problem 1

In each of the following, find a value of $x$ that satisfies the given congruence, or argue that no such $x$ exists. Show how you found $x$.

a. $4(x - 3) \equiv 8x - 3 \pmod{41}$

b. $7(x + 5) \equiv 2x \pmod{13}$

Solution

a. $4(x - 3) \equiv 8x - 3 \pmod{41}$

\[ 4x - 12 \equiv 8x - 3 \pmod{41} \]

\[ 4x \equiv 8x + 9 \pmod{41} \]

\[ -4x \equiv 9 \pmod{41} \]

\[ 4x \equiv -9 \pmod{41} \]

\[ 4x \equiv 32 \pmod{41} \]

Now we know that 41 is prime. Hence, 4 has a multiplicative inverse. We use the tabular Euclidean Algorithm to find the gcd of 4, 41 to find the multiplicative inverse of 4 \pmod{41}.

\[
\begin{array}{c|cc|ccc}
  a & b & s & t & g \\
  \hline
  4 & 41 & -10 & 1 & 1 \\
  1 & 4 & 1 & 0 & 1 \\
  0 & 1 & 0 & 1 & 1 \\
\end{array}
\]

Thus, -10 is the multiplicative inverse of 4 \pmod{41}.

\[ x \equiv -320 \pmod{41} \]

Hence, $x = -320$ is a possible answer.
b. 7(x + 5) ≡ 2x (mod 13)

7x + 35 ≡ 2x (mod 13)

5x ≡ -35 (mod 13)

5x ≡ 4 (mod 13)

We know that 5 and 13 is prime. Hence, 5 and 13 are relatively prime, so 5 has a multiplicative inverse. We use the tabular Euclidean Algorithm to find the gcd of 5, 13 to find the multiplicative inverse of 5 (mod 13).

\[
\begin{array}{c|cccc}
 a & b & s & t & g \\
 5 & 13 & -5 & 2 & 1 \\
 3 & 5 & 2 & -1 & 1 \\
 2 & 3 & -1 & 1 & 1 \\
 1 & 2 & 1 & 0 & 1 \\
 0 & 1 & 0 & 1 & 1 \\
\end{array}
\]

Thus, -5 is the multiplicative inverse of 5 (mod 13).

\[x \equiv -20 \pmod{13}\]

Hence, \(x = -20\) is a possible answer.

---

**Problem 2**

The value of the *Euler ϕ function* at the positive integer \(n\) is defined to be the number of positive integers less than or equal to \(n\) that are relatively prime to \(n\).

a. Find the following values:

(i) \(ϕ(8)\)

(ii) \(ϕ(7)\)

(iii) \(ϕ(15)\)

b. Prove that \(n\) is composite iff \(ϕ(n) < n - 1\).

**Solution**

a. Find the following values:

(i) \(ϕ(8) = 4\), as 1, 3, 5, and 7 are smaller positive integers than 8 that are also relatively prime to 8
Never

(ii) $\phi(7) = 6$ because primes are relatively prime to all positive integers smaller than them.

(iii) $\phi(15) = \phi(3) \cdot \phi(5) = (3 - 1) \cdot (5 - 1) = 8$

b. In order to prove iff, we must prove both directions.

\[ n \text{ composite } \implies \phi(n) < n - 1 \]

$n$ composite means there is some $p \in \mathbb{Z} \; 1 < p < n$ such that $p \mid n$. As such, $\phi(n)$ is at most $n - 2$, which means that $\phi(n) < n - 1$

\[ n \text{ not composite } \implies \phi(n) \not< n - 1 \]

If $n$ is not composite, then $n$ is must be either 1 or a prime number.

If $n = 1$, then $\phi(n) = \phi(1) = 1 = n$, which means that $\phi(n) \not< n - 1$.

Similarly, if $n$ is a prime integer, then $\phi(n) = n - 1$, which means that $\phi(n) \not< n - 1$. In either case, the proof holds.

Conclusion: Since both directions hold, we have proven that $n$ is composite iff $\phi(n) < n - 1$.

Problem 3

Suppose $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Let $n \in \mathbb{Z}^+$. Prove the following statements:

a. $ac \equiv bd \pmod{m}$.

b. $a^n \equiv b^n \pmod{m}$.

\textbf{Hint:} Try induction on $n$.

Solution

a. \textbf{Claim:} $ac \equiv bd \pmod{m}$.

By the definition of mod, $\exists \; k, l \in \mathbb{Z}$ such that

\[ a = b + km \]
\[ c = d + lm \]

Multiplying these equations gives:

\[
\begin{align*}
ac &= (b + km)(d + lm) \\
ac &= bd + blm + kmd + klm^2 \\
ac &= bd + m(bl + kd + klm)
\end{align*}
\]

Notice that the second term on the RHS is divisible by \( m \). Therefore, we may rewrite the equation above in the form

\[ ac \equiv bd \pmod{m}. \]

b. **Claim:** \( \forall n \in \mathbb{Z}^+, a^n \equiv b^n \pmod{m} \).

We prove this by induction on the exponent, \( n \).

**Base Case:** \( n = 1 \). It is given that \( a \equiv b \pmod{m} \), and since \( x = x^1 \) for all integers, we can conclude that \( a^1 \equiv b^1 \pmod{n} \).

**Inductive Step:** Suppose \( a^k \equiv b^k \pmod{m} \) for some \( k \in \mathbb{Z}^+ \). We must now show that \( a^{k+1} \equiv b^{k+1} \pmod{m} \) holds. Note that we may rewrite \( a^{k+1} \) as \( a \cdot a^k \). Likewise, we may rewrite \( b^{k+1} \) as \( b \cdot b^k \). Using what we proved in part a (and substituting \( a^k \) for \( c \) and \( b^k \) for \( b \), we know that since \( a \equiv b \pmod{m} \) and \( a^k \equiv b^k \pmod{m} \), we can conclude that

\[ a \cdot a^k \equiv b \cdot b^k \pmod{m}. \]

It follows that

\[ a^{n+1} \equiv b^{n+1} \pmod{m} \]

as needed.

We have shown that the base case and the inductive step hold, so the claim holds for all \( n \in \mathbb{Z}^+ \).

**Counting**

**Problem 1**

Consider a finite set \( S \). Count the number of pairs of non-overlapping subsets, justifying your answer.
Note: The order in which you pick the pair does not matter.

Solution

Consider a subset $a \in S$ of size $|a| = k$, where $0 \leq k \leq n$. To pair this subset up with another subset such that they don’t overlap, the other subset must not contain any element $e \in s$. Hence, we can pair $a$ with any subset $b \subseteq \overline{a}$ such that $\forall e \in b, e \notin a$.

There are $\binom{n}{k}$ ways to pick a subset $a$ of size $k$. Since $b \in P(\overline{a})$, we find that there are $2^{n-k}$ ways to choose a subset $b$ to pair with $a$. Since $0 \leq k \leq n$, we conclude that there are

$$\sum_{k=0}^{n} 2^{n-k} \binom{n}{k}$$

ways to choose a valid pair $a$ and $b$.

Finally, since the order in which we pick the pair does not matter, we divide by $2! = 2$. Hence, the number of ways in which we can pick pairs of non-overlapping subsets of $S$ is given by

$$\sum_{k=0}^{n} 2^{n-k-1} \binom{n}{k}$$

Problem 2

Consider $n$ distinct objects. How many distinct sequences are there of these $n$ non-repeating items (any length)?

Solution

Consider a subset $s$ of these $n$ items of size $|s| = k$, where $0 \leq k \leq n$. There are $\binom{n}{k}$ ways to choose such a subset. Once this subset has been chosen, there are $k!$ ways to arrange them into a sequence. Hence, the number of distinct sequences of any length of these $n$ non-repeating items is

$$\sum_{k=0}^{n} k! \binom{n}{k}$$
Problem 3

How many different ways are there to list the numbers $1, 2, \ldots, 2n$ such that the even numbers appear in increasing order and the odd numbers appear in decreasing order?

Solution

There are $n$ even numbers and $n$ odd numbers. Considering these groups separately, there is only one way to order them in increasing and decreasing order, respectively.

Consider $2n$ spots in which we can put these numbers. There are $\binom{2n}{n}$ ways to choose $n$ of those spots to put the $n$ even numbers increasing order. The remaining $n$ spots are then filled with the $n$ odd numbers in decreasing order. Hence, we conclude that there are $\binom{2n}{n}$ ways to list the numbers $1, 2, \ldots, 2n$ such that the even numbers appear in increasing order and the odd numbers appear in decreasing order.

Probability

Problem 1

Consider a line of $n$ aliens at a spaceport looking to board a rocket containing $n$ free seats. Each of them has a ticket, and the $i^{th}$ alien is assigned to the $i^{th}$ seat.

The first alien in line enters the rocket, and instead of looking at its ticket for its assigned seat, sits uniformly at random. Every following alien that enters chooses its assigned seat if it is available, otherwise chooses one of the remaining seats uniformly at random. What is the probability that the $n^{th}$ alien sits down in its assigned seat?

Solution

Every alien either sits in its assigned seat or picks one of the remaining seats uniformly at random. Note that the $n^{th}$ alien sits down in whatever seat remains. Since the first alien picks uniformly at random regardless of circumstance, there is always at least one alien that picks a seat at random.

Let us consider the $i^{th}$ alien having to choose a seat out of the remaining seats
uniformly at random, where \(1 \leq i < n\). There are \(n - i + 1\) remaining seats. There are now three cases to consider.

1. If the \(i^{th}\) alien chooses any seat \(s\) where \(2 \leq s \leq n - 1\), then it displaces another alien in line. Thus, we return to these three cases recursively.

2. If the \(i^{th}\) alien chooses the first seat with probability \(\frac{1}{n-i+1}\), then the first alien and the \(i^{th}\) alien have essentially switched seats. Hence, no remaining alien in line is displaced, the shuffling terminates, and the \(n^{th}\) alien sits down in its assigned \(n^{th}\) seat.

3. If the \(i^{th}\) alien chooses the \(n^{th}\) seat with probability \(\frac{1}{n-i+1}\), then the \(n^{th}\) alien does not sit in its assigned seat and instead sits in the 1\(st\) seat.

Note here that we either return to the above three cases recursively through case (1), or we find two equally likely cases in which the \(n^{th}\) alien either sits down in the \(n^{th}\) seat or sits down in the 1\(st\) seat. Hence, we conclude that the \(n^{th}\) alien sits down the \(n^{th}\) seat with probability \(\frac{1}{2}\).

Problem 2

You have 100 coins on a table. 99 of them are fair and 1 of them has H on both sides.

a. You choose a coin uniformly at random, and flip it. Let \(X\) be a random variable where \(X = 1\) if you get heads, and \(X = 0\) if you get tails. What is \(E[X]\)?

b. You choose a coin again uniformly at random, flip it, record the result, and put the coin back. You repeat this experiment 9 more times (for a total of 10). Let \(X\) be a random variable denoting the total number of heads you get. What is \(E[X]\)?

c. You choose a coin again uniformly at random, but flip this same coin 10 times. If you get heads every time, what is the probability you will also get heads the 11th time?

Solution

a. The probability we get heads is \(Pr(H|\text{fair coin})Pr(\text{fair coin}) + Pr(H|\text{biased coin})Pr(\text{biased coin})\).

- \(Pr(H|\text{fair coin}) = \frac{1}{2}\)
Never

- \( Pr(\text{fair coin}) = \frac{99}{100} \)
- \( Pr(H|\text{biased coin}) = 1 \)
- \( Pr(\text{biased coin}) = \frac{1}{100} \)

The total probability is 0.505.

b. Let \( X_i \) be a random variable that is 1 if the \( i \)-th flip is heads, and 0 otherwise.
\[
X = \sum_{i=1}^{10} X_i.
\]

By the linearity of expectation, \( E[X] = \sum_{i=1}^{10} E[X_i] \). From part a, each \( E[X_i] = 0.505 \). So, \( E[X] = 5.05 \).

c. We want to find \( Pr(H\text{ 11th time}|10\text{ H}) \). This can be expanded into two cases: whether the coin we picked is a fair coin or the biased coin. We also have to factor in the probability of the coin being fair or unfair based on the fact that we’ve just gotten 10 heads in a row. So, we are looking for:

\[
P(H \text{ 11th time}|\text{fair coin})P(\text{fair coin}|10\text{ H}) + P(H \text{ 11th time}|\text{unfair coin})P(\text{unfair coin}|10\text{ H})
\]

Using Bayes’ Theorem, we can calculate each component:

\[
= .5 \times \frac{P(10\text{ H}|\text{fair coin})P(\text{fair coin})}{P(10\text{ H})} + 1 \times \frac{P(10\text{ H}|\text{biased coin})P(\text{biased coin})}{P(10\text{ H})}
\]

\[
= \frac{.5 \times .5^{10} \times .99 + 1 \times 1 \times .01}{.5^{11} \times .99 + .01} = \frac{.5^{11} \times .99 + .01}{.5^{10} \times .99 + .01} = 0.956
\]

Graph Theory

Problem 1

Show that, in any graph \( G \), if there is a vertex \( v \) of odd degree, then there is a path from \( v \) to some other vertex of odd degree.
Solution

Recall from lecture that because vertices share edges, the sum of the degrees in a graph must be equal to $2|E|$. Hence, we know that if there is one vertex of odd degree, there must be at least one other.

We can construct a path starting at one of the odd-degree vertices $v$ in the following manner: follow any edge from $v$. There are now an even number of unexplored edges incident to $v$. Continue following unexplored edges in this way. For each vertex we visit, there are two cases.

1. The vertex is an odd-degree vertex, as needed, and we are done.

2. The vertex is an even-degree vertex (or our original vertex). We use two edges to enter and leave the vertex, meaning this leaves this vertex with an even number of unexplored edges.

Because we cannot enter an even-degree vertex and not have another edge upon which to leave, we must eventually reach a vertex of odd degree.

Thus, there is always a path between odd-degree vertices in a simple graph if it has an odd-degree vertex.

Problem 2

Prove that by joining together any $n \geq 2$ connected graphs that have connected Eulerian tours the resulting graph will also have a Eulerian tour. In this problem, we define joining as merging any two vertices together into a single new vertex, as depicted in the image below:

![Graph Image]

Solution

We prove this problem by using build-down induction.
**Proof. Proposition:** Let \( P(n) \) be the predicate that joining any \( n \) connected graphs each with a connected Eulerian tour results in a new graph with a Eulerian tour, for \( n \geq 2 \).

**Base Case:** Consider the case \( n = 2 \).

Let \( n = 2 \). Suppose the two Euler tours are connected at a vertex \( u \). Let \( v \) be a vertex on one of the Euler tours. Traverse that tour until the point of connection \( u \). The second Euler tour is a tour from \( u \) that loops back to \( u \), so follow that tour back to \( u \). Then resume following the original Euler tour back to \( v \).

Since no other edges are introduced, this construction traverses all edges in the merged graph. Hence, it is a Eulerian tour and \( P(2) \) holds.

**Inductive Hypothesis:** Assume \( P(k) \) is true for \( n = k \).

**Inductive Step:**

We want to show \( P(k+1) \) is true, ie. that a graph resulting from connecting \( k + 1 \) connected graphs with a Eulerian tour has an Eulerian tour.

Consider \( k + 1 \) connected graphs with a Eulerian tour. Take \( k \) of these \( k + 1 \) graphs and connect them. By the inductive hypothesis, the result is a graph \( G_k \) with a Eulerian tour. Then we have two Eulerian tours — the tour in \( G_k \) and the \((k+1)th\) unmerged graph. These tours can be connected as explained in the second base case, so \( P(k + 1) \) holds if \( P(k) \) holds.

**Conclusion:** We have shown that \( P(2) \) is true, and that if \( P(k) \) is true then so is \( P(k+1) \). Hence, \( P(n) \) is true for all \( n \geq 2 \) by the principle of induction.

---

**Problem 3**

Pluto spotted this proof of the ‘Graph Pigeonhole Principle.’

**Claim:** For \( n \geq 4 \), if an \( n \) vertex graph has at least \( n + 1 \) edges, it must contain a subgraph that is a triangle (a simple cycle of length 3).

**Proof:**

Define \( P(n) \): For every graph on \( n \) vertices, if the graph has at least \( n + 1 \) edges, it contains a subgraph that is a triangle.

Consider the base case \( P(4) \). The complete graph \( K_4 \) has 6 edges and vertices \( \{v_1, v_2, v_3, v_4\} \). We’re interested in a graph on these vertices with at least \( n + 1 = 5 \)
edges. If the graph has 6 edges, it is a complete graph and any 3 of its vertices forms a triangle. If it has 5 edges, we can assume without loss of generality that the missing edge is \((v_1, v_2)\). The edges \(\{v_1, v_3\}\), \(\{v_3, v_4\}\), and \(\{v_1, v_4\}\) are in the graph and form a triangle. Hence, \(P(4)\) is true, which proves our base case.

Assume that \(P(k)\) is true for \(n = k\). For the inductive step, consider a graph \(G\) with \(k\) vertices and at least \(k + 1\) edges. By our inductive hypothesis, \(G\) contains a triangle. Construct an \(k + 1\) vertex graph \(G'\) by adding one vertex to \(G\) and at least one edge (so the number of edges is at least \(k + 2\)). By the inductive hypothesis, \(G\) contains a triangle. Since \(G\) is a subgraph of \(G'\), \(G'\) also contains a triangle. Hence, if \(P(k)\) is true, so is \(P(k + 1)\).

We have shown that \(P(4)\) holds and that if \(P(k)\) holds so does \(P(k + 1)\). Thus, we have shown that \(P(n)\) holds for all \(n \geq 4\) by the principle of induction. QED.

a. Prove that Pluto’s Graph Pigeonhole Principle is false.

b. What’s wrong with Pluto’s proof?

c. Repair the proof by showing that a simple graph with \(n\) vertices where the minimum degree is more than \(n/2\) must contain a triangle.

   **Hint:** Pigeonhole Principle!

---

**Solution**

a. A counterexample suffices to disprove the claim. For example: the cyclic graph \(C_6\) with an added ‘midline’ connecting one vertex to the vertex on the opposite side of the cycle.

b. It showed that if we build graphs with \(n + 1\) vertices and \(n + 2\) edges out of graphs with \(n\) vertices and \(n + 1\) edges, this property persists. But some graphs of \(n + 1\) vertices and \(n\) edges cannot be built that way. Thus, it does not generalize and the induction did not build-down as required. Hence why we were able to come up with the counterexample from part (a). This counterexample is a graph with 6 nodes and 7 edges. But any vertex we remove from this graph will remove at least 2 edges, so the resulting graph will have 5 nodes and no more than 5 edges.

c. This is a form of Mantel’s Theorem. Let us demonstrate this theorem by direct proof using the Pigeonhole Principle.

Consider a graph \(G\) with \(n\) vertices where the minimum degree more than \(\frac{n}{2}\). Without loss of generality, number these vertices 1 to \(n\) and consider the vertex \(v_1, v_2\) where \((v_1, v_2) \in E(G)\). We know this to be possible since there is at least one edge in \(G\).
We know that \( v_1 \) and \( v_2 \) must be connected to at least half of the other vertices in the graph. There are two cases to consider.

1. If \( n \) is even, then the graph \( G \) has a minimum degree of at least \( \frac{n}{2} + 1 \).
   Since \( (v_1, v_2) \in E(G) \) then \( v_1 \) has an edge to at least \( \frac{n}{2} + 1 - 1 = \frac{n}{2} \) of the other vertices \( \{v_3, \ldots, v_n\} \). The same is true for \( v_2 \).
   Therefore, there are a total \( 2 \left( \frac{n}{2} \right) = n \) edges from \( \{v_1, v_2\} \) to \( \{v_3, \ldots, v_n\} \).
   Now there are \( n - 2 \) vertices in the set \( \{v_3, \ldots, v_n\} \). Therefore, by the Pigeonhole Principle there is at least one \( v \in \{v_3, \ldots, v_n\} \) such that there exists two edges from \( \{v_1, v_2\} \) to \( v \). Since we are considering simple graphs, this means that \( (v_1, v), (v_2, v) \in E(G) \). Since \( (v_1, v_2) \in E(G) \), we have a triangle within the set of vertices \( \{v_1, v_2, v\} \).

2. If \( n \) is odd, then the graph \( G \) has a minimum degree of at least \( \lceil \frac{n}{2} \rceil \).
   Since \( (v_1, v_2) \in E(G) \) then \( v_1 \) has an edge to at least \( \frac{n}{2} + 1 - 1 = \frac{n}{2} \) of the other vertices \( \{v_3, \ldots, v_n\} \). The same is true for \( v_2 \).
   Therefore, there are a total \( 2 \left\lceil \frac{n}{2} \right\rceil = n + 1 \) edges from \( \{v_1, v_2\} \) to \( \{v_3, \ldots, v_n\} \).
   Now there are \( n - 2 \) vertices in the set \( \{v_3, \ldots, v_n\} \). Therefore, by the Pigeonhole Principle there is at least one \( v \in \{v_3, \ldots, v_n\} \) such that there exists two edges from \( \{v_1, v_2\} \) to \( v \). Since we are considering simple graphs, this means that \( (v_1, v), (v_2, v) \in E(G) \). Since \( (v_1, v_2) \in E(G) \), we have a triangle within the set of vertices \( \{v_1, v_2, v\} \).

We have shown that in both cases there exists a triangle in the graph \( G \). Hence, a simple graph with \( n \) vertices where the minimum degree is more than \( n/2 \) must contain a triangle.