Quick Solution to Practice Problems 2

ALL of the following problems:

1. **Base case:** For \( n = 1 \) it’s true because 5 divides \( 15^1 - 1 = 0 \).

   **Inductive step:** Assume that 5 divides \( n^5 - n \). We will prove that 5 divides \((n+1)^5 -(n+1)\).

   We note that
   \[
   (n + 1)^5 - (n + 1) = n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1
   = (n^5 - n) + 5(n^4 + 2n^3 + 2n^2 + n)
   \]

   Since 5 divides \( n^5 - n \) by the inductive hypothesis, and 5 divides \( 5(n^4 + 2n^3 + 2n^2 + n) \),

   5 divides the sum. Therefore 5 divides \((n+1)^5 -(n+1)\).

   Therefore the statement is true for any natural number \( n \) from the principle of induction.

2. Let \( a_1a_2a_3\ldots a_b \) be the secret, where \( a_i \) are bits and \( a_1\ldots a_b \) denotes the number represented by the bit-string. Using Lagrange interpolation we find a polynomial on \( GF(p) \) of degree \( k - 1 \) for which:

   \[
   P(1) = \overline{a_1a_2\ldots a_{\lfloor b/k \rfloor}}
   P(2) = \overline{a_{\lfloor b/k \rfloor + 1} \ldots a_{2\lfloor b/k \rfloor}}
   \ldots = \ldots
   P(k) = \overline{a_{(k-1)\lfloor b/k \rfloor + 1} \ldots a_b}
   \]

   Then we give \( P(k+i) \) to person \( i \) for \( i = 1, 2, \ldots n \). If any \( k \) people get together they can reconstruct the polynomial and the whole secret, since \( k \) points completely determine a polynomial of degree \( k - 1 \).

   Any \( k - 1 \) people won’t be able to reconstruct any chunk of the secret, and in particular the first \( \lfloor b/k \rfloor \) bits. This is true because for any value of the first \( \lfloor b/k \rfloor \) bits \( c_1, c_2, \ldots c_{\lfloor b/k \rfloor} \), there exists a polynomial \( Q \) with \( Q(1) = \overline{c_1c_2\ldots c_{\lfloor b/k \rfloor}} \) and the \( k - 1 \) values of the present people.

   The size of the field \( p \) has to be such that most of its elements are written using \( \lceil b/k \rceil \) bits. So choose a prime \( p \) such that \( 2^{\lceil b/k \rceil - 1} < p < 2^{\lfloor b/k \rfloor} \).

   Also, to be sure no-one can individually retrieve \( P(1), p \) must be chosen so that it’s strictly greater than \( n + k \).

ALL of the following problems:

1. Suppose there is no Hamiltonian cycle. Add edges to the graph until we are one edge away from having a Hamiltonian cycle, that is, until there is an edge we can add next that would cause a cycle. That edge will be connecting some vertices \( v_1 \), and \( v_n \) that are the ends of a Hamiltonian path \( v_1, v_2, \ldots v_n \). The degrees of all vertices are still > \( n/2 \). Let \( S \) be the set of vertices \( v_i \) such that \( v_{i+1} \) is a neighbor of \( v_i \) (i.e. the edge \((v_1, v_{i+1}) \) is in the graph) for \( i = 1, 2, \ldots n - 1 \). The size of \( -S \) — is larger than \( n/2 \) since the degree of \( v_1 \) is larger than \( n/2 \). Let \( T \) be the set of neighbors of \( v_n \). The size of \( T \) is also larger than \( n/2 \) since the degree of \( v_n \) is also larger than \( n/2 \). \( S \) and \( T \) are both subsets of \( \{v_2, v_3, \ldots v_{n-1}\} \), which is of size \( n - 2 \). Therefore there is at least one vertex that is both in \( S \) and \( T \). Let that vertex be \( v_k \). By the definitions of \( S \) and \( T \),
(v_k, v_n) is an edge, and (v_1, v_{k+1}) is an edge. However, this implies that the following is a Hamiltonian cycle: (v_1, v_{k+1}, v_{k+2}, \ldots v_n, v_k, v_{k-1}, v_{k-2}, \ldots v_1). This is a contradiction since we stopped adding edges before a Hamiltonian cycle appeared. Therefore our initial assumption was false, and the original graph necessarily had a Hamiltonian cycle.

2. (a) \(2k\)
   (b) \(n!/(n-k)! \cdot 2k\)
   (c) Using method of indicator, let \(I_i\) to be a random variable that is one only when the \(i\)th \(k\)-cycle is in \(G\). Hence, \(E(I_i) = P(I_i = 1) = p^k\)

   Then, \(E(N) = \sum_i E(I_i) = X \cdot p^k\), which \(X\) is the answer to part b.

The following problem:

1. We count the number of ways to split \(n\) elements into 3 labeled groups by two different methods.

   - There are 3 different choices for each element, so \(3^n\) for all of them.
   - For every \(i\) from 0 to \(n\), choose \(i\) elements to go in group A, then for every \(j\) from 0 to \(n - i\) choose \(j\) elements to go in group B, the remaining go in group C. This gives:

\[
\sum_{i=0}^{n} \binom{n}{i} \sum_{j=1}^{n-i} \binom{n-i}{j}
\]

At least two of the following problems:

1. (a) \(\{1, 2, 3, 4\} \times \{H, TH, TTH, \ldots\}\)

\[
\sum_{i=1}^{4} \sum_{n=0}^{\infty} \frac{1}{4^i} \cdot \frac{1}{i} \cdot \frac{i-1^n}{i}
\]

Working on the algebra, you’ll get 1.

(b) \(Pr(H_2) = Pr(H_2 \cap C_1) + Pr(H_2 \cap C_2) + Pr(H_2 \cap C_3) + Pr(H_2 \cap C_4)\)

\[= \frac{95}{576}\]

(c) Use the definition of conditional probability and the solution to part b to get \(Pr(C_i \mid H_2)\).

2. \(\frac{k^m}{N} - \frac{k-1^m}{N}\)

3. There’re different ways to interpret this problem which each can be correct. The probability my friend received my letter is \(m - 1/m\), and since I didn’t get any reply, it was probably lost, so \(1/m\). Hence, the desired probability is \((m - 1)/m^2\).

At least two of the following problems:
1. This seems to contradict Markov’s Inequality. It does not. We can use a random variable which can have negative values. In this case, we have \( \Pr(X = 1) = \frac{2}{3} \), and we need another value \( a \) such that \( \Pr(X = a) = \frac{1}{3} \) and \( 1 \cdot \frac{2}{3} + a \cdot \frac{1}{3} = \frac{1}{2} \). Solving that equation, we get that \( a = -\frac{1}{2} \).

2. (a) Define \( I_i = 1 \), if \( i \)th student get his own cell phone.
   
   \[
   E[I_i] = P(I_i = 1) = \frac{1}{n}
   \]
   
   \[E[N] = \sum_i E[I_i] = n \cdot \frac{1}{n} = 1\]
   
   (b) Define \( I_{ij} = 1 \) (given \( i < j \)), if \( i \)th and \( j \)th students will need to swap cell phones.
   
   \[
   E[I_{ij}] = P(I_{ij} = 1) = \frac{n(n-1)}{n(n-1)} = \frac{1}{2}
   \]
   
   \[E[N] = \sum_{i,j} E[I_{ij}] = \frac{n!}{(n-1)!} \cdot \frac{(n-2)!}{n!} = 1/k\]
   
   Remember that the number of different configurations for \( k \) objects on a circle is \((k-1)! \) not \( k! \). ( \( (k-1)! = k!/k \) )

   (c) Define \( I_{i_1,i_2,...,i_k} = 1 \), if the \( k \)-tuple satisfy the property.
   
   \[
   E[I_{i_1,i_2,...,i_k}] = P(I_{i_1,i_2,...,i_k} = 1) = \frac{(n-k)!}{n!} \cdot \frac{n!}{n!} = 1/k
   \]

   (d) \( E[N] = \sum_{k=1}^{n} E[N_k] = \sum_{k=1}^{n} 1/k\)

3. Eliminated!

**The following problem:**

1. The covariance, \( \text{Cov}(X, Y) \), of two random variables, \( X \) and \( Y \), is defined to be \( E(XY) - E(X)E(Y) \). Note that if two random variables are independent, then their covariance is zero.

   (a) Let \( (X, Y) \) have joint probability given as:
   
   \[
   \Pr(X = -1 \cap Y = 1) = \frac{1}{3}
   \]
   \[
   \Pr(X = 0 \cap Y = 0) = \frac{1}{3}
   \]
   \[
   \Pr(X = 1 \cap Y = 1) = \frac{1}{3}
   \]
   
   Note that \( X \) and \( Y \) are not independent since: \( \Pr(X = 1 \cap Y = 1) = \frac{1}{3} \neq \frac{2}{9} = \Pr(X = 1) \Pr(Y = 1) = \frac{1}{3} \)
   
   But \( \text{Cov}(X, Y) = 0 \).

   (b)
   
   \[
   \text{Var}(X_1 + \ldots + X_n) = E[(X_1 + \ldots + X_n)^2] - (E[X_1] + \ldots + E[X_n])^2
   \]
   
   \[
   = E[\sum_i X_i^2 + \sum_{i<j} 2X_iX_j] - [E[X_1]^2 + \ldots + E[X_n]^2 + \sum_{i<j} 2E[X_i]E[X_j]]
   \]
   
   \[
   = \sum_{i=1}^{n} \text{Var}(X_i) + 2 \sum_{i<j} \text{Cov}(X_i, X_j)
   \]