1. Answer each problem below briefly. (4 points each)
Suffice it to write down the solutions; no computations are required.

(a) (**4 points**) Given the premises
$\forall x \forall y (P(x,y) \rightarrow Q(x,y))$
$\forall x \forall y \forall z (P(x,y) \wedge Q(y,z) \rightarrow Q(x,z))$
What is the *weakest* condition for $Q(a,b)$ to be true? That is, write down the *weakest* formula F $(\neq Q(a,b))$ such that $F \rightarrow Q(a,b)$ is a logical consequence of the premises.

(b) (**4 points**) For each pair of sets below, determine if $|A| < |B|, |A| = |B|,$ or $|A| > |B|$
(N.B. $\mathbf{N}$ is the set of natural numbers.)
1) $A =$ The set of all computable functions from $\mathbf{N}$ to $\mathbf{N}$.
$B =$ The set of all uncomputable functions from $\mathbf{N}$ to $\mathbf{N}$.
2) $A =$ The set of all C++ programs that terminate.
$B =$ The set of all C++ programs that don't terminate

(c) (**4 points**) Consider the following primality testing algorithm based on Fermat's little theorem

function FermatPrimalityTest(n,k)
for $i = 1$ **to** k **do**
generate an integer b in the interval $(1, n-1]$ uniformly at random
if $b^{n-1} \not\equiv 1 \pmod{n}$ **then return** $false$
return $true$

Given the smallest Carmichael number $561 = 3 \cdot 11 \cdot 17$, what is the probability that the call FermatPrimalityTest(561,1) returns $true$?

(d) (**4 points**) Find all solutions, if any, to the system of congruences.
$2x \equiv 4 \pmod{8}$
$x \equiv 6 \pmod{9}$

2. (a) (**4 points**) Give a recursive definition of the set S of odd integers.

(b) (**5 points**) Prove by induction that for all $n \in \mathbf{Z}$, $2n+1 \in S$, where $\mathbf{Z}$ is the set of integers.

3. In the following questions, just give the answer, do not give any explanation.

(a) (**3 points**) A computer randomly prints three-digit codes, with no repeated digits in any code (for example, 387, 072, 760). What is the minimum number of codes that must be printed in order to guarantee that at least five of the codes are identical?

(b) (**3 points**) What is the largest value of n for which K_n (a complete graph on n vertices) is planar?

(c) (**3 points**) If the permutations of 1,2,3,4,5,6 are written in lexicographic order, with 123456 in position #1, 123465 in position #2, etc., find the permutation in position #484.

4. In the following questions, just give the answer, do not give any explanation.

   (a) (**4 points**) a_n = the number of bit strings of length n with an even number of 0s. Describe the sequence recursively. Include initial condition and assume that the sequence begins with a_1.

   (b) (**4 points**) Find the number of ways in which nine identical blocks can be given to four children, if the oldest child gets at most three blocks.

   (c) (**4 points**) Suppose A is a set with n symbols, |A| = n. Find the number of symmetric binary relations on A.

   (d) (**4 points**) How many non-isomorphic simple undirected graphs with 5 vertices and 3 edges?

5. Let $\mathbf{A}$ be an $m \times n$ matrix, $\mathbf{x} \in \mathcal{R}^n$ denote a vector, and $L(\mathbf{x}) = \mathbf{Ax}$ be a linear transformation. $\mathbf{row(A)}$, $\mathbf{col(A)}$, and $\mathbf{N(A)}$ respectively represent the row space, the column space, and the null space of $\mathbf{A}$. $\mathbf{rank(A)}$ and $\mathbf{nullity(A)}$ respectively represent the rank and nullity of $\mathbf{A}$. $\mathbf{kernel}(L)$ and $\mathbf{range}(L)$ respectively represent the kernel and the range of L. If V is a vector space/subspace, $\mathbf{dim}(V)$ denotes the dimension of V. Consider the following statements:

   (A) $\mathbf{row(A)} = \mathcal{R}^n$.
   (B) $\mathbf{col(A)} = \mathcal{R}^m$.
   (C) $\mathbf{dim}(\mathbf{col(A)}) < m$.
   (D) $\mathbf{Ax} = \mathbf{0}$ has infinite solutions.
   (E) $\mathbf{Ax} = \mathbf{0}$ has exactly one solution.
   (F) $\mathbf{Ax} = \mathbf{0}$ has no solutions.
   (G) $\mathbf{Ax} = \mathbf{0}$ is an inconsistent system.
   (H) $\mathbf{Ax} = \mathbf{0}$ is a consistent system.
   (I) $\mathbf{N(A)} = \emptyset$.
   (J) $\mathbf{rank(A)} = m$.
   (K) $\mathbf{nullity(A)} = m$.
   (L) $\mathbf{kernel}(L) = \mathcal{R}^n$.
   (M) $\mathbf{range}(L) \subseteq \mathcal{R}^m$.
   (N) $\mathbf{AA}^T$ is not symmetric.

   (a) (**2 points**) Which statements are always false?

   (b) (**2 points**) Which statements are always true?

   (c) (**2 points**) Which statements are equivalent to the statement (B)?

   (d) (**2 points**) What does the statement (L) imply about L?

6. (**5 points**) Assume $\mathbf{A}$, $\mathbf{B}$, and $\mathbf{C}$ are respectively $m \times p$, $p \times q$, and $q \times n$ matrices, and $\mathbf{M} = \mathbf{ABC}$. Let $\mathbf{M}^{kl} = \boldsymbol{a}_k \boldsymbol{c}^l$ for $1 \le k \le p$ and $1 \le l \le q$, here $\boldsymbol{a}_k$ and $\boldsymbol{c}^l$ respectively denote the k-th column vector of $\mathbf{A}$ and the l-th row vector of $\mathbf{C}$. Prove that $\mathbf{M} = \sum_{k=1}^{p} \sum_{l=1}^{q} b_{kl} \mathbf{M}^{kl}$.

7. Let $L:\mathcal{R}^2 \to \mathcal{R}^3$ be a linear transformation. Assume $L\left(\begin{bmatrix}1\\2\end{bmatrix}\right) = \begin{bmatrix}3\\0\\1\end{bmatrix}$ and $L\left(\begin{bmatrix}2\\3\end{bmatrix}\right) = \begin{bmatrix}5\\1\\3\end{bmatrix}$. In addition, $B_1 = \left\{\begin{bmatrix}1\\2\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}\right\}$ is an ordered basis of $\mathcal{R}^2$, and $B_2 = \left\{\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}\right\}$ and $B_3 = \left\{\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}5\\1\\3\end{bmatrix}, \begin{bmatrix}3\\0\\1\end{bmatrix}\right\}$ are ordered bases of $\mathcal{R}^3$.

   (a) (**4 points**) Find the matrix representation of L with respect to the bases B_1 and B_3.

   (b) (**4 points**) Find the (coordinate) transition matrix from the basis B_2 to the basis B_3.

   (c) (**4 points**) Solve $L\left(\begin{bmatrix}1\\0\end{bmatrix}\right)$ and $L\left(\begin{bmatrix}0\\1\end{bmatrix}\right)$.

8. (**10 points**) If $\mathbf{A}$ is a real symmetric matrix, find a matrix $\mathbf{V}$ such that $\mathbf{VAV}^{\mathrm{T}} = \mathbf{I}$. You need to prove your answer is correct.

9. The inner product of the vector space C[-1,1] is defined as $< f, g >= \int_{-1}^{1} f(x)g(x)dx$.

   (a) (**9 points**) Find an orthonormal basis for the subspace spanned by 1, x, and x^2.

   (b) (**6 points**) Find the best quadratic least squares approximation to e^x on [-1,1].