1. **Short Questions: 2/2/2/2/2 Provide a clear and concise justification of your answer.**

   In this problem, you roll two balanced six-sided dice. *Hint: Draw a picture.*

   1. What is the probability that the number of pips (dots) on the second die is equal to the number on the first?

      There are six such outcomes: $(1,1),\ldots,(6,6)$. Hence, the probability is $6/36 = 1/6$.

   2. What is the probability that the number of pips (dots) on the second die is strictly larger than the number on the first?

      In view of the previous problem, the numbers are different with probability $5/6$. The number on the second is strictly larger that on the first with probability $(1/2)(5/6) = 5/12$.

   3. What is the probability that the first die yields a value less than or equal to 2 given that the sum of the two values is strictly larger than 5? Let A be the event that the first die yields a value 1 or 2 and B the event that the sum of the two values is strictly larger than 5. Then, looking at our picture, we find that $Pr[A \cap B] = 5/36$ and $Pr[B] = 26/36$. Consequently, $Pr[A|B] = Pr[A \cap B]/Pr[B] = 5/26$.

   4. What is the probability that the two values differ by 4 or more in absolute value? There are only six outcomes (a,b) that satisfy that condition: $\{(1,5),(1,6),(2,6),(6,2),(6,1),(5,1)\}$. Consequently, the probability of that event is $6/36 = 1/6$.

   5. What is the probability that the maximum of the two values is 5 or 6? The outcomes in that event are (a,b) where $a \in \{5,6\}$ or $b \in \{5,6\}$. Let A be the first set and B the second. Then $|A \cap B| = |A| + |B| - |A \cap B| = 12 + 12 - 4 = 20$. (You can also look at the picture and count.) Hence, the probability of that event is $20/36 = 5/9$.

2. **Short Questions: 3/3/3/3/3/3/3 Provide a clear and concise justification of your answer.**

   In this problem, there is a probability space with sample space Ω.

   1. True or False (and justification): Two disjoint events A and B with $Pr[A] > 0$ and $Pr[B] > 0$ cannot be independent.

      True: If they are independent, then $Pr[A \cap B] = Pr[A]Pr[B]$, so that $0 = Pr[A]Pr[B]$, a contradiction.

   2. True or False (and justification): Let $\{A_1,\ldots,A_N\}$ be a partition of Ω. That is, the events $\{A_1,\ldots,A_N\}$ are pairwise disjoint and their union is Ω. Let also B and C be two other events. If $Pr[B|A_n] > Pr[C|A_n]$, then it must be that $Pr[A_n|B] > Pr[A_n|C]$.

      False: For instance, consider the case where $Pr[C|A_m] = 0$ for $m \neq n$. Then $Pr[A_n|C] = 1$ and one can certainly choose the model so that $Pr[A_n|B] < 1$.

   3. True or False (and justification): If A and B are positively correlated and so are B and C, then A and C are necessarily positively correlated. (Recall that, by definition, two events A and B are positively correlated if $Pr[A \cap B] > Pr[A]Pr[B]$.)

      False: Let $\Omega = \{a,b,c,d,e,f\}$ be uniform and $A = \{a,b\}, B = \{b,c\}, C = \{c,d\}$, In this case, A and B are positively correlated since $Pr[A \cap B] = 1/6 > Pr[A]Pr[B] = 1/9$. Similarly, B and C are positively correlated. However, A and C are negatively correlated since they are disjoint.

   4. There is a bag with 50 red and 50 blue balls. You pick four balls, without replacement. Given that the first ball is red, what is the probability that the fourth ball is also red?

      By symmetry, this probability is the same as for the second ball. Thus, it is $49/99$.

   5. True or False (and justification): For any event A, the events A and Ω are independent.

      True. $Pr[A \cap \Omega] = Pr[A]Pr[\Omega]$ since $A \cap \Omega = A$ and $Pr[\Omega] = 1$.

6. True or False (and justification): If the events A, B, C are such that $A \cap B \cap C = \emptyset$, then $Pr[A \cup B \cup C] = Pr[A] + Pr[B] + Pr[C]$.
   False. For instance, if $C = \emptyset$, it may not be that $Pr[A \cup B] = Pr[A] + Pr[B]$.

7. (a) Let $\Omega = \{1,2,3,4,5,6\}$ be a uniform probability space. Find two independent events A and B with $0 < Pr[A] < 1$ and $0 < Pr[B] < 1$.
   (b) Let $\Omega = \{1,2,\ldots,n\}$ be a uniform probability space. Assume that n is not a prime number. Find two independent events A and B with $0 < Pr[A] < 1$ and $0 < Pr[B] < 1$.
   (a) One can choose $A = \{1,2,3\}$ and $B = \{3,4\}$.
   (b) Let $n = ab$ where $a > 1$ and $b > 1$. We choose $A = \{1,2,\ldots,a\}$ and $B = \{a, a+1, \ldots, a+b-1\}$. We then see that $Pr[A] = a/n = 1/b$ and $Pr[B] = b/n = 1/a$. Also, $Pr[A \cap B] = 1/n = Pr[A]Pr[B]$.

3. Longer Questions: 8/8/8 Provide a clear and concise justification of your answer.

1. You select a three digit decimal number uniformly in $\{000, 001, \ldots, 999\}$. Note that we consider 023 to be a three digit decimal number, etc.
   (a) What is the probability that the number has three identical digits given that it has at least two identical digits?
   (b) What is the probability that the sum of the three digits is 9.
   (a) There are 3 ways of choosing which two digits are identical. There are then 10 ways of choosing that common digit and 9 ways of choosing the third digit. Thus, there are 270 ways of choosing a three digit number with exactly two identical digit. There are 10 three-digit numbers that have three identical digits. Thus, there are $10 + 270 = 280$ numbers with at least two identical digits and 10 among those have three identical digits. Hence, the probability that the number has three identical digits given that it has at least two identical digits is $10/280 = 1/28$.
   (b) We know that there are $\binom{11}{2} = 55$ ways of splitting 9 among the three digits. Thus, the desired probability is 55×10^{-3}.

2. There are two bags. One contains 4 red and 6 blue balls. The other contains 6 red and 4 blue balls. You select one of the two bags with equal probabilities and pick three balls without replacement.
   Hint: Give names to the appropriate events. For instance, let A_1 be the event that you selected the first bag, etc.
   (a) Given that you selected the first bag, what is the probability that the first two balls are red?
   (b) Given that you selected the first bag, what is the probability that the three balls are red?
   (c) Given that you selected the second bag, what is the probability that the first two balls are red?
   (d) Given that you selected the second bag, what is the probability that the three balls are red?
   (e) What is the probability that the first two balls are red?
   (f) What is the probability that the three balls are red?
   (g) Given that the first two balls are red, what is the probability that the third one is also red?
   (h) What is the probability that you selected the first bag given that the first two balls are red?
   Let A_1 be the event that you selected the first bag and A_2 the event that you selected the second. Also, let B be the event that the first two balls are red and C the event that the third one is red. Then $Pr[A_1] = Pr[A_2] = 0.5$.
   (a) $Pr[B|A_1] = (4/10)(3/9) = 4/30$.
   (b) $Pr[B \cap C|A_1] = (4/10)(3/9)(2/8) = 1/30$.
   (c) $Pr[B|A_2] = (6/10)(5/9) = 1/3$.
   (d) $Pr[B \cap C|A_2] = (6/10)(5/9)(4/8) = 1/6$.

(e) $Pr[B] = Pr[A_1]Pr[B|A_1] + Pr[A_2]Pr[B|A_2] = 0.5(4/30) + 0.5(1/3) = 7/30.$
(f) $Pr[B \cap C] = Pr[A_1]Pr[B \cap C|A_1] + Pr[A_2]Pr[B \cap C|A_2] = 0.5(1/30) + 0.5(1/6) = 1/10.$
(g) $Pr[C|B] = \frac{Pr[B \cap C]}{Pr[B]} = \frac{1/10}{7/30} = 3/7.$
(h) $Pr[A_1|B] = Pr[B|A_1]Pr[A_1]/Pr[B] = (4/30)(0.5)/(7/30) = 2/7.$

4. A car mechanic is great with probability 0.2 and ordinary otherwise. A great mechanic is great every day and an ordinary one is ordinary every day. The car mechanic works on one car at a time and, when he starts working on a car, he works on it day after day until he finishes. If he is great, he finishes a car repair with probability 0.6 independently on each day. If he is ordinary, he finishes it with probability 0.4 independently on each day. You ask two friends who used that mechanic. He completed their car repairs in 3 and 4 days, respectively.

(a) What is the probability p that the mechanic is great?

(b) What is the probability that he would repair your car repair in at most 2 days?

Note: The expression for p is a bit complicated. We don't want you to spend time evaluating its value. You can express the answer to (b) in terms of p.

Let G be the event that the car mechanic is great and F the event that he completed the repairs of the two cars in 3 and 4 days, respectively. Then,

$$Pr[F|G] = 0.4^2 0.6 \times 0.4^3 0.6 = 0.4^5 0.6^2 \text{ and } Pr[F|\bar{G}] = 0.6^2 0.4 \times 0.6^3 0.4 = 0.6^5 0.4^2.$$

Also, $Pr[G] = 0.2$ and $Pr[\bar{G}] = 0.8$.

(a) Using Bayes's Rule, we find

$$p := Pr[G|F] = \frac{Pr[G \cap F]}{Pr[F]} = \frac{Pr[G]Pr[F|G]}{Pr[G]Pr[F|G] + Pr[\bar{G}]Pr[F|\bar{G}]} = \frac{(0.2)0.4^5 0.6^2}{(0.2)0.4^5 0.6^2 + (0.8)0.6^5 0.4^2}.$$

(b) Let T be the event that he would complete your car repair in at most two days. Then

$$P[T|G] = 0.6 + 0.4 \times 0.6 = 0.84 \text{ and } P[T|\bar{G}] = 0.4 + 0.6 \times 0.4 = 0.64.$$

Hence, the desired probability is

$$0.84p + 0.64(1-p) = 0.64 + 0.2p.$$

5. How many? (1/1/2/3/3/4)

1. How many length 10 ternary strings are there? (A ternary number has three possible symbols: 0,1,2. The first digit can be 0! So, 0000000000 is a 10 symbol string.)
   3^{10}. Three choices for each digit.
2. How many length 10 ternary strings are there with a 1 as the first symbol?
   1×3^9. One choice for the first digit and three for each of the others.
3. How many 10 digit ternary numbers are there with a 1 in either of the first two digits. (You should count the numbers starting with 1 in both of the first two.)
   $2 \times 3^9 - 3^8$.
   Inclusion/exclusion, digit 1 in either and then subtract the intersection (first two digits are 1.)

4. How many length ternary strings are there where the symbols add up to 10? (Recall the symbols are $0, 1$ and 2. An example of such a string is 2222200000, since there are five 2's and five 0's and the sum of their numeric values is 10.)

   $\sum_{i=0}^{5} \binom{10}{i}\binom{10-i}{10-2i}$.

   To add to 10, one can have i 2's and $10-2i$ 1's. We sum over the possible number of i's. For each term, we construct a situation by choosing positions for the 2's and then positions for the $10-2i$ positions for the 1's.

5. How many ways are there to split up n dollars among r friends where each friend gets at least 1 dollar and no friend gets half or more of the dollars. (You may assume that n is even and $k \geq 3$. If convenient you can assume that $\binom{n}{m} = 0$ for $m > n$.)

   $\binom{n-1}{k-1} - \binom{k}{1}\sum_{i=n/2}^{n-k+1}\binom{n-i-1}{k-2}$

   The first term is the way to assign dollars to the friends so that each has at least one; it uses the trick that we assign $n-k$ dollars to the friends and add one to each to get a configuration.

   The second is subtracting the configurations where one friend gets more than half. The $\binom{k}{1}$ is selecting which friend. The sum is over the amount that the friend could have recieved.

6. Give a combinatorial proof that

$$3^n = \sum_{i=0}^{n} \binom{n}{i} 2^{n-i}.$$

   The left hand side is the number of ternary strings of length n.

   Each term in the right hand side counts the number of ternary string i 3's; there are $\binom{n}{i}$ chooses for positions of the 2's, and there are 2^{n-i} possible patterns of 0 and 1's in the remaining positions. The sum then gets you all the ternary strings.

6. Polynomials (1/1/1/5/4/1)

Consider two polynomials, $P(x)$ of degree d and $E(x)$ of degree k over $GF(p)$ (modulo p) for a prime p where $p > d > k$.

1. What is the maximum number of solutions to $P(x) = 5 \pmod{p}$?
   d solutions. Since there are at most d zeros for the polynomial $P(x) - 5$ since its degree is d.
2. What is the maximum number of solutions to $E(x)P(x) = 5 \pmod{p}$?
   $\min(d + r, p - 1)$ solutions.
   Since there are at most d zeros for the polynomial $P(x)E(x) - 5$ as the degree of the polynomial is at most $d + r$.
   We also no that no polynomial has degree larger than $p - 1$ modulo p.
3. What is the maximum number of solutions to $E(x) + P(x) = 5 \pmod{p}$?
   d solutions. Since the degree of the polynomial $E(x) + P(x) - 5$ is d and there are at most d solutions for this situation.
4. Assume that $d = 2$, $P(1) = 1$, $P(2) = 2$, and $P(3) = 2$ and $p = 7$, what is $P(0)$?
   $a + b + c = 1 \pmod{7}$
   $4a + 2b + c = 2 \pmod{7}$
   $2a + 3b + c = 2 \pmod{7}$

   Combining the last two, we obtain $b = 2a$, plug in to the first two equations yields,
   $3a + c = 1 \pmod{7}$ and $a + c = 2 \pmod{7}$.
   We then get $2a = -1 \pmod{7}$ and $a = -4 = 3 \pmod{7}$ (using the fact that 4 is the multiplicative inverse of 7.)
   We then get $b = 6$ and $c = -1 = 6 \pmod{7}$.
   Thus, $P(x) = 3x^2 - x - 1$ (taking negatives for ease of evaluation.) $P(1) = 1$, $P(2) = 2$, and $P(3) = 2$.
   $P(0) = -1 = 6 \pmod{7}$.
5. Assume that $d = 1$, and we are told that $P(1) = 2$, $P(2) = 3$, $P(3) = 2$, $P(4) = 0$ and $p = 5$, but we know there is exactly one incorrect point.
   (a) What is $P(0)$?
   This is a line. Try deleting each and seeing whether a line fits the other three points. Clearly, the line is $P(x) = x + 1$, since $P(1) = 1 + 1 = 2$, $P(2) = 2 + 1 = 3$, and $P(4) = 4 + 1 = 0$.
   (b) What is the error locator polynomial for Berlekamp-Welsh Algorithm for this situation? $E(x) = x - 3$.

7. Countability/Computability (1/1/1/1/1/1/1)

For the following problems, a computer program may run forever, and if it eventually prints every element of a set or every digit of a real number at a finite, specific time, it is said to print out that set or that number. For example, there is a computer program that prints out every natural number. We also allow a computer program access to an infinite amount of memory.

1. The power set (the set of all subsets) of any infinite set is uncountable. (True/False)
   True. If the infinite set has the same cardinality as the integers, we know its power set is uncountable.
   If it is already uncountable, then its power set is at least as large and is thus uncountable.

2. There is a computer program that prints all rational numbers. (True/False)

   True. We can write a program to enumerate the set of rational numbers in the same manner as we counted them.

3. A computer program can print out $\sqrt{2}$. (True/False)

   True. We can calculate successive digits of $\sqrt{2}$ using say binary search and print the digits as we go.

4. There is a computer program that prints all real numbers. (True/False)

   False. This would produce a listing of all the real numbers which we know does not exist due to its uncountability.

5. There is an efficiency checking program that takes another program P and an input n and verifies that P halts within 2^n steps for all inputs of size n. (True/False)

   True. We can enumerate all the inputs of size less than n and then run the program on each for 2^n+1 steps and see if it halts before then.

6. There is a computer program that prints all computer programs and the inputs where they halt. (True/-False.)

   True. We can run enumerate all computer programs and all inputs and all runtimes in three lists. Then we can interleave the lists to get all tuples of program, input, runtime and run each program on the corresponding input for the corresponding runtime. Then, we print out the programs and input when it halts.

7. There is a computer program that given a program P and input x can check if all the subroutines of P are called. (True/False.)

   False. This is undecidable. It is the same problem as the DEAD code problem. The reduction is to add a dummy exit procedure, and always call it when exiting. Deciding whether that procedure is called or not is equivalent to deciding whether the original program halted.

8. Schemes (3/3/3/1/1)

1. Bob saw a show about twin primes, primes p and q where $q = p+2$. Thinking these were cool, he decided to use twin primes to construct his RSA key pair. Give a polynomial time method to break his scheme. Recall that he makes (N,e) public and that $N = pq$ for his twin primes p and q.

   We know $p(p+2) = N$, or $p^2+2p = N$, or $p = \frac{-2\pm\sqrt{4+4N}}{2}$ using the quadratic formula. Computing a sqrt is fast using binary search and as we know there is an integer solution by construction, this method will recover p.

2. A secret has been shared among 10 people using the scheme from class with a degree 3 polymonial. Recall that any 4 people can reconstruct the secret. But say all 10 agree to cooperate but some remember incorrectly (or are just lying). What is the largest number of people who can be incorrect where the group can still correctly reconstruct the secret?

   This is actually error correction where $n = 4$ and $n+2k = 10$. Solving for k, we will be successful when k is at most 3.

3. Consider that some CS70 students want to vote for their favorite superhero: Batman or Superman. If a student i likes Batman, they construct a polynomial $P_i(x) = r_i x + 1$, otherwise they construct a polynomial of $r_i x - 1$ where r_i is chosen uniformly at random in $\{0,\ldots,p-1\}$. The polynomials are in $GF(p)$, that is considered to be evaluated modulo p.

   Then each student gives Professor Walrand $P_i(1)$ and Professor Rao $P_i(2)$. The professors serve as vote counters.

(a) The professors' compute the sum of the values given to each and each professor announces the result. Professor Walrand announces that his sum (or $\sum_i P_i(1) \pmod{11}$) is 3 and Professor Rao announces that his sum (or $\sum_i P_i(2) \pmod{11}$) is 5. If $p = 11$ (the student's polynomials are modulo 11) and 5 students voted, who is the students' favorite? (Justify briefly.)
Consider the polynomial $Q(x) = \sum_i P_i(x)$. It is a degree 1 polynomial whose constant term is the sum of the student's degree 1 terms. Thus, the degree 1 term gives the difference between those who prefer Walrand and those who prefer Rao.
We know that $Q(1) = 3$ and $Q(2) = 5$. Thus, $Q(x) = 2x + 1$ or the sum of the votes is 1, which means more students voted for Batman than Superman.

(b) Can either professor know who a student voted for, given that they do not reveal any individual student's value to the other professor? (Justify briefly.)
No. The professor only knows one point on each student's line. Thus, the value of $P_i(0)$ could be either 1 or -1 from each professor's view.

(c) How could a student have cheated?
A student could have used a polynomial $x + 2$ and have voted for Batman twice. Uh oh!