1. **Short Answer: Modular Arithmetic/RSA. 16 points: 3/3/3/3/4**

   Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

   For each question, please answer in the correct format. When an expression is asked for, it may simply be a number, or an expression involving variables in the problem statement, you have to figure out which is appropriate.

   (a) What is $3^{240} \pmod{77}$?
   Answer: $3^{240} = (3^{60})^4 = 1^4 = 1 \pmod{77}$

   The second step follows from $7^{(p-1)(q-1)} = 1 \pmod{77}$.

   (b) What is $3^{16} * 3^{-1} \mod 7$? (Hint: the multiplicative inverse of 3 is 5 modulo 7 and repeated squaring.)
   Answer: $(3^{16}) * 3^{-1} = ((3^2)^2)^2 * 5 = 6 \pmod{7}$

   (c) Given an RSA scheme for large primes p and q where $q < p < 2q$ we can set $e = p$ and get a valid construction. (True or False.)
   Answer: True. p is co-prime to $(p-1)(q-1)$ in this case, as $p-1$ cannot contain q as a factor, and vice versa, and both p and q are prime.

   (d) What is d for RSA scheme with $(N = 143, e = 11)$?
   Answer: We have $N = 11(13) = 143$, we want $11^{-1} \pmod{(10)(12)}$ which is 11.

   (e) Background: Alice wants a signature of x from Bob but doesn't want Bob to know x.
   Let (N,e) be Bob's public key, and d be his decryption key. Alice chooses a random r that is relatively prime to N, and sends Bob $r^e x \pmod{N}$ to sign, and Bob returns $m = (r^e x)^d \pmod{N}$ to Alice .
   Give an expression that yields Bob's signature of x: $x^d \pmod{N}$. Your expression may use the variables m, x, r, N and e.
   Answer: $r^{-1}m \pmod{N}$, where r is the multiplicative inverse of r.
   Verification: $r^{-1}m = r^{-1}(r^e x)^d = r^{-1}(r^{ed})x^d = r^{-1}rx^d = 1 \pmod{N}$.

2. **Polynomials. 19 points. 3/3/3/3/3/4**

   Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

   (a) How many different degree $\leq d$ polynomials modulo p contain d points; $(x_1, y_1), \ldots, (x_d, y_d)$. (Assume that $p > d$.)
   Answer: Choosing a y value for one more point makes the polynomial unique; thus, since there are only p possible y-values for this point, the number of polynomials is at most p.

   (b) What is the maximum number of times that a degree 4 polynomial, $P(x)$, and a degree 2 polynomial, $Q(x)$, can intersect? (That is, what is the maximum number of x-values where $P(x) = Q(x)$.)
   Answer: At most $d = 4$. The difference polynomial, $P(x) - Q(x) = 0$, has to be 0 at the intersection points, and has at most d zeros.

   (c) What is the minimum modulus that could be used to send the message $3, 4, 3$ through a channel that drops 3 packets?
   Answer: One needs to send 6 packets. Thus, the modulus should be at least 7, which is prime and allows one to have more than 6 different x-values for your points.

   (d) What is the polynomial that encodes the message $3, 3, 0$ modulo 7. (Use the x values $0, 1, 2$ in your encoding.)
   Answer: $P(x) = 2x^2 - 2x + 3$
   Solve a linear system. It works out pretty ok, but takes a minute or two.

(e) What is the error polynomial for Berlekamp-Welsh for a message $\pmod{11}$ where errors appeared at $x = 2$ and $x = 4$?
Answer: $(x-2)(x-4) = x^2+5x+8 \pmod{11}$

(f) We are working modulo seven, $\pmod{7}$, in this problem. We have polynomials

$$\begin{array}{lll} p_1(1)=3 & p_1(2)=0 & p_1(3)=0 \\ p_2(1)=1 & p_2(2)=1 & p_2(3)=0 \\ p_3(1)=0 & p_3(2)=0 & p_3(3)=1 \end{array}$$

Describe a polynomial $p(x)$ where $p(1)=5, p(2)=3$ and $p(3)=1$ in terms of polynomials $p_1(x), p_2(x)$, and $p_3(x)$. (Remember this is all $\pmod{7}$.)
Answer: $3p_1(x)+3p_2(x)+p_3(x)$.
Start with $5(5p_1(x))+3(p_2(x)-5p_1(x))+p_3(x)$ where each term comes from an appropriate Δ functions.

3. Short Answer: Counting. 18 points: 3/3/3/3/3/3

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) How many distinguishable orderings of CALIFORNIA are there?
Answer: $\frac{10!}{2!2!}$

(b) How many ways are there to split up 10 dollars among Bob, Alice and Eve? (Notice that it is valid to give 0 to one or two of the people.)
Answer: $\frac{12!}{2!10!}$

(c) How many ways are there to split up 10 dollars among Bob, Alice and Eve so that Eve gets at least 5 dollars?
Answer: $\frac{7!}{2!5!}$.
It is the same as the situation that 5 dollars are split among the three and then giving Eve 5 more dollars. That darn Eve!

(d) How many ways are there to place k indistinguishable balls into n distinguishable bins?
Answer: $\binom{n+k-1}{n-1}$

(e) How many five card heart flushes are there in a fifty two card poker deck? (A heart flush has all the cards being a heart. Recall also that each suit has thirteen cards.)
Answer: $\binom{13}{5}$ or $\frac{13!}{8!5!}$.

(f) How many five card poker hands have exactly one Ace or is completely composed of clubs (a club flush)?
Answer: $\binom{4}{1}\binom{48}{4}+\binom{13}{5}-\binom{12}{4}$

4. Short Answer: Countable and UnCountable. 6 points. 3/3

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) Give a bijection from the real number interval $(1,\infty)$ to the real number interval $(0,1)$. (Notice the intervals are open.)
Answer: $f(x) = 1/x$

(b) Given an $n \times n$ matrix A where the diagonal consist of alternating 1's and 0's starting from 1, $A[0,0] = 1$, describe a n length vector from $\{0,1\}^n$ that is not equal to a row in the matrix. (Hint: the all ones vector or the all zeros vector of length n could each be rows in the matrix.)

Answer: The row consisting of alternating 1's and 0's starting with 0.
That is, 010101....

5. Short Answer: Computability. 6 points. 3/3.

Clearly indicate your correctly formatted answer: this is what is to be graded. No need to justify!

(a) The problem of determining whether a program halts in time 2^{n^2} on an input of size n is undecidable. (True or False.)

Answer: False. You can simulate a program for 2^{n^2} steps and see if it halts.

(b) There is no computer program DEAD which takes a program P, an input, x, and a line number, n, and determines whether the nth line of code is executed when the program P is run on the input x. (True or False.)

Answer: True.

We implement HALT using DEAD as follows. We take the input P and modify it so that each exit or return statement jumps to a particular new line. Call the resulting program P'. We then hand that program to DEAD along with the input x and the number of the new line. If the original program halts than DEAD would return false, and if not DEAD would return true. Flipping these answers gives a valid program for Halt.

This is contradicts the fact that the program HALT does not exist, so DEAD does not exist.

6. A couple of proofs. 20 points: 8/12.

(a) Give a combinatorial proof that $3^n = \sum_{i=0}^{i=n} \sum_{j=0}^{j=n-i} \binom{n}{i} \times \binom{n-i}{j}$

Answer:

Both count the number of n strings consisting of $\{0,1,2\}$ (3 characters.)

The left hand side clearly counts by the first rule of counting this as there are 3 choices for each position.

The right hand side sums over the number of ways to pick i 0's and j ones; each term is calculated by choosing the places for the 0's and then choosing the places for the j 1's.

(b) Let S_n be the numbers in $\{0,\ldots,n-1\}$ that are relatively prime to n.

(i) For a set $T_a = \{ax \pmod n : \ x \in S_n\}$ where $a \in S_n$ show that $T_a = S_n$.
Answer: Since a has a multiplicative inverse the function is one to one, so $|T_a| \geq |S|$. Also, anything of the form ax is relatively prime to n if both a and x are so $T_a \subseteq S$. This implies they are the same set.

(ii) For any $a \in S_n$, $a^x = 1 \pmod n$. What is x? (State your answer as an expression using S_n and other standard math expression symbols, e.g, $|\cdot|$. Briefly justify.)
Answer: $|S_n|$. From the previous part we know the products of the elements of T_a and S_n are the same, and the product of elements in T_a has $|S_n|$ extra a's when compared to the product of elements of S_n. Thus $a^{|S_n|} = 1 \pmod n$.

(iii) For $n = pq$ where p, and q are distinct primes, what is $|S_n|$?
Answer: $pq - p - q + 1 = (p-1)(q-1)$
Explanation: pq numbers from $\{0,\ldots,pq-1\}$ minus those which are divisible by p, which is q, minus those which are divisible by q, which is p, plus 1 since we subtracted twice for 0 (which is divisible by both p and q.)

7. Hamming: Another optimal code. 16 points. 3/3/3/3/2/2

(a) Consider communicating 7 bits in an 8 bit message where the final bit will be the parity of the number of ones in the first seven. That is, if the number of ones is odd in the first 7 bits, the 8th bit will be 1, if the number of ones is even, the 8th bit is 0. Given that at most 1 bit gets corrupted, how can you tell if the message was corrupted or not. (Notice the parity bit itself could be the bit that was corrupted.)
Answer: You add up the bits modulo 2. If it is odd then there is a corruption.

(b) Consider communicating 4 bits in an 7 bit message. We will make sure the following equations holds.

$$\begin{aligned} m_1 + m_3 + m_5 + m_7 &= 0 \pmod 2 \\ m_2 + m_3 + m_6 + m_7 &= 0 \pmod 2 \\ m_4 + m_5 + m_6 + m_7 &= 0 \pmod 2 \end{aligned}$$

We will send a message 1011 by setting bits $m_1 = 1, m_2 = 0, m_3 = 1, m_4 = 1$. How should the bits m_5, m_6 and m_7 be set to satisfy the equations above.
Answer:
Set $m_5 = 0, m_6 = 1, m_7 = 0$.

(c) Say the previous encoding was used and the message received was 1101100, where there is at most one bit that was flipped. What was the original message? (Note the message you should reconstruct is not necessarily the one from part (b).)
Answer: 1001100. Only the second equation is unsatisfied, only bit m_2 is only in that equation.

(d) Argue that you can recover from any 1-bit error using the scheme above.

Answer: The unsatisfied equations indicate the bit position where the error is. The first equation contains the odd bits, the second contains the bits which have 1 in the second position, and the third contains the bits which contain 1 in the third. For each bit, the binary representaion of the index of the bit indicates the unique set of equations which it is in.

Since only one bit is flipped, the equations containing that bit will be unsatisfied and we can output the index of the bit.

(e) A codeword is any 7-bit string that satisfies the equations above. As the codewords are 7-bit strings, we can consider them to be vertices in a 7 dimensional hypercube. What is the minimum distance (length of a path) in the hypercube between codewords?

Answer: The distance between any two codewords must be 3 as we can recover from 1 error. If the distance was less than that, we could not expect to figure out a unique codeword corresponding to the corruption.

(f) Notice that there are 7 places where an error can occur plus a case where no error occurs or a total of 8 possible outcomes of the transmission. Argue that at least 3 extra bits are required to recover from one error; i.e., that one can only transmit 4 message bits in any scheme that send at least 7 bits and tolerates a single bit flip error.

Answer: There are eight possible outcomes for what happens with the errors as noted. To identify which outcome requires 3 bits as the number of different possibilities for 3 bits is 2^3 or 8. Fewer bits cannot represent all 8 possibilities.