Name: _____KEY_____ E-mail ID: _____@virginia.edu

Pledge: _____

_____

_____

Signature: _____

There are 75 minutes for this exam and 100 points on the test; don't spend too long on any one question!

The 12 short answer questions require only a sentence or two for full credit; the two long answer questions have their own page, and obviously require more. There are 12 short-answer questions worth 5 points each, and two long-answer questions worth 20 points each.

All work must be on these exam pages.

Good luck!

Page 2	_____ / 15
Page 3	_____ / 15
Page 4	_____ / 15
Page 5	_____ / 15
Page 6	_____ / 20
Page 7	_____ / 20
Total	**_____ / 100**

Short answer questions (5 points each): these questions only require a sentence or two for full credit.

1. Why is cracking (i.e. decrypting without the authorized decryption key) an RSA-encrypted message very hard to do?

   Answer:

   Because in order to do so, you must factor a very large number that is the product of two large primes, and there is no known efficient way to do this.

2. Explain, using English only (i.e. no equations or formula), what it means when it is said that a given problem is NP-complete.

   Answer:

   It means that there is no known efficient solution to the given problem, although it is possible (but not widely believed) that such an efficient solution could exist.

3. Explain, using English only (i.e. no equations or formula), what Big-Oh notation means. For example, if a function is said to be $O(n^2)$, what does that mean? Explain for the general case, though – not just the $O(n^2)$ case.

   Answer:

   Big-Oh tells the running time for a function given an input of size n. This running time is expressed as a formula using n, for example, n^2.

4. Solve the halting problem. Explain your answer. And while you're at it, explain what the halting problem is. Use the last page of this exam if you need more space.

Answer:

It can't be solved! It was the first algorithm that was proven (by Alan Turing in 1936) to not have a possible solution.

5. A license plate can consist of the digits 0-9 and the letters A-Z. Consider license plates of the form *dde-edd* and *eel-lee*, where *d* is a digit, *l* is a letter, and *e* can be either a digit or a letter. How may possible combinations of license plates can be formed using these two patterns? You can leave your answer as the product of numbers – you don't have to multiply the values out.

Answer:

There are 10 possibilities for each digit *d*, 36 for each *e*, and 26 for each letter *l*. Thus, the total possibilities is $10^2 36^2 26^2$ for the first pattern (by the product rule), and $36^4 26^2$ for the second pattern (also by the product rule). By the sum rule, the total possibilities is the sum of the two values. There are $10^4 26^2$ common plates (of the form *ddl-ldd*), so by the inclusion-exclusion principle, this value must be subtracted from the total. Thus, the total is $10^2 36^2 26^2 + 36^4 26^2 - 10^4 26^2$ (which is 87,609,600 + 1,135,420,416 - 6,760,000 = 1,216,270,016).

6. Determine the greatest common divisor (gcd) and least common multiple (lcm) of 30,030 and 484,704. For your reference, the factorization of 30,030 is 2*3*5*7*11*13, and the factorization of 484,704 is $2^5 * 3^4 * 11 * 17$. Leave your answer is factored form (i.e. 2*3*5*7*11*13 instead of 30,030).

Answer:

$$30{,}030 = 2^1 3^1 5^1 7^1 11^1 13^1 17^0 \text{ and } 484{,}704 = 2^5 3^4 5^0 7^0 11^1 13^0 17^1$$

$$\begin{aligned}\gcd(30030,484704) &= 2^{\min(1,5)} 3^{\min(1,4)} 5^{\min(1,0)} 7^{\min(1,0)} 11^{\min(1,1)} 13^{\min(1,0)} 17^{\min(0,1)} \\ &= 2^1 3^1 5^0 7^0 11^1 13^0 17^0 = 2^1 3^1 11^1 = 66\end{aligned}$$

$$\begin{aligned}\text{lcm}(30030,484704) &= 2^{\max(1,5)} 3^{\max(1,4)} 5^{\max(1,0)} 7^{\max(1,0)} 11^{\max(1,1)} 13^{\max(1,0)} 17^{\max(0,1)} \\ &= 2^5 3^4 5^1 7^1 11^1 13^1 17^1 = 220{,}540{,}320\end{aligned}$$

7. Explain the difference between countable and uncountable sets. Don't just give an example!

Answer:

Countable sets can be listed in some order such that you will list every element, but you cannot do this with uncountable sets. Alternatively, a countable set has a 1-to-1 correspondence with the integers, whereas an uncountable set does not.

8. What is the difference between weak induction and strong induction?

Answer:

The inductive hypothesis in weak induction only assumes $P(k)$ is true, while the inductive hypothesis in strong induction assumes $P(1), P(2), ..., P(k)$ are all true (where $P(1)$ is the base case). The differing number of base cases is **not** a difference between the two induction types.

9. What is the cardinality of a power set of a set of *n* elements?

Answer:

2^n

10. Explain, using English only (i.e. no pseudo-code), how the bubble sort XOR the insertion sort works. Include the Big-Oh estimate of the running time as well. We're looking for a general overview here, not all the specific details.

Answer:

Insertion sort assumes part of the list is already sorted (initially that part is only the first element). It then selects the next element in the unsorted part of the list, and inserts it into the correct position in the sorted part of the list. Insertion sort is $O(n^2)$.

Bubble sort will compare one element to it's neighbor, and swap them if they are out of order. This causes the elements to "bubble" or "percolate" up (or down) the list. This must be done repeatedly (if there are n elements in the list, then you have to go through the "bubbling" a total of n times). Bubble sort is $O(n^2)$.

11. Explain, using English only (i.e. no equations or formula) how one goes about doing a structural induction proof. Specifically, how is it different than mathematical induction? Don't just list the three steps for structural induction – explain how those steps are different from the other induction types (or, if they are not different, state such).

Answer:

Structural induction is designed to show that some property holds for recursively defined "things", whether those things are formula (such as the Fibonacci sequence), trees, strings, etc. The big difference is that in the inductive hypothesis, you assume that the property holds for some existing elements. In the recursive step (a.k.a. inductive step), you show how to create a new element out of the existing elements, and then show that the property holds for that new element.

12. What (physical) prop did Professor Bloomfield use in class to illustrate how a binary search works?

Answer:

A phonebook.

13. (20 points) Using weak mathematical induction, prove that 5^n+3 is divisible by 4 for $n \geq 0$.

Answer:

Let $P(n) = 5^n + 3 \mid 4$.

Base case: $P(0)$. $5^0+3 = 1+3 = 4$, which proves the base case.

Inductive hypothesis: Assume that $P(k)$ is true (in other words, assume that $5^k + 3 \mid 4$).

Inductive step: Show that $P(k+1)$ is true (in other words, show that $5^{k+1} + 3 \mid 4$).

$$5^{k+1} + 3$$
$$= 5 * 5^k + 3$$
$$= (1+4) * 5^k + 3$$
$$= 5^k + 4 * 5^k + 3$$
$$= 5^k + 3 + 4 * 5^k$$

We know that $5^k + 3 \mid 4$ from the inductive hypothesis. $4 * 5^k$ is clearly divisible by 4. As both parts are divisible by 4, the sum is therefore also divisible by 4. This completes the proof.

(Source: Malik/Sen, exercise 3, page 143)

14. (20 points) Give a recursive definition for each of the following sequences. For this question, the first term of the sequence is $n = 1$, not $n = 0$.

a) (5 points) $a_n = n^2$

Answer:

$a_1 = 1$

$a_n = a_{n-1} + 2n - 1$

b) (5 points) $a_n = \sum_{i=0}^{n} i$

Answer:

Sequence is 1, 3, 6, 10, 15, 21, etc.

$a_1 = 1$

$a_n = a_{n-1} + n$

c) (5 points) The Fibonacci sequence

Answer:

$f_1 = 1, f_2 = 1$

$f_n = f_{n-1} + f_{n-2}$

d) (5 points) The sequence that generates the terms 3, 6, 12, 24, 48, 96, 192, …

Answer:

$a_1 = 3$

$a_n = 2 * a_{n-1}$

This page intentionally left blank

(you can use this space to solve the halting problem, though)