Discrete Mathematics

Spring 2024

Homework #3

Due: Friday, May 17, 2024

Total points: 100

Important Note: In problems where the reasoning isn't totally obvious, EXPLAIN your reasoning. This is an important part of the thinking process (and also gives you a chance for partial credit). Also, note that there are solutions to the odd-numbered problems in the book. You may want to check them out to get ideas for the assigned problems.

1. (5 points) Write down the prime factorization (in ascending order) of each of the following integers (Example: $720 = 2^4 \cdot 3^2 \cdot 5$).
   (a) 258
   (b) 100000
   (c) 6250
   (d) 104
2. (5 points) Use the Euclidean algorithm to determine the following greatest common divisors. Write down every step in your calculation.
   (a) gcd(3300, 550)
   (b) gcd(177, 300)
   (c) gcd(912, 625)
3. (5 points) Use mathematical induction to show that the following equation is true for all natural numbers n:
   (a) $2^0 + 2^1 + 2^2 + \ldots + 2^n = 2^{n+1} - 1$
   (b) $1(1!) + 2(2!) + 3(3!) + \ldots + n(n!) = (n + 1)! - 1$
4. (5 points) Give a recursive definition of each of the following sequences $\{a_n\}$, where n = 1, 2, 3, …,
   (a) $a_n = n + 3$
   (b) $a_n = 2n$
   (a) $a_n = (-1)^n$
   (b) $a_n = 2n!$
5. (5 points) **Converting Back and Forth**
   Show every step of your computation for the following conversions:

   a) Convert the decimal number 2885 into its hexadecimal expansion.

   b) Convert the binary number $(1101100)_2$ into its decimal expansion.

   c) Convert the octal number $(7435)_8$ into its hexadecimal expansion.

   d) Convert the hexadecimal number $(AF81)_{16}$ into its binary expansion.

6. (5 points) **Modulo arithmetic**
Solve the following equations for x modulo the indicated modulus, or show that no solution exists. Show your work.

(a) $7x \equiv 1 \pmod{15}$.

(b) $10x + 20 \equiv 11 \pmod{23}$.

(c) $5x + 15 \equiv 4 \pmod{20}$.

7. (5 points) Determine an integer n such that
$$n \equiv 1 (\mathrm{mod} 7), \quad n \equiv 3 (\mathrm{mod} 8) \quad \text{and} \quad n \equiv 2 (\mathrm{mod} 9).$$

8. (10 points) (a) Use Fermat's little theorem to compute 5^{2003} mod 7, 5^{2003} mod 11, and 5^{2003} mod 13.
(b) Use your results from part (a) and the Chinese remainder theorem to find 5^{2003} mod 1001. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

9. (5 points) Encrypt the message CANCEL THE ORDER using blocks of seven letters and the transposition cipher based on the permutation of $\{1, 2, 3, 4, 5, 6, 7\}$ with $\sigma(1) = 5$, $\sigma(2) = 3$, $\sigma(3) = 6$, $\sigma(4) = 1$, $\sigma(5) = 7$, $\sigma(6) = 2$, and $\sigma(7) = 4$.

10. (10 points) **RSA**
Let p = 17, q = 11 be a RSA private key and n = pq, e = 3 be the public key. Show your work. Feel free to use a computer to assist with the computations, but do show intermediate results.
(a) What is the result of encrypting the message m = 86 with these keys?
(b) What is d?
(c) How would the encrypted message be decrypted?

11. (10 points) **Carmichael numbers**
(a) Given that a and d are relatively prime, show that $ab = cd$ implies that d divides b.
(b) Prove that if $a = b \bmod m_1$ and $a = b \bmod m_2$, $a = b \bmod m_1 m_2$ provided that $\gcd(m_1, m_2) = 1$.
(c) A Carmichael number c can be written as a product of *distinct* primes $p_1 p_2 \cdots p_k$, where $p_i - 1$ divides $c - 1$, for all i. Show that if c is a Carmichael number and a is relatively prime to c, then $a^{c-1} = 1 \pmod{c}$.
(Hint: Use Fermat's little theorem to reason about $a^{p_i - 1} \bmod p_i$. Now, what is $a^{c-1} \bmod p_i$?)

12. (5 points)
(a) Find a formula for
$$\sum_{i=1}^{n} \frac{1}{i \cdot (i+1)} = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \ldots + \frac{1}{n(n+1)}$$
by examining the values of this expression for small values of n.
(b) Prove the formula you conjectured in part (a). (Hint: use induction)

13. (5 points) **Strengthening the claim**
The following is an example where it is easier to prove a stronger result than a weaker one:
(a) Try to prove by induction that $1 + 1/4 + 1/9 + \cdots + 1/n^2 < 2$ for all positive integers n. What happens?
(b) Prove by induction that $1 + 1/4 + 1/9 + \cdots + 1/n^2 < 2 - 1/n$ for all positive integers n.

14. (5 points) **A Quadratic Recurrence**

Given a rooted binary tree with n leaves. We define the cost of each leaf is 0, and the cost at each internal node as the number of leaves in the left subtree times the number of leaves in the right subtree. Prove that the total cost is n(n − 1)/2.

15. (5 points) **Modular inverse**

Prove that the equation $ax \equiv ay \bmod n$ implies $x \equiv y \bmod n$ whenever gcd(a, n) = 1. Show that the condition gcd(a, n) = 1 is necessary by supplying a counterexample with gcd(a, n) > 1.

16. (5 points)

(a) Devise a recursive algorithm to find a^{2^n}, where a is a real number and n is a positive integer. [Hint: Use the equality $a^{2^{n+1}} = (a^{2^n})^2$.]

(b) Give a recursive algorithm for finding the sum of the first n positive integers.

17. (5 points) **Chinese remaindering**

You want to teach two kids to count up to 15. Unfortunately, they can only count up to five. Here's how you do it: You tell one of them to count up to three and go back to one when the number counted exceeds that. Tell the other to do the same thing up to five. Then you can put together the answers (say, 2 and 4) to find the unique number between 1 and 15 that has these remainders modulo 3 and 5, respectively. (In this example, the only such number is 14.)

Here we show that this method always works.

Let $N = p_1 \cdot \cdots p_k$ be the product of k distinct primes. Now consider two integers x, y between 1 and N, and their remainders $x_i \equiv x \pmod{p_i}$, $y_i \equiv y \pmod{p_i}$. Show that, if $y_i \equiv x_i \pmod{p_i}$ for all $i = 1, \ldots, k$, then $x \equiv y \pmod{N}$. [Hint: What does $x_i \equiv y_i \pmod{p_i}$ imply for $x - y$?]