University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ISEN/ISCI-210: Discrete Structures

Fall 2018

Homework Set 3

Chengjiang Long

Assigned Date: Oct 22, 2018 (Monday).
Due Date: Nov 2, 2018 (Friday).
Collaboration Policy. Homeworks will be done individually: each student must hand in their own answers. Use of partial or entire solutions obtained from others or online is strictly prohibited.
Late Policy. No late submissions will be allowed without consent from the instructor. If urgent or unusual circumstances prohibit you from submitting a homework assignment in time, please e-mail me explaining the situation. ***Those submissions $\geq$ 12 hours after the deadline will be considered as "late submission".***
Submission Format. Electronic submission of a PDF file is mandatory.

Problem 1: Algorithms, Growth of Functions and Complexity (24 points)

(a) Use the selection sort to sort 6, 2, 3, 1, 5, 4, showing the lists obtained at each step.

(b) Use the bubble sort to sort d, f, k, m, a, b, showing the lists obtained at each step.

(c) Use the greedy algorithm to make change using quarters, dimes, nickels, and pennies for 99 cents, showing the details at each step.

(d) Show that $(x^2 + xy + xlogy)^3$ is $O(x^6y^3)$.

(e) Show that $x^5y^3 + x^4y^4 + x^3y^5$ is $\Omega(x^3y^3)$.

(f) Show that $3x^2 + x + 1$ is $\Theta(3x^2)$.

(g) Suppose that $f(x)$, $g(x)$, and $h(x)$ are functions such that $f(x)$ is $\Theta(g(x))$ and $g(x)$ is $\Theta(h(x))$. Show that $f(x)$ is $\Theta(h(x))$.

(h) Show that if $f_1(x)$ and $f_2(x)$ are functions from the set of positive integers to the set of real numbers and $f_1(x)$ is $\Theta(g_1(x))$ and $f_2(x)$ is $\Theta(g_2(x))$, then $(f_1f_2)(x)$ is $\Theta((g_1g_2)(x))$.

Problem 2: Integers and Division (16 points) What are the quotient and remainder when

(a) 44 is divided by 8?
(b) 777 is divided by 21?
(c) -123 is divided by 19?
(d) -1 is divided by 23?
(e) -2002 is divided by 87?
(f) 0 is divided by 17?
(g) 1,234,567 is divided by 1001?
(h) -100 is divided by 101?

Problem 3: Modular Arithmetic (14 points) Find each of these values:

(a) $(177 \bmod 31 + 270 \bmod 31) \bmod 31$
(b) $(177 \bmod 31 \times 270 \bmod 31) \bmod 31$
(c) $(-133 \bmod 23 + 261 \bmod 23) \bmod 23$
(d) $(976 \bmod 32)^3 \bmod 15$
(e) $(49 \bmod 17)^2 \bmod 11$
(f) $(193 \bmod 23)^2 \bmod 31$
(g) $(893 \bmod 79)^4 \bmod 26$

Problem 4: Integer Representations and Modular Exponentiation Algorithom (20 points)

(a) [2 points] Convert the decimal expansion 100632 to a binary expansion.

(b) [2 points] Convert the binary expansion $(110100100010000)_2$ to decimal expansion.

(c) [2 points] Convert the octal expansion $2417)_8$ to a binary expansion.

(d) [2 points] Convert the binary expansion $(101010101010101)_2$ s to an octal expansion.

(e) [2 points] Convert $(BADFACED)_{16}$ from its hexadecimal expansion to its binary expansion.

(f) [2 points] Convert $(1100001100011)_2$ from its binary expansion to its hexadecimal expansion.

(g) [8 points] Use Modular Exponention Algorithm to find $123^{1001} \bmod 101$. [**Hint***: you can refer to the textbook on Page 254, or slides 22-24 in Lecture 17.*]

Problem 5:Primes and Greatest Common Divisors (26 points)

(a) [2 points] Determine whether 111 is prime with detailed explanation.

(b) [2 points] Determine whether the integers in the set $\{17, 18, 19, 23\}$ are pairwise relatively prime.

(c) [4 points] What are the greatest common divisor and the least common multiple for $3^7 \cdot 5^3 \cdot 7^3$, $2^{11} \cdot 3^5 \cdot 5^9$

(d) [4 points] Find gcd(1000, 625) and lcm(1000, 625) and verify that gcd(1000, 625) $\cdot$ lcm(1000, 625) $= 1000 \cdot 625$.

(e) [4 points] Show that if a and b are positive integers, then ab = gcd(a,b) · lcm(a,b). [**Hint**: *Use the prime factorizations of a and b and the formulae for gcd(a,b) and lcm(a,b) in terms of these factorizations.*]

(f) [4 points] Use the Euclidean algorithm to find gcd(12345, 54321).

(g) [6 points] Use the Euclidean algorithm and the conclusion in (e) to find lcm(1529, 14038).

[Optional] Extra Points (20 points)

(a) [4 points] Which memory locations are assigned by the hashing function h(k) = k mod 97 to the records of insurance company customers with these Social Security number 987255335 and 501338753?

The United States Postal Service (USPS) sells money orders identified by an 11-digit number $x_1 x_2 \ldots x_{11}$. The first ten digits identify the money order; x11 is a check digit that satisfies $x_{11} = x_1 + x_2 + \ldots + x_{10}$ mod 9.

(b) [3 points] Find the check digit for the USPS money orders that have identification number that start with these ten digits 3289744134.

(c) [3 points] Determine whether 66606631178 is a valid USPS money order identification number.

In the RSA cryptosystem, each individual has an encryption key (n, e) where $n = pq$, the modulus is the product of two large primes p and q, say with 200 digits each, and an exponent e that is relatively prime to $(p-1)(q-1)$. To produce a usable key, two large primes must be found. This can be done quickly on a computer using probabilistic primality tests, referred to earlier in this section. However, the product of these primes $n = pq$, with approximately 400 digits, cannot, as far as is currently known, be factored in a reasonable length of time. As we will see, this is an important reason why decryption cannot, as far as is currently known, be done quickly without a separate decryption key.

(d) [5 points] Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers.

(e) [5 points] What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671? [**Hint**: *To decrypt, first find the decryption exponent d which is the inverse of* $e = 13$ *modulo* $42 \cdot 58$.]