University at Albany, SUNY

College of Engineering and Applied Sciences, Computer Science

ICSI-521: Discrete Mathematics with Applications

Spring 2019

Homework Set 3

Chengjiang Long

Assigned Date: Feb 28, 2019 (Thursday).
Due Date: Mar 14, 2018 (Thursday), 11:59 PM.
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. If urgent or unusual circumstances prohibit you from submitting a homework assignment in time, please e-mail the instructor explaining the situation to get exempt from late penalty. Otherwise, any late submissions without consent from the instructor will result in exponential penalty – late for one day loses 25%, two days loses 50%, and so on and so forth. **Those submissions $\geq$ 3 hours after the deadline will be considered as "late submission" with no exemption.**
Submission Format. Electronic submission as a zip file including a PDF file and code files to blackboard is mandatory.

- You can write your solution in Word and save it as a PDF file.
- You also can write it on any physical papers and scan them to a PDF file.
- If you don't have condition to scan, you still can take pictures by your smart phone and convert images to a PDF file by the online tool (https://imagetopdf.com).
- If you have multiple PDF files, please combine them to a PDF file by the online tool (https://www.pdfmerge.com) or (https://www.ilovepdf.com/merge_pdf).

Problem 1: Modular Arithmetic (10 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) $(893 \bmod 79)^4 \bmod 26$

Problem 2: Integer Representations and Modular Exponentiation Algorithom (20 points)

(a) [3 points] Convert the decimal expansion 100632 to a binary expansion.

(b) [3 points] Convert the binary expansion $(110100100010000)_2$ to decimal expansion.

(c) [3 points] Convert the octal expansion $2417)_8$ to a binary expansion.

(d) [3 points] Convert $(BADFACED)_{16}$ from its hexadecimal expansion to its binary expansion.

(e) [8 points] Use Modular Exponention Algorithm to find $123^{1001} \bmod 101$.

Problem 3: Primes and Greatest Common Divisors (20 points)

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

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

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

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

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

Problem 4: Solving Congruences and Chinese Reminder Theorem (10 points)

(a) [3 points] Show that 15 is an inverse of 7 modulo 26.

(d) [3 points] State the Chinese remainder theorem.

(c) [4 points] Find the solutions to the system $x \equiv 1 (\text{mod } 4)$, $x \equiv 2 (\text{mod } 5)$, and $x \equiv 3 (\text{mod } 7)$.

Problem 5: Computer Projects (40 points)

Write a program with any programming language you like to solve and answer the following problems. Please keep in mind that you should provide details to run your program and testing cases with necessary descriptions, as well as the complexity analysis, to make a solid solution.

(a) [10 points] Given a positive integer, find the prime factorization of this integer.

(b) [10 points] Given two positive integers, find their greatest common divisor using both prime fractorization and Euclidean algorithm, and then compare the corresponding running time.

(c) [10 points] Given the positive integers a, b, and m with $m > 1$, find $a^b \bmod m$ using modular exponention algorithm.

(d) [10 points] Given two integers L and R, find the count of numbers in the range $[L, R]$ (inclusive) having a prime number of set bits in their binary representation.

Recall that **the number of set bits** *an integer has is the number of* 1*s present when written in binary. For example,* 21 *written in binary is* 10101 *which has* 3 *set bits. Also,* 1 *is not a prime.*

Note: (1) L, R will be integers $L \leq R$ in the range $[1, 10^6]$; (2) $R - L$ will be at most 10000.

Example 1
Input: $L = 6$, $R = 10$
Output: 4
Explanation:
$6 \rightarrow 110$ (2 set bits, 2 is prime)
$7 \rightarrow 111$ (3 set bits, 3 is prime)
$9 \rightarrow 1001$ (2 set bits , 2 is prime)
$10 \rightarrow 1010$ (2 set bits , 2 is prime)

Example 2
Input: $L = 10$, $R = 15$
Output: 5
Explanation:
$10 \rightarrow 1010$ (2 set bits, 2 is prime)
$11 \rightarrow 1011$ (3 set bits, 3 is prime)
$12 \rightarrow 1100$ (2 set bits, 2 is prime)
$13 \rightarrow 1101$ (3 set bits, 3 is prime)
$14 \rightarrow 1110$ (3 set bits, 3 is prime)
$15 \rightarrow 1111$ (4 set bits, 4 is not prime)

[Optional Problem] (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 $x_{11} = x_1 + x_2 + \ldots + x_{10} \bmod 9$.

(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* $42 \cdot 58$.]