CS201: Discrete Mathematics (Fall 2024)
Written Assignment #3
(100 points maximum but 110 points in total)
Deadline: 11:59pm on Nov 8 (please submit to Blackboard)
PLAGIARISM WILL BE PUNISHED SEVERELY
Hint: Corollary 1 of Bézout's Theorem is heavily used in this assignment.

Q.1 (**5p**) Show that if a, b, and c are integers such that $ac \mid bc$, where $a \neq 0$ and $c \neq 0$, then $a \mid b$.

Q.2 (**5p**) Evaluate the following quantities:

(a) (**1p**) $-2024 \text{ div } 33$

(b) (**2p**) $(20234 - 2024) \bmod 25$

(c) (**2p**) $94232 \cdot 2982 \bmod 7$

Q.3 (**10p**) Integer representations.

(a) (**2p**) Convert $(11011)_2$ to its decimal expansion.

(b) (**2p**) Convert $(101100)_2$ to its octal expansion.

(c) (**3p**) Convert $(AE01F)_{16}$ to its binary expansion.

(d) (**3p**) Convert $(720235)_8$ to its hexadecimal expansion.

Q.4 (**5p**) Find the prime factorization of the following integers:

(a) (**2p**) 8085

(b) (**3p**) 12!

Q.5 (**20p**) The (extended) Euclidean algorithm.

(a) (**4p**) Use the Euclidean algorithm to find $\gcd(267, 79)$.

(b) (**4p**) Find Bézout coefficients of 267 and 79.

(c) (**2p**) Solve the linear congruence $267x \equiv 3 \pmod{79}$.

(d) (**6p**) Use the extended Euclidean algorithm (see page 286∼287 of the textbook) to express $\gcd(252, 356)$ as a linear combination of 252 and 356.

(e) (**4p**) Prove that the number of divisions required by the Euclidean algorithm to find $\gcd(a, b)$, where $a \geq b > 0$, is $O(\log b)$. (Hint: prove that the remainders r_i satisfy $r_{i+2} < r_i/2$.)

Q.6 (**5p**) Prove that if $c \mid ab$ then $c \mid a \cdot \gcd(b, c)$.

Q.7 (**10p**) In class, we already proved that "if $\gcd(a, m) = 1$ for positive integers a and m, then there exists an inverse of a modulo m". Now, show that the following statements are also true.

(a) (**5p**) Prove that the above inverse of a is *unique* modulo m. That is, suppose $\bar{a} \in \mathbf{Z}_m$ is an inverse of a modulo m, then every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.

(b) (**5p**) Prove that "if $\gcd(a, m) > 1$ for positive integers a and m, then a does *not* have an inverse modulo m".

Note that the above tells us that "for positive integers a and m, there exists an inverse of a modulo m if and only if $\gcd(a, m) = 1$".

Q.8 (**10p**) In class, we proved that one can use the Chinese remainder theorem to construct a solution of the system of linear congruences $\{x \equiv a_i \pmod{m_i}\}_{1 \le i \le n}$ where the moduli $m_1, m_2, \ldots, m_n$ are pairwise coprime integers greater than or equal to 2. Now, let us prove that the solution is *unique* modulo $m = m_1 m_2 \cdots m_n$.

(a) (**7p**) Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m}$, where $m = m_1 m_2 \cdots m_n$.

(b) (**3p**) Use (a) to complete the proof of uniqueness in the Chinese remainder theorem.

Q.9 (**10p**) We learned from class that a system of linear congruences can be solved by the Chinese remainder theorem. However, this requires all pairs of moduli be relatively prime. Now, let us solve this system of linear congruences: $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{35}$.

(a) (**5p**) Transform the above system of linear congruences into a new equivalent system that can be solved by the Chinese remainder theorem, i.e., the moduli for the new system are pairwise coprime. Explain your answer. (Hint: Do prime factorization of the moduli.)

(b) (**5p**) Find all solutions to the new system derived in (a).

Q.10 (**15p**) Let us prove Fermat's little theorem. Suppose p is prime and a is not divisible by p.

(a) (**5p**) Prove that *no* two of the integers $1 \cdot a, 2 \cdot a, \ldots, (p-1)a$ are congruent modulo p.

(b) (**5p**) Based on (a), prove that $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$.

(c) (**3p**) Based on (b) and $p \nmid (p-1)!$, prove that $a^{p-1} \equiv 1 \pmod{p}$.

(d) (**2p**) Based on (c), prove that $a^p \equiv a \pmod{p}$ holds for any integer a. (Note that a could be divisible by p.)

Q.11 (**5p**) Compute the following quantities:

(a) (**2p**) Use Fermat's little theorem to compute $5^{2023} \bmod 7$.

(b) (**3p**) Use Euler's theorem to compute $8^{2023} \bmod 15$.

Q.12 (**10p**) Consider the RSA encryption scheme. Let our public key be $(n, e) = (65, 7)$, and our private key be d. Answer the following questions and show your computation steps.

(a) (**3p**) What is the ciphertext C (i.e., the encryption) of the message $M = 8$?

(b) (**4p**) Find the decryption key d.

(c) (**3p**) Using d, run the RSA decryption of the above ciphertext C.