CS201: Discrete Math for Computer Science
2024 Spring Semester Written Assignment #3
Due: Apr. 15th, 2023

The assignment needs to be written in English. Assignments in any other language will get zero point. Any plagiarism behavior will lead to zero point.

Q. 1. Compute the following without calculator and explain your answer.

(1) $(33^{15} \mod 32)^3 \mod 15$

(2) $\gcd(210, 1638)$

(3) $34x \equiv 77 \pmod{89}$

(4) The last decimal digit of 3^{1000} (Hint: Fermat's little theorem)

Q. 2. Use extended Euclidean algorithm to express $\gcd(561, 234)$ as a linear combination of 561 and 234.

Q. 3. Let a, b, and c be integers. Suppose m is an integer greater than 1 and $ac \equiv bc \pmod{m}$. Prove $a \equiv b \pmod{m/\gcd(c, m)}$.

Q. 4. For two integers a, b, suppose that $\gcd(a, b) = 1$ and $b \geq a$. Prove that $\gcd(b + a, b - a) \leq 2$.

Q. 5. Given an integer a, we say that a number n passes the "Fermat primality test (for base a)" if $a^{n-1} \equiv 1 \pmod{n}$.

(a) For $a = 2$, does $n = 561$ pass the test?

(b) Did the test give the correct answer in this case?

Q. 6. Solve the following linear congruence equations.

(a) $778x \equiv 10 \pmod{379}$.

(b) $312x \equiv 3 \pmod{97}$.

Q. 7. Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

Q. 8. (a) Show that if n is an integer, then $n^2 \equiv 0$ or $1 \pmod{4}$.

(b) Use (a) to show that if m is a positive integer of the form $4k + 3$ for some nonnegative integer k, then m is not the sum of the squares of two integers.

Q. 9. Prove that if a and m are positive integers such that $\gcd(a, m) \neq 1$ then a does not have an inverse modulo m.

Q. 10. Find counterexamples to each of these statements about congruences.

(a) If $ac \equiv bc \pmod{m}$, where a, b, c, and m are integers with $m \geq 2$, then $a \equiv b \pmod{m}$.

(b) If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with c and d positive and $m \geq 2$, then $a^c \equiv b^d \pmod{m}$.

Q. 11. Show that we can easily factor n when we know that n is the product of two primes, p and q, and we know the value of $(p - 1)(q - 1)$.

Q. 12. Consider the RSA encryption method. Let our public key be $(n, e) = (65, 7)$, and our private key be d.

(a) What is the encryption $\hat{M}$ of a message $M = 8$?

(b) To decrypt, what value d do we need to use?

(c) Using d, run the RSA decryption method on $\hat{M}$.