CS215: Discrete Math (H)
2024 Fall Semester Written Assignment # 3
Due: Nov. 13th, 2024, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 8085

(b) 10!

Q.3 For three integers a, b, y, suppose that $\gcd(a, y) = d_1$ and $\gcd(b, y) = d_2$. Prove that

$$\gcd(\gcd(a, b), y) = \gcd(d_1, d_2).$$

Q.4 Prove the following statement. If $c|(a \cdot b)$, then $c|(a \cdot \gcd(b, c))$.

Q.5 Solve the following modular equation.

$$312x \equiv 3 \pmod{97}.$$

Q.6 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.7 Prove that if a and m are positive integer such that $\gcd(a, m) = 1$ then the function

$$f : \{0, \ldots, m-1\} \to \{0, \ldots, m-1\}$$

defined by

$$f(x) = (a \cdot x) \bmod m$$

is a bijection.

Q.8 Convert the decimal expansion of each of these integers to a binary expansion.
(a) 231 (b) 4532

Q.9 Let the coefficients of the polynomial $f(n) = a_0 + a_1 n + a_2 n^2 + \cdots + a_{t-1} n^{t-1} + n^t$ be integers. We now show that ***no*** non-constant polynomial can generate only prime numbers for integers n. In particular, let $c = f(0) = a_0$ be the constant term of f.

(1) Show that $f(cm)$ is a multiple of c for all $m \in \mathbb{Z}$.

(2) Show that if f is non-constant and $c > 1$, then as n ranges over the nonnegative integers $\mathbb{N}$, there are infinitely many $f(n) \in \mathbb{Z}$ that are not primes. [Hint: You may assume the fact that the magnitude of any non-constant polynomial $f(n)$ grows unboundedly as n grows.]

(3) Conclude that for every non-constant polynomial f there must be an $n \in \mathbb{N}$ such that $f(n)$ is not prime. [Hint: Only one case remains.]

Q.10 Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.

Q.11 Prove that there are infinitely many primes of the form $4k + 3$, where k is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes $q_1, q_2, \ldots, q_n$, and consider the number $4q_1 q_2 \cdots q_n - 1$.]

Q.12

(1) Show that if n is an integer then $n^2 \equiv 0$ or $1 \pmod 4$.

(2) 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.13

(a) State Fermat's little theorem.

(b) Show that Fermat's little theorem does not hold if p is not prime.

(c) Compute $302^{302} \pmod{11}$, $4762^{5367} \pmod{13}$, $2^{39674} \pmod{523}$.

Q.14 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 $m = m_1 m_2 \cdots m_n$.

Q.15 Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the methods of Chinese Remainder Theorem or back substitution.

Q.16 For a collection of balls, the number is not known. If we count them by 2's, we have 1 left over; by 3's, we have nothing left; by 4, we have 1 left over; by 5, we have 4 left over; by 6, we have 3 left over; by 7, we have nothing left; by 8, we have 1 left over; by 9, nothing is left. How many balls are there? Give the details of your calculation.

Q.17 Recall how the *linear congruential method* works in generating pseudorandom numbers: Initially, four parameters are chosen, i.e., the modulus m, the multiplier a, the increment c, and the seed x_0. Then a sequence of numbers $x_1, x_2, \ldots, x_n, \ldots$ are generated by the following congruence

$$x_{n+1} = (ax_n + c) \pmod m.$$

Suppose that we know the generated numbers are in the range $0, 1, \ldots, 10$, which means the modulus $m = 11$. By observing three consecutive numbers $7, 4, 6$, can you predict the next number? Explain your answer.

Q.18 Recall that Euler's totient function $\phi(n)$ counts the number of positive integers up to a given integer n that are coprime to n. Prove that for all integers $n \geq 3$, $\phi(n)$ is even.

Q.19 Recall the RSA public key cryptosystem: Bob posts a public key (n, e) and keeps a secret key d. When Alice wants to send a message $0 < M < n$ to Bob, she calculates $C = M^e \pmod n$ and sends C to Bob. Bob then decrypts this by calculating $C^d \pmod n$. In class we learnt that in order to make this scheme work, n, e, d must have special properties.

For each of the three public/secret key pairs listed below, answer whether it is a **valid** set of RSA public/secret key pairs (whether the pair satisfies the required properties), and explain your answer.

(a) $(n, e) = (91, 25)$, $d = 51$

(b) $(n, e) = (91, 25)$, $d = 49$

(c) $(n, e) = (84, 25)$, $d = 37$

Q.20 Consider the RSA system. Let (e, d) be a key pair for the RSA. Define

$$\lambda(n) = \mathrm{lcm}(p-1, q-1)$$

and compute $d' = e^{-1} \bmod \lambda(n)$. Will decryption using d' instead of d still work? (prove $C^{d'} \bmod n = M$)