**CS215: Discrete Math (H)**
**2025 Fall Semester Written Assignment # 3**
**Due: Nov. 10th, 2025, please submit at the beginning of class**

Q.1 What are the prime factorizations of

(1) 6560

(2) 12!

Q.2 Convert the decimal expansion of each of these integers to a binary expansion.
(a) 321 (b) 1023 (c) 100632

Q.3 For two integers $a, b$, prove that if $\gcd(a, b) = 1$, then

$$\gcd(b + a, b - a) \leq 2.$$

Q.4

(1) Give the prime factorization of 312.

(2) Use Euclidean algorithm to find $\gcd(312, 97)$.

(3) Find integers $s$ and $t$ such that $\gcd(312, 97) = 312s + 97t$.

(4) Solve the modular equation

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

Q.5 Suppose that $p, q$ and $r$ are distinct primes. Show that there exist integers $a, b$ and $c$, such that

$$a(pq) + b(qr) + c(rp) = 1.$$

Q.6 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.7 Prove that there are infinitely many primes of the form $6k + 5$.

Q.8 Let $a$ and $b$ be positive integers. Show that $\gcd(a,b) + \mathrm{lcm}(a,b) = a + b$ if and only if $a$ divides $b$, or $b$ divides $a$.

Q.9

(1) Show that there is no integer solution $x$ to the equation

$$x^2 \equiv 31 \pmod{36}.$$

(2) Find the integer solutions $x$ to the system of equations

$$\begin{cases} x^2 \equiv 10 \pmod{31}, \\ x^2 \equiv 30 \pmod{37}. \end{cases}$$

Q.10 Compute the following without calculator. You may find Fermat's little theorem useful for some of these.

(1) The last decimal digit of $3^{1000}$

(2) $3^{1000} \bmod 31$

(3) $3/16$ in $\mathbb{Z}_{31}$

Q.11 Show that if $a$ and $m$ are relatively prime positive integers, then the inverse of $a$ modulo $m$ is unique modulo $m$.

Q.12 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.13 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.14 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.15

(1) Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

(2) Use your results from part (a) and the Chinese remainder theorem to find $5^{2003} \bmod 1001$. (Note that $1001 = 7 \cdot 11 \cdot 13$.)

Q.16 Given an integer $a$, we say that a number $n$ passes the "Fermat primality test (for base $a$)" if $a^{n-1} \equiv 1 \pmod{n}$.

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

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

Q.17 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.18 Consider the RSA encryption method. Let our public key be $(n, e) = (65, 7)$, and our private key be $d$.

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

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

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

Q.19 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 $C^{d'} \bmod n = M$)