CS201: Discrete Math for Computer Science
2021 Fall Semester Written Assignment # 3
Due: Nov. 3rd, 2021, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 511

(b) 6560

(c) 12!

Q.2

(a) Use Euclidean algorithm to find $\gcd(561, 234)$.

(b) Find integers s and t such that $\gcd(561, 234) = 234s + 561t$.

Q.3 For two integers a, b, suppose that $\gcd(a, b) = 1$. Prove that

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

Q.4 Prove that for three integers a, b, c, if $c|(a \cdot b)$, then $c|(a \cdot \gcd(b, c))$.

Q.5

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

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

(c) Solve the modular equation

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

Q.6 Solve the following modular equations.

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

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

Q.7 Let a and b be positive integers. Show that $\gcd(a, b) + \operatorname{lcm}(a, b) = a + b$ if and only if a divides b, or b divides a.

Q.8 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.9

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

(b) 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.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 Convert the decimal expansion of each of these integers to a binary expansion.

(a) 321 (b) 1023 (c) 100632

Q.12

Convert the binary expansion of each of these integers to a octal expansion.

(a) $(1111\ 0111)_2$

(b) $(111\ 0111\ 0111\ 0111)_2$

Q.13 Show that $\log_2 3$ is an irrational number. Recall that an irrational number is a real number x cannot be written as the ratio of two integers.

Q.14

Prove that for every positive integer n, there are n consecutive composite integers.

Q.15 Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.

Q.16 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 $4q_1q_2 \cdots q_n - 1$.]

Q.17

(a) State Fermat's little theorem.

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

(c) Use Fermat's little theorem to compute $3^{302} \bmod 5$, $3^{302} \bmod 7$, and $3^{302} \bmod 11$.

(d) Use your results from part (c) and the Chinese remainder theorem to find $3^{302} \bmod 385$. (Note that $385 = 5 \cdot 7 \cdot 11$.)

Q.18 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 $m = m_1m_2 \cdots m_n$.

Q.19 Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the method of Chinese Remainder Theorem or back substitution.

Q.20 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.21 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 $\hat{M}$.