CS201: Discrete Math for Computer Science
2020 Fall Semester Written Assignment # 3
Due: Nov. 6th, 2020, please submit at the beginning of class

Q.1 What are the prime factorizations of

(a) 497

(b) 6560

(c) 10!

Q.2

(a) Use Euclidean algorithm to find $\gcd(267, 79)$.

(b) Find integers s and t such that $\gcd(267, 79) = 79s + 267t$.

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

(a) Give the prime factorization of 312.

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

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

(d) Solve the modular equation

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

Q.5

(a) State Fermat's little theorem.

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

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

Q.6 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.7 Solve the following modular equations.

(a) $267x \equiv 3 \pmod{79}$.

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

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

(a) 231 (b) 4532 (c) 97644

Q.10

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

(a) $(1010\ 1010\ 1010)_2$

(b) $(101\ 0101\ 0101\ 0101)_2$

Q.11 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.12

Show that if a, b, and m are integers such that $m \geq 2$ and $a \equiv b \bmod m$, then $\gcd(a, m) = \gcd(b, m)$.

Q.13 Show that if a and m are relatively prime positive integers, then the inverse of a modulo m is unique modulo m.

Q.14 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.15

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

(b) 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 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.17 Show that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime moduli is *unique* modulo the product of these moduli.

Q.18 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.19 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.20

Suppose that (n, e) is an RSA encryption key, with $n = pq$ where p and q are large primes and $\gcd(e, (p-1)(q-1)) = 1$. Furthermore, suppose that d is an inverse of e modulo $(p-1)(q-1)$. Suppose that $C \equiv M^e \pmod{pq}$. In the text we showed that RSA decryption, that is, the congruence $C^d \equiv M \pmod{pq}$ holds when $\gcd(M, pq) = 1$. Show that this decryption congruence also holds when $\gcd(M, pq) > 1$. [Hint: Use congruences modulo p and modulo q and apply the Chinese remainder theorem.]