CS201: Discrete Math for Computer Science
2022 Spring Semester Written Assignment # 3
Due: Apr. 6th, 2022, please submit one pdf file through Sakai
Please answer questions in English. Using any other language will lead to a zero point.

Q. 1. (5 points) Show that if $a \mid b$ and $b \mid a$, where a and b are integers, then $a = b$ or $a = -b$.

Q. 2. (5 points)

(a) Convert $(1768)_{10}$ to hexadecimal

(b) Convert $(10101)_2$ to octal

(c) Convert $(3B5A)_{16}$ to binary number

Q. 3. (5 points) What are the prime factorizations of

(a) 256

(b) 1890

(c) 5!

Q. 4. (5 points)

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

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

Q. 5. (5 points) 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. 6. (5 points) Suppose that $\gcd(b, a) = 1$. Prove that $\gcd(b+a, b-a) \leq 2$.

Q. 7. (10 points) Fermat's little theorem: If p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

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

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

Q. 8. (5 points) Solve the following modular equations.

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

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

Q. 9. (5 points) 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. 10. (5 points) Show that if n is an integer, then $n^2 \equiv 0 \text{ or } 1 \pmod{4}$.

Q. 11. (5 points) Use Q. 10 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. 12. (5 points) 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. 13. (5 points)

(a) Convert $(1768)_{10}$ to hexadecimal

(b) Convert $(10101)_2$ to octal

(c) Convert $(3B5A)_{16}$ to binary number

Q. 14. (5 points) 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. 15. (5 points) Solve the system of congruence $x \equiv 3 \pmod 6$ and $x \equiv 4 \pmod 7$ using the method of back substitution.

Q. 16. (10 points) 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. 17. (10 points) 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 lecture, 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.]