The Chinese University of Hong Kong, Shenzhen
School of Data Science

CSC 3001 · Assignment 3

Due: 23:59, November 8th, 2024

Instructions:

- Homework problems must be carefully and clearly answered to receive full credit. Complete sentences that establish a clear logical progression are highly recommended.
- You must independently complete each assignment.
- You must submit your assignment in Blackboard with all necessary supplemental material.
- Late submission will not be graded.

Question 1 (10 marks)

Please use the Euclid's GCD algorithm to calculate the greatest common divisor of 534 and 271.

Question 2 (10 marks)

For any integers a and b which at least one of them doesn't equal to 0, show that any common divisor of a and b divides $\gcd(a, b)$.

Question 3 (10 marks)

Show that $\gcd(ab, c) = \gcd(a, c)$ if $\gcd(b, c) = 1$.

Question 4 (10 marks)

Show that if $\gcd(a, b) = 1$, then $\gcd(ab, c) = \gcd(a, c)\gcd(b, c)$.

Question 5 (10 marks)

For every linear transformation $A : \mathbb{R}^2 \to \mathbb{R}^2$, $\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} X \\ Y \end{pmatrix}$ satisfied $a, b, c, d \in \mathbb{Z}$, prove that $\gcd(x, y) \mid \gcd(X, Y) \mid \det(A)\gcd(x, y)$ for any $x, y \in \mathbb{Z}$.

Question 6 (10 marks)

Find all solutions x, if they exist, to the system of equivalences:

$$\begin{aligned} 2x &\equiv 6 \pmod{14} \\ 3x &\equiv 9 \pmod{15} \\ 5x &\equiv 20 \pmod{60}. \end{aligned}$$

Question 7 (10 marks)

Prove the following statements:

1. If $ac \equiv bc \pmod{m}$, we have $a \equiv b \pmod{\frac{m}{\gcd(c,m)}}$;
2. Denote a' and b' as the inverse of $a \pmod{m}$ and $b \pmod{m}$. If $\gcd(a, m) = \gcd(b, m) = 1$, $a \equiv b \pmod{m}$ if and only if $a' \equiv b' \pmod{m}$.

Question 8 (10 marks)

Consider the Fibonacci sequence $\{F_n\}$, where $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for other n. Prove that $3 \mid F_n$ if and only if $4 \mid n$ for $n \in \mathbb{N}$.

Question 9 (10 marks)

For an arbitrary prime number $p \geq 5$, we have the inverse i' of $i \pmod{p}$ if $p \nmid i$. Prove that $\sum_{i=1}^{p-1} (i')^2 \equiv 0 \pmod{p}$.

Question 10 (10 marks)

p is prime and a and b are integers, prove $(a + b)^p \equiv a^p + b^p \pmod{p}$.