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.

Solution
$\gcd(534, 271) = \gcd(263, 271) = \gcd(263, 8) = \gcd(7, 8) = \gcd(7, 1) = 1$.

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 $\gcd(a, b)$.

Solution
If one of a and b equals to 0, $\gcd(a, b)$ is just the absolute value of the nonzero one of them, the common divisors of a and b are just the divisors of the nonzero one. So the statement is true.
If both a and b don't equal to 0, we assume d is a common divisor of a and b. Suppose that $\gcd(a, b) = \alpha a + \beta b$ where $\alpha, \beta \in \mathbb{Z}$, $d \mid a, d \mid b$, so $d \mid \gcd(a, b)$.
Then we conclude 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 $\gcd(b, c) = 1$.

Solution
Since $\gcd(a, c) \mid a, \gcd(a, c) \mid c$, we know $\gcd(a, c) \mid ab, \gcd(a, c) \mid c$, so $\gcd(a, c)$ is a positive common divisor of ab and c. $\gcd(a, c) \leq \gcd(ab, c)$.

Then since we know $\gcd(a,c) = \alpha_0 a + \beta_0 c$ and $1 = \gcd(b,c) = \alpha_1 b + \beta_1 c$ for some integers $\alpha_0, \alpha_1, \beta_0, \beta_1$, we have

$$\begin{aligned}\gcd(a,c) &= (\alpha_0 a + \beta_0 c)(\alpha_1 b + \beta_1 c)\\ &= \alpha_0\alpha_1 ab + (\alpha_0 a\beta_1 + \beta_0\alpha_1 b + \beta_0 c\beta_1)c.\end{aligned}$$

So from $\gcd(ab,c) = \text{spc}(ab,c)$, we have $\gcd(ab,c) \leq \gcd(a,c)$. Then we conclude that $\gcd(ab,c) = \gcd(a,c)$ if $\gcd(b,c) = 1$.

Question 4 (10 marks)

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

Solution
Since we have $\gcd(a,c) = m_0 a + n_0 c$ and $\gcd(b,c) = m_1 b + n_1 c$ for some integers m_0, m_1, n_0, n_1, we have

$$\gcd(a,c)\gcd(b,c) = (m_0 a + n_0 c)(m_1 b + n_1 c) = m_0 m_1 ab + (m_0 n_1 a + n_0 m_1 b + n_0 n_1 c)c$$

is a positive integer linear combination of ab and c, we know $\gcd(ab,c) \leq \gcd(a,c)\gcd(b,c)$.
Then for the reverse inequality, firstly we know $\gcd(a,c)\gcd(b,c) \mid ab$, then we want to prove that $\gcd(a,c)\gcd(b,c) \mid c$. Since $\gcd(a,b) = 1$, we know there is an integer linear combination $\alpha a + \beta b = 1$ and we have $\alpha ac + \beta bc = c$. Since $\gcd(a,c) \mid a$ and $\gcd(b,c) \mid c$, we have $\gcd(a,c)\gcd(b,c) \mid ac$. By similarity, $\gcd(a,c)\gcd(b,c) \mid bc$. So $\gcd(a,c)\gcd(b,c) \mid \alpha ac + \beta bc$ i.e. $\gcd(a,c)\gcd(b,c) \mid c$. So $\gcd(a,c)\gcd(b,c)$ is a common divisor of ab and c, so $\gcd(a,c)\gcd(b,c) \leq \gcd(ab,c)$.
We conclude 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 $x, y \in \mathbb{Z}$.

Solution
Since both X and Y are integer linear combination of x and y, we know $\gcd(x,y) \mid \gcd(X,Y)$ from the question 2.
Then we suppose $\gcd(x,y) = mx + ny$ which is an integer linear combination of x and y. We have

$$\begin{aligned}&(md - nc)X + (an - mb)Y\\ =&(md - nc)(ax + by) + (an - mb)(cx + dy)\\ =&(ad - bc)mx + (ad - bc)ny\\ =&(ad - bc)(mx + ny)\\ =&det(A)\gcd(x,y).\end{aligned}$$

Since both $md - nc$ and $an - mb$ are integers, we know $\gcd(X,Y) \mid det(A)\gcd(x,y)$.

Question 6 (10 marks)

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

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

Solution

Since $\gcd(2,14)=2 \mid 6, \gcd(3,15)=3 \mid 9, \gcd(5,60)=5 \mid 20$, every single equation has solutions. Then we transform the system as

$$\begin{aligned} x &\equiv 3 \pmod{7} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{12}. \end{aligned}$$

Since each two numbers of $7, 5, 12$ are coprime, we can use Chinese remainder theorem to solve the system. We assume $x = 60a + 84b + 35c$ and we have

$$\begin{aligned} 60a &\equiv 3 \pmod{7} \\ 84b &\equiv 3 \pmod{5} \\ 35c &\equiv 4 \pmod{12}. \end{aligned}$$

We further reduce the coefficients as

$$\begin{aligned} 4a &\equiv 3 \pmod{7} \\ 4b &\equiv 3 \pmod{5} \\ 11c &\equiv 4 \pmod{12}. \end{aligned}$$

Then from the multiplicative inverse, we have

$$\begin{aligned} a &\equiv 6 \pmod{7} \\ b &\equiv 2 \pmod{5} \\ c &\equiv 8 \pmod{12}. \end{aligned}$$

So we have $x \equiv 60 \times 6 + 84 \times 2 + 35 \times 8 \pmod{420}$, we arrange it as $x \equiv 388 \pmod{420}$.

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 $a' \equiv b' \pmod{m}$.

Solution

1. Since $m \mid c(a-b)$, $\frac{m}{\gcd(c,m)} \mid \frac{c}{\gcd(c,m)}(a-b)$. $\gcd(\frac{m}{\gcd(c,m)}, \frac{c}{\gcd(c,m)}) = 1$, so we have $\frac{m}{\gcd(c,m)} \mid (a-b)$.

2. If $a \equiv b \pmod{m}$, we have $a'a \equiv a'b \pmod{m}$, i.e. $1 \equiv a'b \pmod{m}$. Since $1 \equiv b'b \pmod{m}$, we have $m \mid (a'-b')b$. Since $\gcd(m,b) = 1$, $m \mid a'-b'$. So $a' \equiv b' \pmod{m}$.

   By the same method, we can prove the reverse argument and prove the whole argument.

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 $n \in \mathbb{N}$.

Solution

$$F_0 \equiv 0 \pmod{3}; F_1 \equiv 1 \pmod{3}; F_2 \equiv 1 \pmod{3}; F_3 \equiv 2 \pmod{3};$$
$$F_4 \equiv 0 \pmod{3}; F_5 \equiv 2 \pmod{3}; F_6 \equiv 2 \pmod{3}; F_7 \equiv 1 \pmod{3} \ldots$$

We can prove that for arbitrary $i \in \mathbb{Z}^*$, we have

$$F_{8i-8} \equiv 0 \pmod{3}; F_{8i-7} \equiv 1 \pmod{3}; F_{8i-6} \equiv 1 \pmod{3}; F_{8i-5} \equiv 2 \pmod{3};$$
$$F_{8i-4} \equiv 0 \pmod{3}; F_{8i-3} \equiv 2 \pmod{3}; F_{8i-2} \equiv 2 \pmod{3}; F_{8i-1} \equiv 1 \pmod{3} \ldots$$

The $i = 1$ case is true as above. We assume when $i = k$ the statement is true, we prove for $i = k+1$ case.
Since $F_{8i-8} = F_{8(i-1)-1} + F_{8(i-1)-2}$ and $F_{8(i-1)-1} \equiv 1 \pmod{3}, F_{8(i-1)-2} \equiv 2 \pmod{3}$, we have $F_{8(i-1)-1} + F_{8(i-1)-2} \equiv 1+2 \pmod{3}$, i.e. $F_{8i-8} \equiv 0 \pmod{3}$. Then we following the same process, we can prove that $i = k+1$ case is true.
Then we observe that for every $k \in \mathbb{N}, F_{4k} \equiv 0 \pmod{3}$, we conclude 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 $\sum_{i=1}^{p-1} (i')^2 \equiv 0 \pmod{p}$.

Solution
We know all $i \in \{1, 2, \ldots, p-1\}$ are different respect to $i \pmod{p}$ and the inverse of i is congruent to some unique $j \in \{1, 2, \ldots, p-1\}$ modulo p. So we have

$$\sum_{i=1}^{p-1} (i')^2 \equiv \sum_{i=1}^{p-1} i^2 = \frac{1}{6} p(p-1)(2p-1) \equiv 0 \pmod{p}.$$

Question 10 (10 marks)

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

Solution

We first prove that for any integer k, $k^p \equiv k \pmod{p}$. If $p \mid k$, we have $k^p \equiv k \equiv 0 \pmod{p}$. If $p \nmid k$, we know $k \equiv i \pmod{p}$ for some $i \in \{1, 2, \ldots, p-1\}$. Then from Fermat's little theorem we know

$$k^p \equiv i^p \equiv i \equiv k \pmod{p}.$$

With the conclusion above, we have

$$(a+b)^p \equiv a + b \equiv a^p + b^p \pmod{p}.$$

So we prove the statement.