**COMP 2711 Discrete Mathematical Tools for Computer Science**
**2022 Fall Semester – Tutorial 7**

**Question 1:** Find the integer $a$ such that

(a) $a \equiv -15 \pmod{27}$ and $-26 \leq a \leq 0$.
(b) $a \equiv 24 \pmod{31}$ and $-15 \leq a \leq 15$.
(c) $a \equiv 99 \pmod{41}$ and $100 \leq a \leq 140$.

**Solution :** (a) $-15$.
(b) $24 - 31 = -7$.
(c) $99 + 41 = 140$.

**Question 2:** Use the extended Euclidean algorithm to express $\gcd(26, 91)$ as a linear combination of 26 and 91.

**Solution :** First find $\gcd(26, 91)$:

$$\begin{aligned} 91 &= 26 \cdot 3 + 13 \\ 26 &= 13 \cdot 2 + 0 \end{aligned}$$

So, $\gcd(26, 91) = 13$.

Rewriting:

$$13 = 91 - 26 \cdot 3$$

So, $(-3) \cdot 26 + 1 \cdot 91 = 13$

**Question 3:** Prove that if $a - c \mid ab + cd$ then $a - c \mid ad + bc$

**Solution :** We know that $a - c \mid a - c \implies a - c \mid (a - c)(b - d) \implies a - c \mid ab + cd - bc - ad \implies a - c \mid (ab + cd) - (ad + bc)$.
Also based on the question we know that $a - c \mid ab + cd$. So we conclude that $a - c \mid ad + bc$

**Question 4:** assume $a, b$ are non-zero integers. Prove that:

(a) $gcd(a, b) = gcd(a, b + ka)$ for any $k \in \mathbb{Z}$.
(b) $gcd(na, nb) = n \cdot gcd(a, b)$ for any $n \in \mathbb{N}$.

**Solution :** (a) Solution 1: Based on Euclidean algorithm we have $gcd(b + ka, a) = gcd(a, b)$.

Solution 2: Assume $d = gcd(a, b)$ and $d' = gcd(a, b + ka)$. We know $d \mid a$ and $d \mid a + kb$ (why?). So $d \mid d'$. On the other hand $d' \mid a \implies d' \mid ka$. We Also know $d' \mid ka + b$. So this implies that $d' \mid (b + ka) - ka \implies d' \mid b$. Thus $d' | d$. So $d = d'$.

(b) Assume $d = gcd(a, b)$ and $d' = gcd(an, bn)$ . This means $d \mid a \implies dn \mid an$ and also $d \mid b \implies dn \mid bn$. These two implies that $dn \mid gcd(an, bn)$. This implies that $d' = dnc$ for some integer c.

We also know that $d' \mid na \implies dnc \mid na \implies dc \mid a$ and similarly we can show $dc \mid b$. This proves $dc \mid gcd(a, b) \implies dc \mid d \implies c = 1$.
So $gcd(an, bn) = d' = ndc = nd = n \cdot gcd(a, b)$

**Question 5:** Prove that the following fraction can not be simplified for any $n \in N$.

$$\frac{21n + 4}{14n + 3}$$

**Solution :** **Solution 1:** Based on Euclidean algorithm we have $gcd(21n+4, 14n+3) = gcd(14n + 3, 7n + 1) = gcd(7n + 1, 1) = 1$.

**Solution 2:** Assume $d$ is their $gcd$. $d \mid 21n + 4 \implies d \mid 42n + 8$.
Also $d \mid 14n + 3 \implies d \mid 42n + 9$

So $d \mid (42n + 9) - (42n + 8) \implies d \mid 1$. The only possible value for $d$ is 1 which means they are co-prime with each other. So this fraction can not be simplified.

**Question 6:**

(a) Prove that $gcd(n, n + 1) = 1$ for any natural number $n$

(b) Prove that there are infinitely many prime numbers. (Hint: Use part a)

**Solution :**

(a) Let us assume $d = gcd(n, n+1)$. This means $d \mid n$ and $d \mid n+1$. This implies $d \mid (n + 1) - n \implies d \mid 1$. which means $d = 1$.

(b) Assume that there are only finitely many prime numbers $p_1, p_2, ..., p_k$. Let $n = p_1 \cdot p_2 \cdot ... \cdot p_k$. Also assume that $N = n + 1$. We know that $gcd(n, n + 1) = 1$. If $N$ is prime then this is in contradiction with our assumption. Because $N$ is bigger than the biggest prime number $p_k$. If $N$ is not prime then it means that it has prime factors which are not in $p_1, p_2, ..., p_k$. Because their gcd is 1. So this also contradicts our assumption because we assumed that $p_1, p_2, ..., p_k$ contains all the possible prime values.