MATH1061
Discrete Mathematics I

Problem Set 2

Michael Kasumagic, sID#: 44302669

Due: 5pm, 6^{th} of September, 2024

Question 1: *(10 marks)*

Prove the following statements:

(a) The sum of every five consecutive integers is always divisible by 5.

(b) Suppose n is an odd integer. The sum of every n consecutive integers is always divisible by n.

Solution: (a)

Proof. We can express five consecutive integers as follows:

$$i_0, i_1, i_2, i_3, i_4,$$

where $i_0, a \in \mathbb{Z}$ and $i_a = i_0 + a$.
Then, the sum of five consecutive integers can be expressed

$$\begin{aligned} i_0 + i_1 + i_2 + i_3 + i_4 &= i_0 + i_0 + 1 + i_0 + 2 + i_0 + 3 + i_0 + 4 \\ &= 5i_0 + 10 \\ &= 5(i_0 + 2) \\ \therefore i_0 + i_1 + i_2 + i_3 + i_4 &= 5k, \quad k \in \mathbb{Z} \\ &\implies 5 \mid i_0 + i_1 + i_2 + i_3 + i_4 \end{aligned}$$

So, the sum of any 5 consecutive integers is always divisible by 5. □

Solution: (b)

Proof. We can express n consecutive integers, where n is an odd integer, as follows:

$$i_0, i_1, i_2, \ldots, i_{n-2}, i_{n-1}, i_n,$$

where $i_0, a, j \in \mathbb{Z},\ i_a = i_0 + a$, and $n = 2j + 1$

$$\begin{aligned} i_0 + i_1 + i_2 + \cdots + i_{n-2} + i_{n-1} + i_n &= i_0 + i_0 + 1 + i_0 + 2 + \cdots + i_0 + n - 2 + i_0 + n - 1 + i_0 + n \\ &= ni_0 + (1 + 2 + 3 \cdots + n - 2 + n - 1 + n) \\ &= ni_0 + \sum_{a=1}^{n} a \end{aligned}$$

We can apply Gauß's formula for the sum of consecutive natural numbers,

$$\begin{aligned} &= ni_0 + \frac{n(n+1)}{2} \\ &= n\left(i_0 + \frac{n+1}{2}\right) \end{aligned}$$

$$\begin{aligned} \therefore i_0 + i_1 + i_2 + \cdots + i_{n-2} + i_{n-1} + i_n &= nk, \quad k \in \mathbb{Z} \\ &\implies n \mid i_0 + i_1 + i_2 + \cdots + i_{n-2} + i_{n-1} + i_n \end{aligned}$$

So, the sum of any n consecutive integers, where n is odd, is always divisible by 5. □

Question 2: (*5 marks*)

(a) Compute the following quantities

$$\lfloor 3.6 \rfloor, \qquad \lceil \pi \rceil, \qquad \lceil e \rceil, \qquad \lceil e + 0.5 \rceil$$

(b) Prove or disprove the following statements: for all numbers x:

$$\lceil x + 0.5 \rceil = \lceil x \rceil + 1$$

Solution: (a)

$$\begin{aligned} \lfloor 3.6 \rfloor &= 3 \\ \lceil \pi \rceil &= \lceil 3.1415\ldots \rceil = 4 \\ \lceil e \rceil &= \lceil 2.7182\ldots \rceil = 3 \\ \lceil e + 0.5 \rceil &= \lceil 2.7182\cdots + 0.5 \rceil = \lceil 3.2182\ldots \rceil = 4 \end{aligned}$$

Solution: (b)

Proof. Take $x = 0.1$.

$$\lceil x + 0.5 \rceil = \lceil 0.1 + 0.5 \rceil = \lceil 0.6 \rceil = 1 \neq 2 = 1 + 1 = \lceil 0.1 \rceil + 1 = \lceil x \rceil + 1$$

Therefore, for all $x \in \mathbb{R}$, $\lceil x + 0.5 \rceil = \lceil x \rceil + 1$ is not true. □

For the sake of interest, let's examine the expressions and see under what circumstances they are equal or not.

Proof. In general, let's think of the number x as being equal to $n+r$, where n is an integer component, and r is the real, decimal component. For example, $\pi = n + r$, where $n = 3$ and $r = 0.1415\ldots$. By definition, $0 \leq r < 1$. With all this in mind, we can can consider

$$\lceil x + 0.5 \rceil = \lceil n + r + 0.5 \rceil$$

This allows us to consider two cases,
Case 1: $0 \leq r \leq 0.5$

$$\begin{aligned} n < n + r + 0.5 &\leq n + 1 \\ \therefore \lceil n + r + 0.5 \rceil &= n + 1 \\ n \leq n + r &\leq n + 1 \\ \therefore \lceil n + r \rceil + 1 &= n + 1 + 1 \end{aligned} \tag{!!}$$

Case 2: $0.5 < r < 1$

$$\begin{aligned} n + 1 < n + r + 0.5 &< n + 1.5 \\ \therefore \lceil n + r + 0.5 \rceil &= n + 2 \\ n < n + r &< n + 1 \\ \therefore \lceil n + r \rceil + 1 &= n + 1 + 1 \end{aligned}$$

Therefore, for $x \in \mathbb{R} : x = n + r,\ n \in \mathbb{Z}, r \in \mathbb{R}$ if $0.5 < r < 1$ then $\lceil x + 0.5 \rceil = \lceil x \rceil + 1$. However, if $0 \leq r \leq 0.5$ then $\lceil x + 0.5 \rceil \neq \lceil x \rceil + 1$ (see the (!!) tag).
Which means the given statement, $\forall x \in \mathbb{R}, \lceil x + 0.5 \rceil = \lceil x \rceil + 1$ is false. □

Question 3: *(10 marks)*

(a) Use the definition, prove or disprove

$$3 \equiv -4 \bmod 7$$

(b) Use the definition, prove or disprove: for all integers x,

$$2x \equiv -14x \bmod 8$$

(c) Prove or disprove the following statement: Suppose a, b, c, d are positive integers, $ac \equiv bc \bmod d$, then

$$a \equiv b \bmod d$$

(d) Prove or disprove the following statement: Suppose a, b, c, d are positive integers, $ac \equiv bc \bmod d$ and $\gcd(c, d) = 1$, then

$$a \equiv b \bmod d$$

(Hint: you may use a fact we mentioned in Lecture 12.)

Solution: (a)

Proof. We'll use the definition,

$$\begin{aligned} 3 \equiv -4 \bmod 7 &\iff 7 \mid (3 - (-4)) \\ &\iff 7 \mid 7 \equiv \text{True} \end{aligned}$$

Therefore, by biconditional logical, $3 \equiv -4 \bmod 7$ is also true. □

Solution: (b)

Proof. Using the definition, suppose $x \in \mathbb{Z}$,

$$\begin{aligned} 2x \equiv -14x \bmod 8 &\iff 8 \mid (2x - (-14x)) \\ &\iff 8 \mid 16x \\ &\iff 8 \mid 8(2x) \equiv \text{True}. \end{aligned}$$

Therefore, by biconditional logical, $2x \equiv -14x \bmod 8, \forall x \in \mathbb{Z}$ □

Solution: (c) I will disprove this by giving a counter example.

Proof. Suppose $a = 1, b = 2, c = 3, d = 3$,

$$\begin{aligned} ac \equiv bc \bmod d &\iff 3 \equiv 6 \bmod 3 \\ &\iff 3 \mid (3 - 6) \\ &\iff 3 \mid (-3) \\ &\iff 3 \mid 3(-1) \equiv \text{True}. \end{aligned}$$

Therefore, by biconditional logic, $ac \equiv bc \bmod d$.
We expect $a, b, c, d \in \mathbb{N}, ac \equiv bc \bmod d$ to imply that $a \equiv b \bmod d$, however,

$$\begin{aligned} a \equiv b \bmod d &\iff 1 \equiv 2 \bmod 3 \\ &\iff 3 \mid (1 - 2) \end{aligned}$$

$$
\begin{aligned}
&\iff 3 \mid (-1) \\
&\iff 3 \mid -1 \equiv \text{False} && ※
\end{aligned}
$$

This counter example gives rise to a contradiction, therefore the statement that, given $a, b, c, d \in \mathbb{N}, ac \equiv bc \bmod d$ then $a \equiv b \bmod d$ is false. □

Solution: (d)

Proof. Suppose $a, b, c, d \in \mathbb{N}$, $ac \equiv bc \bmod d$ and $\gcd(c, d) = 1 \implies c$ and d are co-prime, sharing no common factors.

$$
\begin{aligned}
ac \equiv bc \bmod d &\iff d \mid (ac - bc) \\
&\iff d \mid c(a - b)
\end{aligned}
$$

Since d and c are co-prime, $d \nmid c$.
Therefore, $d \mid (a - b)$

$$a \equiv b \bmod d \iff d \mid (a - b) \equiv \text{True}.$$

Therefore, by biconditional logic, $a \equiv b \bmod d$.
Thus, we can conclude that, given $a, b, c, d \in \mathbb{N}, ac \equiv bc \bmod d, \gcd(c, d) = 1$ then $a \equiv b \bmod d$. □

Question 4: *(5 marks)*

Use the Euclidean algorithm to compute

$$\gcd(101, 24)$$

Solution:

$$\begin{aligned}
& \gcd(101, 24) & \implies & \quad 101 & = & \quad 24 \cdot 4 + 5 \\
= \; & \gcd(24, 5) & \implies & \quad 24 & = & \quad 5 \cdot 4 + 4 \\
= \; & \gcd(5, 4) & \implies & \quad 5 & = & \quad 4 \cdot 1 + 1 \\
= \; & \gcd(4, 1) & \implies & \quad 4 & = & \quad 1 \cdot 4 + 0 \\
= \; & \gcd(1, 0) = 1 & & & &
\end{aligned}$$

$$\therefore \gcd(101, 24) = 1$$

Question 5: (*10 marks*)

The least common multiple of the integers a, b, denoted as lcm(a, b), is defined as the smallest positive integer which is divisible by both a and b.
Let $a = 2^7 \cdot 3^2 \cdot 5^1$ and $b = 2^3 \cdot 3^3 \cdot 7^1$.

(a) Compute $\gcd(a, b)$.

(b) Compute $\mathrm{lcm}(a, b)$.

(c) Verify that $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$.

(d) Can you prove the statement $\gcd(a, b) \cdot \mathrm{lcm}(a, b) = ab$ for arbitrary positive integers a and b? (Hint: use the prime factorisation.)

Solution: (a)
The greatest common divisor of a and b is the largest $n \in \mathbb{N}$ such that $n \mid a$ and $n \mid b$. In other words, there exists $k, l \in \mathbb{Z}$ such that

$$a = kn, \qquad b = ln$$

Rearranging we can see that $n = a/k = b/l$. If we apply the Fundamental Theorem of Arthimentic, $a = 2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} \ldots$, $b = 2^{y_1} \cdot 3^{y_2} \cdot 5^{y_3} \ldots$, and consider that k and l must cancel these factors of a and b, such that the results of those divisions is equal, we can see that

$$n = 2^{\min\{x_1,y_1\}} \cdot 3^{\min\{x_2,y_2\}} \cdot 5^{\min\{x_3,y_3\}} \cdot \ldots .$$

We've seen this simply by considering the definition of $\gcd(a, b)$. In this specific example,

$$\begin{aligned}
\gcd\left(2^7 \cdot 3^2 \cdot 5^1, b = 2^3 \cdot 3^3 \cdot 7^1\right) &= n \\
n = \frac{2^7 \cdot 3^2 \cdot 5^1}{2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot 7^{k_4}} &= \frac{2^3 \cdot 3^3 \cdot 7^1}{2^{l_1} \cdot 3^{l_2} \cdot 5^{l_3} \cdot 7^{l_4}} \\
k_1 = 7 - 3 \quad & l_1 = 0 \\
k_2 = 0 \quad & l_2 = 3 - 2 \\
k_3 = 1 \quad & l_3 = 0 \\
k_4 = 0 \quad & l_4 = 1 \\
n = \frac{2^7 \cdot 3^2 \cdot 5^1}{2^4 \cdot 3^0 \cdot 5^1 \cdot 7^0} &= \frac{2^3 \cdot 3^3 \cdot 7^1}{2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1} \\
\therefore n = 2^3 \cdot 3^2 \cdot 5^0 &= 2^3 \cdot 3^2 \cdot 7^0
\end{aligned}$$

Therefore, given the prime factorisation of a and b, $\gcd(a, b) = 2^3 \cdot 3^2$.

Solution: (b)
The least common multiple of a and b is, effectively, the smallest number we can construct using all the prime factors of a and b. In other words, $\mathrm{lcm}(a, b) = n$, where n is the smallest natural number such that $n \mid a$ and $n \mid b$. From this we can can conclude that there exist $k, l \in \mathbb{Z}$ such that

$$n = ka, \qquad n = lb,$$

and n is as minimised. We can see that $ka = lb$. If we apply the Fundamental Theorem of Arthimentic, $a = 2^{x_1} \cdot 3^{x_2} \cdot 5^{x_3} \ldots$, $b = 2^{y_1} \cdot 3^{y_2} \cdot 5^{y_3} \ldots$, and consider that k and l must eqaulise the equation, we can see that

$$n = 2^{\max\{x_1,y_1\}} \cdot 3^{\max\{x_2,y_2\}} \cdot 5^{\max\{x_3,y_3\}} \cdot \ldots$$

In this specific example,

$$\operatorname{lcm}\left(2^7 \cdot 3^2 \cdot 5^1, b = 2^3 \cdot 3^3 \cdot 7^1\right) = n$$
$$n = 2^7 \cdot 3^2 \cdot 5^1 \left(2^{k_1} \cdot 3^{k_2} \cdot 5^{k_3} \cdot 7^{k_4}\right) = 2^3 \cdot 3^3 \cdot 7^1 \left(2^{l_1} \cdot 3^{l_2} \cdot 5^{l_3} \cdot 7^{l_4}\right)$$
$$\begin{array}{ll} k_1 = 0 & l_1 = 7 - 3 \\ k_2 = 3 - 2 & l_2 = 0 \\ k_3 = 0 & l_3 = 1 - 0 \\ k_4 = 1 - 0 & l_4 = 0 \end{array}$$
$$n = 2^7 \cdot 3^2 \cdot 5^1 \left(2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1\right) = 2^3 \cdot 3^3 \cdot 7^1 \left(2^4 \cdot 3^0 \cdot 5^1 \cdot 7^0\right)$$
$$\therefore n = 2^7 \cdot 3^3 \cdot 5^1 \cdot 7^1 = 2^7 \cdot 3^3 \cdot 5^1 \cdot 7^1$$

Therefore, given the prime factorisation of a and b, $\operatorname{lcm}(a, b) = 2^7 \cdot 3^3 \cdot 5^1 \cdot 7^1$.

Solution: (c)
We've established that

$$a = 2^7 \cdot 3^2 \cdot 5^1, \qquad b = 2^3 \cdot 3^3 \cdot 7^1$$
$$\gcd(a, b) = 2^3 \cdot 3^2$$
$$\operatorname{lcm}(a, b) = 2^7 \cdot 3^3 \cdot 5^1 \cdot 7^1$$

We seek to show that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$.
Let's compute the LHS

$$\begin{aligned} \gcd(a, b) \cdot \operatorname{lcm}(a, b) &= 2^3 \cdot 3^2 \cdot 2^7 \cdot 3^3 \cdot 5^1 \cdot 7^1 \\ &= 2^{3+7} \cdot 3^{2+3} \cdot 5^{0+1} \cdot 7^{0+1} \\ &= 2^{10} \cdot 3^5 \cdot 5^1 \cdot 7^1 \end{aligned}$$

Now let's compute the RHS.

$$\begin{aligned} 2^7 \cdot 3^2 \cdot 5^1 \cdot 2^3 \cdot 3^3 \cdot 7^1 &= 2^{7+3} \cdot 3^{2+3} \cdot 5^{1+0} \cdot 7^{0+1} \\ &= 2^{10} \cdot 3^5 \cdot 5^1 \cdot 7^1 \end{aligned}$$

Therefore, LHS = RHS. Therefore, for $a = 2^7 \cdot 3^2 \cdot 5^1$ and $b = 2^3 \cdot 3^3 \cdot 7^1$, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = a \cdot b$.

Solution: (d)

Proof. As previously discussed, we can apply the Fundamental Theorem of Arthimentic to two natural numbers $a, b \in \mathbb{N}, a = p_1^{x_1} \cdot p_2^{x_2} \cdot p_3^{x_3} \ldots,\ b = p_1^{y_1} \cdot p_2^{y_2} \cdot p_3^{y_3} \ldots$, where p_i is the i-th prime number. The greatest common divisor of a and b is

$$\gcd(a, b) = p_1^{\min\{x_1, y_1\}} \cdot p_2^{\min\{x_2, y_2\}} \cdot p_3^{\min\{x_3, y_3\}} \cdots = \prod_{i=1}^{\infty} p_i^{\min\{x_i, y_i\}}$$

The least common multiple of a and b is

$$\operatorname{lcm}(a, b) = p_1^{\max\{x_1, y_1\}} \cdot p_2^{\max\{x_2, y_2\}} \cdot p_3^{\max\{x_3, y_3\}} \cdots = \prod_{i=1}^{\infty} p_i^{\max\{x_i, y_i\}}$$

We seek to prove that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.
Let's compute the LHS, $\gcd(a, b) \cdot \operatorname{lcm}(a, b)$,

$$\prod_{i=1}^{\infty} p_i^{\min\{x_i, y_i\}} \cdot \prod_{i=1}^{\infty} p_i^{\max\{x_i, y_i\}} = \prod_{i=1}^{\infty} \left(p_i^{\min\{x_i, y_i\}} \cdot p_i^{\max\{x_i, y_i\}}\right) = \prod_{i=1}^{\infty} p_i^{\min\{x_i, y_i\} + \max\{x_i, y_i\}}$$

Let's consider $\min\{x_i, y_i\} + \max\{x_i, y_i\}$
$\forall i$, there are 3 cases: $x_i < y_i$, $x_i = y_i$ and $x_i > y_i$.
Case 1, $x_i < y_i$:

$$\min\{x_i, y_i\} + \max\{x_i, y_i\} = x_i + y_i$$

Case 2, $x_i > y_i$:

$$\min\{x_i, y_i\} + \max\{x_i, y_i\} = y_i + x_i = x_i + y_i$$

Case 3, $x_i = y_i$:

$$\min\{x_i, y_i\} + \max\{x_i, y_i\} = y_i + x_i = x_i + x_i = y_i + y_i = x_i + y_i$$

All three cases are equal, so we can conclude that $\forall i, \min\{x_i, y_i\} + \max\{x_i, y_i\} = x_i + y_i$.

$$\therefore LHS = \gcd(a, b) \cdot \operatorname{lcm}(a, b) = \prod_{i=1}^{\infty} p_i^{x_i + y_i}$$

Let's now compute the RHS, ab,

$$p_1^{x_1} \cdot p_2^{x_2} \cdot p_3^{x_3} \ldots \cdot p_1^{y_1} \cdot p_2^{y_2} \cdot p_3^{y_3} \cdots = \prod_{i=1}^{\infty} p_i^{x_i} \cdot \prod_{i=1}^{\infty} p_i^{y_i} = \prod_{i=1}^{\infty} (p_i^{x_i} \cdot p_i^{y_i}) = \prod_{i=1}^{\infty} p_i^{x_i + y_i}$$

Therefore, LHS = RHS

Given two arbitrary integers, a and b, we can apply the Fundamental Theorem of Arthimentic to them, and use their prime factorisations and the definitions of $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ to conclude that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ $\square$

Question 6: *(10 marks)*

A sequence is defined recursively as:

$$a_0 = 1, \qquad a_1 = 2,$$
$$a_n = 4a_{n-1} - 3a_{n-2}, \qquad n \geq 2.$$

Prove the formula

$$a_n = \frac{3^n + 1}{2}$$

Solution:

Proof. We will use the principle of strong mathematical induction to prove the formula. Let $P(n)$ be the predicate "$a_n = (3^n + 1)/2$." Let's consider the first 2 terms of the sequence

n	0	1
a_n	1	2
$\frac{3^n+1}{2}$	$\frac{3^0+1}{2} = 1$	$\frac{3^1+1}{2} = 2$

Basis Step: P(0) and P(1) are True. We've proved this in the above table.
Inductive Hypothesis: Suppose that, for some integer $k : 1 \leq k \leq n$, $P(0)$, $P(1)$, $P(2)$, $\ldots$, $P(k)$ are true.
Inductive Step: We seek to prove $P(n+1)$.

$$a_{n+1} = 4a_n - 3a_{n-1}$$

From the inductive step, $P(n)$ and $P(n-1)$ are true.

$$\begin{aligned}
\therefore a_{n+1} &= 4\frac{3^n+1}{2} - 3\frac{3^{n-1}+1}{2} \\
&= 4\frac{3^n+1}{2} - \frac{3^n+1}{2} \\
&= \frac{3^n+1}{2}(4-1) \\
&= \frac{3^n+1}{2}(3) \\
&= \frac{3^{n+1}+1}{2}
\end{aligned}$$

$P(n+1)$ is true
Therefore, by the principle of strong mathematical induction, it follows that $P(n)$ is true for all integers, $n \geq 0$. □