Professor Shanta Laishram
Lodha Genius Programme 2025

Number Theory

Problem Set 1

Collaborators: Vishnu Varadrajan **Name:** Anwesha Ghosh

Problem 1

For a positive integer n, show that:

(i) $1 \cdot 2 + 2 \cdot 5 + \ldots + n \cdot (3n-1) = n^2(n+1)$

(ii) $1^2 + 3^2 + 5^2 + \ldots + (2n-1)^2 = \frac{n(4n^2-1)}{3}$

Solution

(i) We will prove the statement by induction on n.

Proof:

Base Case: For $n = 1$,

LHS:

$$1 \cdot 2 = 2$$

RHS:

$$1^2(1+1) = 1^2 \cdot 2 = 2$$

$\therefore$ LHS = RHS. Base case holds.

Induction Hypothesis: Assume the statement holds for $n = k$, i.e.,

$$1 \cdot 2 + 2 \cdot 5 + \ldots + k \cdot (3k-1) = k^2(k+1)$$

Induction Step: We need to show that the statement holds for $n = k+1$, i.e.,

$$1 \cdot 2 + 2 \cdot 5 + \ldots + k \cdot (3k-1) + (k+1)(3(k+1)-1) = (k+1)^2(k+2)$$

$$\begin{aligned}
&1 \cdot 2 + 2 \cdot 5 + \ldots + k \cdot (3k-1) + (k+1)(3(k+1)-1) \\
&= k^2(k+1) + (k+1)(3k+2) \quad \text{(From Induction Hypothesis)} \\
&= (k+1)(k^2+3k+2) \\
&= (k+1)(k+1)(k+2) \\
&= (k+1)^2(k+2)
\end{aligned}$$

$\therefore$ The statement holds for $n = k+1$.

□

(ii) We will prove the statement by induction on n.

Proof: **Base Case:** For $n = 1$,

LHS:

$$1^2 = 1$$

RHS:

$$\frac{1(4 \cdot 1^2 - 1)}{3} = \frac{1(4-1)}{3} = \frac{3}{3} = 1$$

$\therefore$ LHS = RHS. Base case holds.

Induction Hypothesis: Assume the statement holds for $n = k$, i.e.,

$$1^2 + 3^2 + 5^2 + \ldots + (2k-1)^2 = \frac{k(4k^2-1)}{3}$$

Induction Step: We need to show that the statement holds for $n = k+1$, i.e.,

$$1^2 + 3^2 + 5^2 + \ldots + (2k-1)^2 + (2(k+1)-1)^2 = \frac{k+1(4(k+1)^2-1)}{3}$$

$$\begin{aligned}
&1^2 + 3^2 + 5^2 + \ldots + (2k-1)^2 + (2(k+1)-1)^2 \\
&= \frac{k(4k^2-1)}{3} + (2(k+1)-1)^2 \quad \text{(From Induction Hypothesis)} \\
&= \frac{k(4k^2-1)}{3} + (2k+1)^2 \\
&= \frac{k(4k^2-1)}{3} + (4k^2+4k+1) \\
&= \frac{k(4k^2-1) + 3(4k^2+4k+1)}{3} \\
&= \frac{4k^3 - k + 12k^2 + 12k + 3}{3} \\
&= \frac{4k^3 + 11k^2 + 11k + 3}{3} \\
&= \frac{(k+1)(4k^2+4k+3)}{3} \\
&= \frac{(k+1)(4(k+1)^2-1)}{3}
\end{aligned}$$

$\therefore$ The statement holds for $n = k+1$.

□

Problem 2

Prove that any non-empty finite set of integers has a maximum and minimum element.

Solution

Proof: We use induction on the number of elements in the set.
Base Case: For $n = 1$, the set has only one element, which is both the maximum and minimum.
Induction Hypothesis: Assume the statement holds for $n = k$, i.e., any finite set of k integers has a maximum and minimum element.

Induction Step: We need to show that the statement holds for $n = k + 1$.
Let S be a set of $k + 1$ integers. We can remove one element from the set, say x, to get a new set S'. By the induction hypothesis, S' has a maximum and minimum element, say m and M.
Now, we need to compare x with m and M.
If $x < m$, then m is the minimum of S.
If $x > M$, then M is the maximum of S.
If $m \leq x \leq M$, then m is the minimum and M is the maximum of S.
Thus, in all cases, we have shown that S has a maximum and minimum element.
□

Problem 3

The number $\overline{144l}$ written in base 10 is given to be a prime. Find the last digit l.

Solution

We have to check for l = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
If $l = 0, 2, 4, 6, 8$, then $\overline{144l}$ is even and hence not prime.
If $l = 5$, then $\overline{1445}$ is divisible by 5 and hence not prime.
If $l = 1$, then $\overline{1441}$ is divisble by 11 and hence not prime.
If $l = 3$ or $l = 9$, then $\overline{1443}$ and $\overline{1449}$ are divisible by 3 and hence not prime.

Given that $\overline{144l}$ is prime, for $l = 7$ it must be prime.
Hence, the only possible value of l is 7.

Problem 4

Prove that the product of any k consecutive integers is always divisble by $k!$.
Hint: Use induction on n to show that $\binom{n}{k}$ is an integer.

Solution:

First, we will show that $\binom{n}{k}$ is an integer for all $n \geq k$.

Proof: We will prove the statement by strong induction on n.

Base Case: For $n = k$, we have:

$$\binom{k}{k} = 1$$

$\because$ 1 is an integer, the Base Case holds.

Induction Hypothesis: Assume the statement holds for $n = m$, $\forall m$ such that $k \leq m \leq q$, i.e., $\binom{m}{k}$ is an integer.

Induction Step: We need to show that the statement holds for $n = m + 1$.

$$\begin{aligned}\binom{m+1}{k} &= \frac{(m+1)!}{k!(m+1-k)!} \\ &= \binom{m}{k-1} + \binom{m}{k} \qquad \text{(By Pascal's Identity)}\end{aligned}$$

By the Induction Hypothesis, we know that $\binom{m}{k}$ is an integer. And since $k - 1$ is less than k, we can also say that $\binom{m}{k-1}$ is an integer. Hence, we can conclude that $\binom{m+1}{k}$ is an integer.
□

Now, we will show that the product of any k consecutive integers is always divisible by $k!$.

Proof: Now for any integer a, take the k consecutive integers $a, a+1, a+2, \dots, a+k-1$. The product of these integers is:

$$a(a+1)(a+2)\dots(a+k-1) = \frac{(a+k-1)!}{(a-1)!}$$

From the previous proof, we know that: $\binom{n}{k}$ is an integer for all $n \geq k$.
Hence, we can say that:

$$\begin{aligned}\binom{n}{k} &= \frac{(a+k-1)!}{k!(a+k-1-k)!} \\ &= \frac{(a+k-1)!}{k!(a-1)!} \\ &= \frac{a(a+1)(a+2)\dots(a+k-1)}{k!}\end{aligned}$$

Since $\binom{n}{k}$ is an integer, we can conclude that $a(a+1)(a+2)\dots(a+k-1)$ is divisible by $k!$. Hence, the product of any k consecutive integers is always divisible by $k!$.

□

Problem 5

Show that for every integer $n \geq 1$, the number

$$(4-\frac{2}{1})(4-\frac{2}{2})(4-\frac{2}{3})\dots(4-\frac{2}{n})$$

is an integer.

Solution

Proof: We will prove the statement by induction on n.

Base Case: For $n = 1$,

$$4-\frac{2}{1} = 2$$

Since, 2 is an integer, the Base Case holds.

Induction Hypothesis: Assume the statement holds for $n = k$, i.e.,

$$(4-\frac{2}{1})(4-\frac{2}{2})(4-\frac{2}{3})\dots(4-\frac{2}{k}) = I_k \quad \text{(where } I_k \text{ is an integer)}$$

Induction Step: We need to show the statement holds for $n = k+1$, i.e.,

$$(4-\frac{2}{1})(4-\frac{2}{2})(4-\frac{2}{3})\dots(4-\frac{2}{k})(4-\frac{2}{k+1}) = I_{k+1} \quad \text{(where } I_{k+1} \text{ is an integer)}$$

$$\begin{aligned}&(4-\frac{2}{1})(4-\frac{2}{2})(4-\frac{2}{3})\dots(4-\frac{2}{k})(4-\frac{2}{k+1}) \\ &= I_k(4-\frac{2}{k+1}) \quad \text{(From Induction Hypothesis)} \\ &= I_k(\frac{4(k+1)-2}{k+1}) \\ &= I_k(\frac{4k+4-2}{k+1}) \\ &= I_k(\frac{4k+2}{k+1}) \\ &=\end{aligned}$$

□

Problem 6

Let $n \geq 2$. Show that $(n+1)! + k$ is composite for $k = 2, 3, \ldots, n+1$. This shows that there exists arbitrarily long chains of composite numbers. In particular, find a list of 2025 consecutive composite numbers.

Solution

Proof: Let $n \geq 2$. Consider the following n consecutive integers:

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1)$$

Fix any integer k such that $2 \leq k \leq n+1$. Since $(n+1)!$ is divisible by all integers from 1 to $n+1$, it is also divisible by k. Therefore, we can write:

$$(n+1)! \equiv 0 \mod k \implies (n+1)! + k \equiv k \mod k$$

We can see that $k \mid (n+1)! + k$. We know that $(n+1)! + k \geq k$ and since $k \geq 2$, we can conclude that $(n+1)! + k$ is composite for $k = 2, 3, \ldots, n+1$.
$\therefore$ We have shown that there exists arbitrarily long chains of composite numbers.
$\square$

To find a list of 2025 consecutive composite numbers:

Put $n = 2025$. Then we can consider the following 2025 consecutive integers:

$$(2026)! + 2, (2026)! + 3, \ldots, (2026)! + 2026$$

Each of these integers is composite, as shown in the previous proof. Thus, we have found a list of 2025 consecutive composite numbers.

Problem 7

Show that for $n \geq 1$, the n^{th} Harmonic number

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$$

is not an integer for any $n \geq 2$.

Solution

too sleepy rn.

Problem 8

Let n be a positive integer, and let S be a subset of $n+1$ elements of the set $\{1, 2, \ldots, 2n\}$. Show that

(i) There exist two elements of S which are relatively prime.

(ii) There exist two elements of S, one of which divides the other.

Solution

Proof:
(i) We know $S \subset \{1, 2, \ldots, 2n\}$ and $|S| = n+1$. This means that there will always be at least one pair of elements in S which are consecutive integers, by the Pigeonhole Principle. Since consecutive integers are relatively prime, we can conclude that there exist two elements of S which are relatively prime.

(ii) We can write each number in the set as $2^a \cdot b$, where b is odd and $a \geq 0$.
Consider $n+1$ boxes $B_0, B_1, \ldots, B_n$, where B_i contains all numbers of the form $2^i \cdot b$ for odd b.
Now if we put the elements of S into each box depending on the value of b, we can see that there are n possible values of b because b is odd. But there are $n+1$ elements, so by the Pigeonhole Principle, there will exist one box such that it has 2 elements. Thus, 2 elements will have the same

odd part b and one of them will divide the other.
Hence, we can conclude that there exist two elements of S, one of which divides the other.

□

Problem 9

Let m and n be two integers. Prove that $2m+3n$ is divisible by 17 if and only if $9m+5n$ is divisible by 17.

Solution

Proof:
($\implies$)
Assume $2m+3n$ is divisible by 17.
We know,

$$\begin{aligned}&13 \cdot 2 \mod 17\\&= 26 \mod 17\\&= 9\end{aligned}$$

and we know,

$$\begin{aligned}&13 \cdot 3 \mod 17\\&= 39 \mod 17\\&= 5\end{aligned}$$

Now, we can multiply both sides of the equation $2m+3n \equiv 0 \mod 17$ by 13:

$$\begin{aligned}13(2m+3n) &\equiv 0 \mod 17\\\implies 26m+39n &\equiv 0 \mod 17\\\implies 9m+5n &\equiv 0 \mod 17\end{aligned}$$

Hence, $9m+5n$ is divisible by 17.

($\impliedby$)
Assume $9m+5n$ is divisible by 17.
We know, the inverse of 13 modulo 17 is 4. So, we can write:

$$\begin{aligned}4(9m+5n) &\equiv 0 \mod 17\\\implies 36m+20n &\equiv 0 \mod 17\\\implies 2m+3n &\equiv 0 \mod 17\end{aligned}$$

Hence, $2m+3n$ is divisible by 17.
□

Problem 10

Prove that $8 \mid (n^2-1)$ for any odd integer n.

Solution

Proof: Consider $n = 2k+1$, where k is an integer.
Then,

$$\begin{aligned}n^2-1 &= (2k+1)^2-1\\&= 4k^2+4k\\&= 4k(k+1)\end{aligned}$$

Since k and $k+1$ are consecutive integers, one of them is even. WLOG, say k is even, which means $k = 2m$ for some integer m. Then, $4k(k+1) = 8m(2m+1)$ which is clearly divisible by 8.
Hence, we can conclude that $8 \mid (n^2 - 1)$ for any odd integer n.
□

Problem 11

Prove that $6 \mid (n^3 - n)$ for every integer n. Further show that $24 \mid (n^3 - n)$ for any odd integer n.

Solution

Proof: We can factor $n^3 - n$ as follows:

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

The product $n(n-1)(n+1)$ consists of three consecutive integers, which means at least one of them is divisble by 2 and at least one of them is divisible by 3. Hence, we can conclude that $6 \mid (n^3 - n)$ for every integer n.

Now, for the second part, we will show that $24 \mid (n^3 - n)$ for any odd integer n.
Let $n = 2k + 1$, where k is an integer. Then,

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

Now let us simplify $4k(2k+1)(k+1)$ further.
Consider the following cases:

Case 1: If k is even, then $k = 2m$ for some integer m.

$$
\begin{aligned}
&4k(2k+1)(k+1) \\
&= 8m(4m+1)(2m+1)
\end{aligned}
$$

Since $8m$ is divisible by 8, we need to show that $(4m+1)(2m+1)$ is divisible by 3.
We can check the values of m modulo 3:

- If $m \equiv 1 \mod 3$, then $4m + 1 \equiv 2 \mod 3$ and $2m + 1 \equiv 0 \mod 3$.
- If $m \equiv 2 \mod 3$, then $4m + 1 \equiv 0 \mod 3$ and $2m + 1 \equiv 2 \mod 3$.
- If $m \equiv 0 \mod 3$, then $8m \equiv 0 \mod 3$ and hence $(4m+1)(2m+1) \equiv 0 \mod 3$.

Thus, in all cases, we can conclude that $(4m+1)(2m+1)$ is divisible by 3.

Case 2: If k is odd, then $k = 2m + 1$ for some integer m.

$$
\begin{aligned}
&4k(2k+1)(k+1) \\
&= 8m(4m+3)(2m+2)
\end{aligned}
$$

Since $8m$ is divisible by 8, we need to show that $(4m+3)(2m+2)$ is divisible by 3.
We can check the values of m modulo 3:

- If $m \equiv 1 \mod 3$, then $4m + 3 \equiv 2 \mod 3$ and $2m + 2 \equiv 0 \mod 3$.
- If $m \equiv 2 \mod 3$, then $4m + 3 \equiv 0 \mod 3$ and $2m + 2 \equiv 2 \mod 3$.
- If $m \equiv 0 \mod 3$, then $8m \equiv 0 \mod 3$ and hence $(4m+3)(2m+2) \equiv 0 \mod 3$.

Thus, in all cases, we can conclude that $(4m+3)(2m+2)$ is divisible by 3.

Hence, in both cases, we can conclude that $24 \mid (n^3 - n)$ for any odd integer n.

□

Problem 12

Find all positive integers d such that d divides both n^2+1 and $(n+1)^2+1$ for some integer n.

Solution

We want to find all positive integers d such that

$$d \mid (n^2+1) \quad \text{and} \quad d \mid ((n+1)^2+1)$$

for some integer n.
Let us define the expressions:

$$A = n^2+1,$$
$$B = (n+1)^2+1 = n^2+2n+2.$$

Suppose $d \mid A$ and $d \mid B$. Then $d \mid B-A$, so:

$$B - A = (n^2+2n+2) - (n^2+1) = 2n+1,$$
$$\Rightarrow \quad d \mid (2n+1).$$

So now we have:

$$d \mid n^2+1 \quad \text{and} \quad d \mid 2n+1.$$

From $d \mid 2n+1$, we get:

$$2n \equiv -1 \pmod{d}.$$

Now square both sides:

$$(2n)^2 \equiv (-1)^2 = 1 \pmod{d} \quad \Rightarrow \quad 4n^2 \equiv 1 \pmod{d}.$$

But since $d \mid n^2+1$, we also have:

$$n^2 \equiv -1 \pmod{d} \quad \Rightarrow \quad 4n^2 \equiv -4 \pmod{d}.$$

So we now have:

$$4n^2 \equiv 1 \pmod{d} \quad \text{and} \quad 4n^2 \equiv -4 \pmod{d}.$$

Subtracting gives:

$$1 \equiv -4 \pmod{d} \quad \Rightarrow \quad 5 \equiv 0 \pmod{d} \quad \Rightarrow \quad d \mid 5.$$

Thus, the only possible values for d are the positive divisors of 5, which are:

$$\boxed{1 \quad \text{and} \quad 5}.$$

Note (June 26, 2025)

This assignment is not complete. I will update it later with the remaining solutions.