CSE 301

Anwarul Bashir Shuaib Student ID: 1805010

May 28, 2023

Solution Outline:

Chapter	Solved	#Solved	Unsolved	#Unsolved
1	5, 6, 10, 11, 13, 14, 15, 19	8	17, 21	2
2	11, 12, 14, 19, 20, 21, 22, 23, 24, 25 26, 29	12	13, 15, 30, 32	4
4	2, 14, 18, 24, 31, 32, 41, 42, 46, 47	10	30, 38, 61	3
7	1, 7, 21, 35	4	8, 9, 22, 50	4
Practice PDF	1-14	14	15	1
	Total #solved	48	Total #unsolved	14

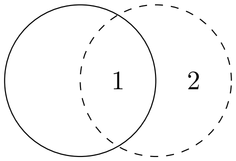
Editable link for future modification: `https://www.overleaf.com/9426722193mtddcqwvcxpx`

Chapter 1

Problem 5

No, we can prove by deriving a recurrence relation for the number of regions created by n circles.
Let, C_n be the number of regions created by n circles. Then,

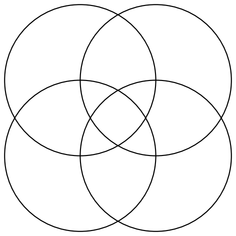
- For C_0, we have no circle, only a single region. Therefore, $C_0 = 1$.
- For C_1, we have an inner and an outer region. So $C_1 = 2$.
- Suppose we add the nth circle, and it intersects the previous $(n-1)$ circles. For each circle the new one intersects with, it creates 2 additional regions.



So, for $n \geq 2$,

$$\begin{aligned} C_n &= C_{n-1} + 2 \times (n-1) \\ &= C_{n-2} + 2 \times (n-2) + 2 \times (n-1) \\ &= C_1 + 2 \times 1 + 2 \times 2 + \ldots + 2 \times (n-2) + 2 \times (n-1) \\ &= 2 + 2 \times (1 + 2 + \ldots + (n-2) + (n-1)) \\ &= 2 + 2 \times \frac{n(n-1)}{2} \\ &= n^2 - n + 2 \end{aligned}$$

For $n = 4$, we get $C_4 = 14$. We can have at most 14 regions (13 inner, 1 outer) with 4 circles intersecting each other.



Problem 6

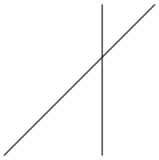
In the original problem, the maximum number of regions, both bounded and unbounded for n line segments was bounded by $O(n^2)$. So, the maximum number of *only bounded* regions must also be bounded by $O(n^2)$. Let us assume that the solution is $B_n = an^2 + bn + c$, where B_n indicates the maximum number of bounded regions possible by n straight lines.

- For $n = 1$, we have a single line, and no bounded regions, hence $B_1 = 0$.

$$a + b + c = 0 \tag{1}$$

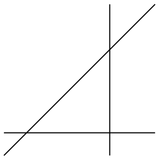
- For $n = 2$, we have two intersecting lines, and no bounded regions. Hence $B_2 = 0$.

$$4a + 2b + c = 0 \tag{2}$$



- For $n = 3$, we have a single bounded region, so $B_3 = 1$.

$$9a + 3b + c = 1 \tag{3}$$



Solving these system of equations $(1), (2)$ and (3), we get:

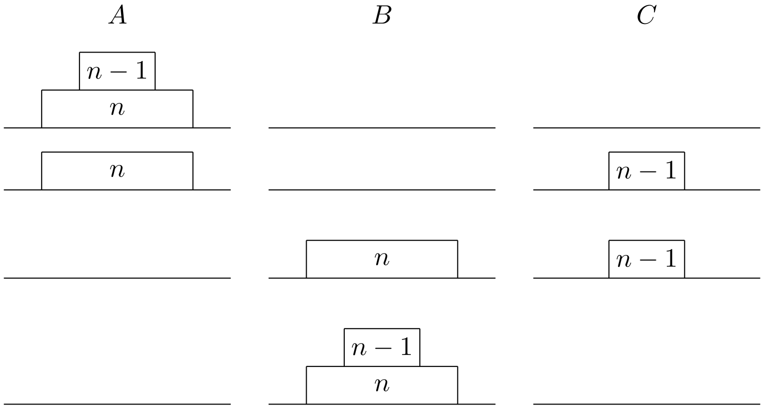
$$\begin{aligned} a &= \frac{1}{2} \\ b &= -\frac{3}{2} \\ c &= 1 \\ B_n &= \frac{n^2}{2} - \frac{3n^2}{2} + 1 \end{aligned}$$

Problem 10

We denote the other peg as C. For this problem, we can move the disks only clockwise, that is either from A to B, B to C or C to A. From the problem statement,

(i) Q_n is the number of moves required to shift n disks from peg A to peg B under the given restrictions. Since the moves are symmetric, shifting n disks from B to C or C to A require the same number of moves as shifting from A to B.

(ii) R_n is the number of moves required to shift n disks from B to A. By the same reasoning, shifting n disks from C to B or A to C also require R_n number of moves.



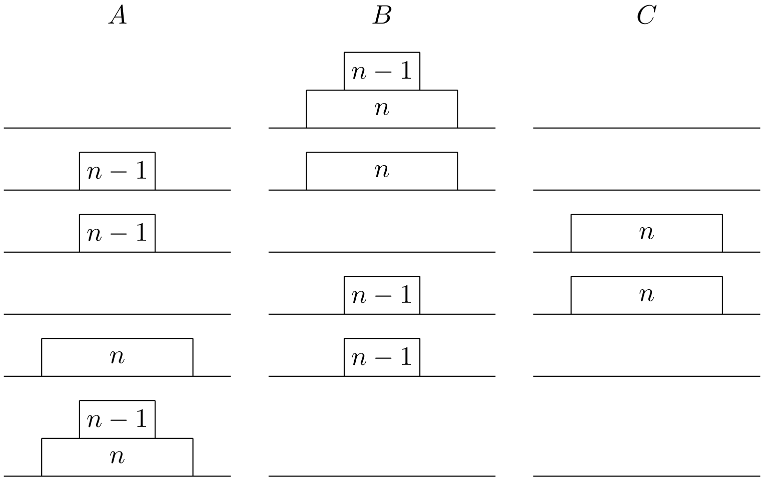
$\implies Q_n =$

R_{n-1} (move $n-1$ disks from A to C)

$+1$ (move nth disk from A to B)

$+R_{n-1}$ (move $n-1$ disks from C to B)

$$\begin{aligned} Q_n &= R_{n-1} + 1 + R_{n-1} \\ &= 2R_{n-1} + 1 \qquad (1) \end{aligned}$$



$\implies R_n =$

R_{n-1} (move $n-1$ disks from B to A)

$+1$ (move nth disk from B to C)

$+Q_{n-1}$ (move $n-1$ disks from A to B)

$+1$ (move nth disk from C to A)

$+R_{n-1}$ (move $n-1$ disks from B to A)

$$\begin{aligned} R_n &= R_{n-1} + 1 + Q_{n-1} + 1 + R_{n-1} \\ &= 2R_{n-1} + 2 + Q_{n-1} \qquad (2) \end{aligned}$$

From (1), we can rewrite $2R_{n-1}$ as:

$$2R_{n-1} = Q_n - 1 \tag{3}$$

Replacing this in (2), we get:

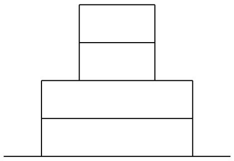
$$\begin{aligned} R_n &= Q_n - 1 + 2 + Q_{n-1} \\ &= Q_n + Q_{n-1} + 1 \end{aligned} \tag{4}$$

Therefore,

$$Q_n = \begin{cases} 0 & \text{if } n = 0 \\ 2R_{n-1} + 1 & \text{if } n > 0 \end{cases} \qquad R_n = \begin{cases} 0 & \text{if } n = 0 \\ Q_n + Q_{n-1} + 1 & \text{if } n > 0 \end{cases}$$

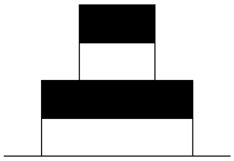
Problem 11

A. Since each of the disks contains an identical copy, we would need exactly 2 moves for moving a single disk including its copy form one peg to another. Hence the total number of moves is just the twice of the original solution, that is $2 \times (2^n - 1)$.



Each disk of the same size is indistinguishable from its pair

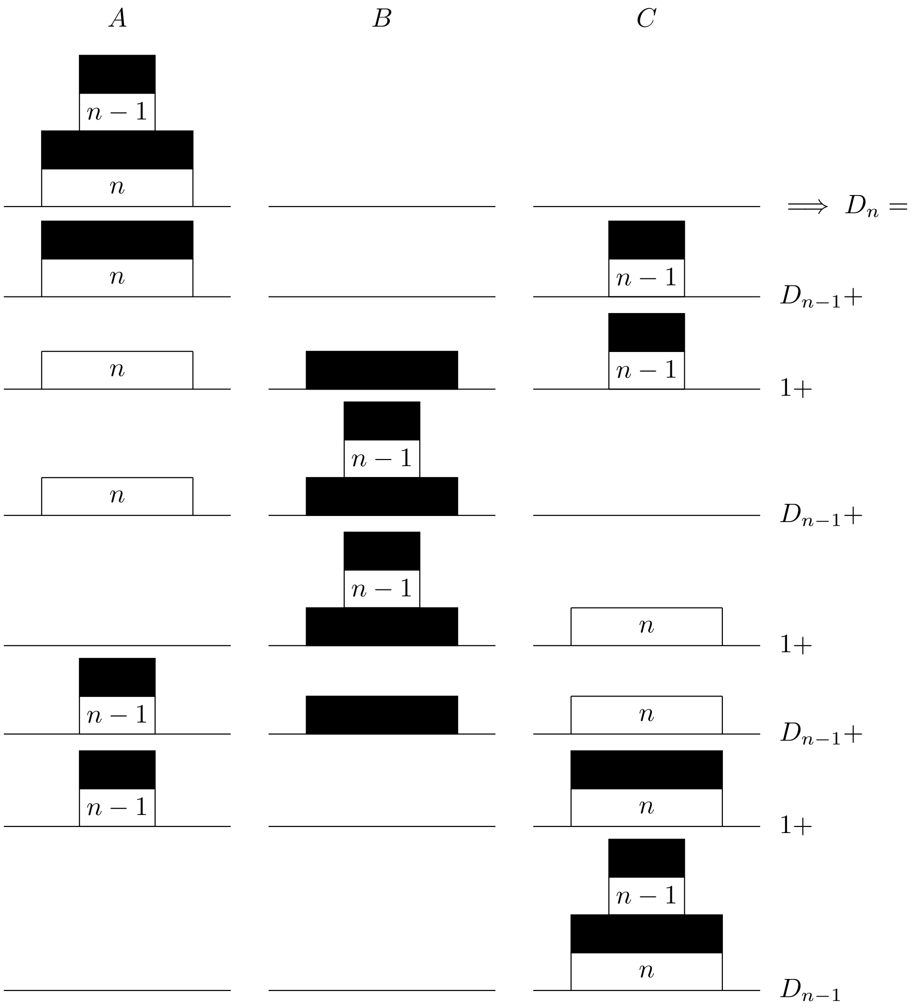
B. Now the disks contain a copy of the same size, but each of the copies is now *distinguishable* from its pair. The additional constraint now imposed is that we would like to shift the disks in a way so that the original ordering is maintained.



We distinguish each pair by giving alternating colors. We can interpret the given constraint in this way:

"*The final arrangement should not contain any black disk under a white disk of the same size.*"

This rephrased constraint ensures that the original ordering in the initial arrangement is maintained in the final arrangement. Let us assume that we need D_n moves to move such a stack of disks under the given constraints from one peg to another.



$$\begin{aligned} D_n &= D_{n-1} + 1 + D_{n-1} + 1 + D_{n-1} + 1 + D_{n-1} \\ &= 4D_{n-1} + 3 \end{aligned} \tag{5}$$

In order to solve this recurrence, we can simplify a bit. We first add 1 to both sides, giving:

$$\begin{aligned} D_n + 1 &= 4D_{n-1} + 4 \\ &= 4(D_{n-1} + 1) \end{aligned}$$

If we let $Z_n = D_n + 1$, we get:

$$Z_n = 4Z_{n-1}$$

Since $D_0 = 0$, $Z_0 = D_0 + 1 = 1$, we can simply unwind the recurrence and find the solution to Z_n directly:

$$\begin{aligned} Z_n &= 4^n \\ \implies D_n &= 4^n - 1 \end{aligned}$$

Problem 13

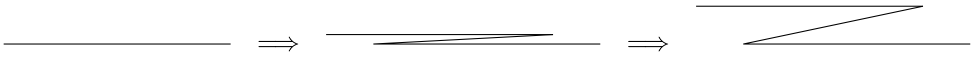
Let ZZ_n denote the maximum number of regions defined by n zig-zag lines. Here,

$$ZZ_0 = 1$$
$$ZZ_1 = 2$$

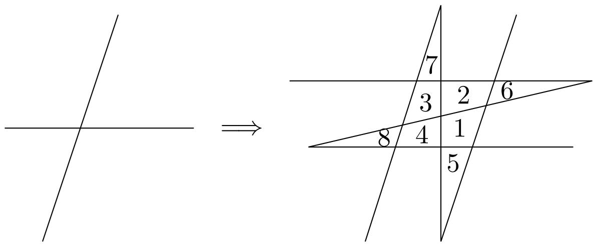
To find a recurrence relation, we notice the following:

(i) Assume we are dealing with straight lines only, no zig-zags. When the nth line intersects the previous $n-1$ lines into $n-1$ distinct points, it creates n additional regions.

(ii) Now assume that we make zig-zags out of each line in the following way:



In this way, if we make the nth line a zig-zag, for each of the previous $n-1$ zig-zags, it will introduce 8 *new* bounded regions.



We will get $8 \times (n-1)$ new bounded regions in this way.

Thus, from (i) we get n regions, and from (ii) we get $8 \times (n-1)$ new bounded regions. We can define ZZ_n as:

$$\begin{aligned} ZZ_n &= ZZ_{n-1} + 8 \times (n-1) + n \\ &= ZZ_{n-1} + 9n - 8 \end{aligned} \tag{6}$$

We can solve this recurrence using perturbation method, or we can break it down into a simpler one:

$$ZZ_n - n = ZZ_{n-1} - (n-1) + 9(n-1) \tag{7}$$

Equation (7) was obtained from observation in such a way so that we can let $T_n = ZZ_n - n$. The base cases are:

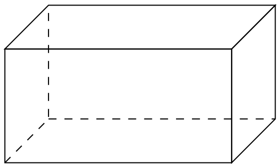
$$T_0 = 1 - 0 = 1$$
$$T_1 = 2 - 1 = 1$$

Replacing $T_n = ZZ_n - n$ in (7):

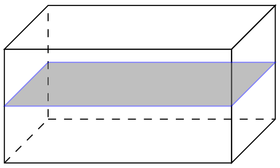
$$\begin{aligned}
T_n &= T_{n-1} + 9(n-1) \\
&= T_{n-2} + 9(n-2) + 9(n-1) \\
&= T_1 + 9 \times 1 + 9 \times 2 + \ldots + 9(n-2) + 9(n-1) \\
&= 1 + 9 \times (1 + 2 + \ldots + (n-2) + (n-1)) \\
&= 1 + 9 \times \frac{n(n-1)}{2} \\
\implies ZZ_n - n &= 1 + \frac{9n^2 - 9n}{2} \\
\implies ZZ_n &= \frac{9n^2}{2} - \frac{7n}{2} + 1
\end{aligned}$$

Problem 14

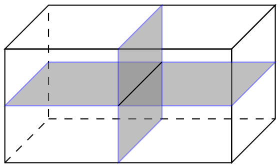
Let us look at a few base cases first. We would use the word *region* to indicate a 2-dimensional slice, and the word *space* to indicate a 3-dimensional slice. When there are no planes through the cube, we get only 1 space, the whole cube itself.



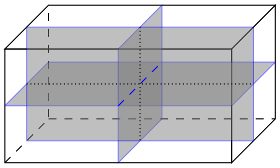
Adding a single plane splits the cube into 2 distinct spaces.

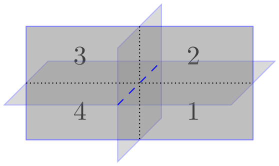


It is clear that we get 4 separate spaces when there are 2 planes. One may think it like this: the new vertical plane is divided into 2 distinct regions by the previous horizontal plane. Their intersection is indicated by a solid line. For each of the divided region in the vertical plane, a single new space is introduced in addition to the previous one, thus we get $2 + 2 = 4$ total spaces.



Adding the 3rd plane divides the cube into 8 separate spaces. The 3rd planes intersects with the previous 2 planes, which gives 2 intersection lines (indicated by the dotted black lines). These 2 dotted lines divide the 3rd plane into 4 separate regions. For each of these regions, we get a new space in addition to the previous 4, thus we get $4 + 4 = 8$ total spaces.





We can see a pattern forming from the base cases. The nth plane is intersected by the previous $n-1$ planes, which can be though of as $n-1$ intersection lines through the nth plane. We know that the number of regions formed by $n-1$ lines through a plane is L_{n-1}. For each of these regions, we are getting a new space. So the number of new spaces is the same as L_{n-1}.

If we denote P_n as the maximum number of 3-dimensional spaces that can be defined by n planes, we can define P_n as:

$$P_n = P_{n-1} + L_{n-1} \tag{8}$$

Problem 15

The problem is undefined for $n = 1$, we will assume $n \geq 2$. We can split the problem into two cases:

(i) Even number of people: If we start with $2n$ persons, after the first round all the even numbered persons will be eliminated. Just like the original problem, we can write:

$$I(2n) = 2I(n) - 1$$

(ii) Odd number of people: Similarly for this case, we can write:

$$I(2n+1) = 2I(n) + 1$$

n	1	2	3	4	5	6	7	8	9	10	11	12
$I(n)$	×	2	1	3	5	1	3	5	7	9	11	1

First few values for the penultimate number

If we look at the values of n for which $I(n) = 1$, we get $n = 3, 6, 12, \ldots = 3 \times 2^0, 3 \times 2^1, 3 \times 2^2, \ldots$.
If we write $n = 3 \times 2^m + r$, where m is the highest integer such that $3 \times 2^m \leq n$, then we can propose $I(n) = I(3\times 2^m + r) = 2r+1$. This formula checks out for other values as well, for example: $n = 8 = 3\times 2^2 + 2$, $I(8) = 2 \times 2 + 1 = 5$. This is our proposed hypothesis. We can use proof by induction to check if this is indeed correct.

Base case: $n = 2 = 3 \times 2^{-1} + \frac{1}{2} \implies I(\frac{1}{2}) = 2 \times \frac{1}{2} + 1 = 2$

Inductive hypothesis: Assume the formula holds for $m = 2, 3, \ldots, k$
$I(n) = I(3 \times 2^k + r) = 2r + 1$

Proof: We have to show that the formula holds for $m = k + 1$.

(i) $n = 3 \times 2^k + r$ even:

$$\begin{aligned}
&I(3 \times 2^{(k+1)} + r) \\
\implies &I(3 \times 2^k \times 2 + r) \\
\implies &2I(3 \times 2^k + \frac{r}{2}) - 1 \qquad \text{Since } I(2n) = 2I(n) - 1 \\
\implies &2(2 \times \frac{r}{2} + 1) - 1 \\
\implies &2r + 1
\end{aligned}$$

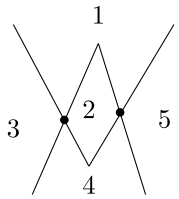
(ii) $n = 3 \times 2^k + r$ odd:

$$\begin{aligned}
&I(3 \times 2^{(k+1)} + r) \\
\implies &I(3 \times 2^k \times 2 + (r-1) + 1) \\
\implies &2I(3 \times 2^k + \frac{r-1}{2}) + 1 \qquad \text{Since } I(2n+1) = 2I(n) + 1 \\
\implies &2(2 \times \frac{r-1}{2} + 1) + 1 \\
\implies &2r + 1
\end{aligned}$$

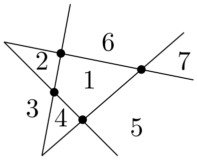
Thus $I(n) = I(3 \times 2^m + r) = 2r + 1$ is the required formula for $n \geq 2$.

Problem 17

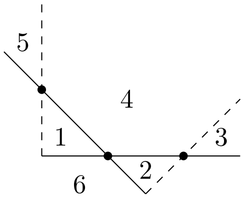
If we place the head of a zig inside another zig, we won't be able to achieve the maximum number of regions, Z_n. From the figure below, we can see that there are only 2 intersection points and we have a total of 5 regions.



In order to maximize the number of regions, we would need to maximize the number of intersections as well. For that we have to place the head of each zigs outside the region of another one. In the figure below, we obtain 4 intersection points and 7 regions, which is the maximum possible number. The mapping from intersection points to the number of regions is distinct: We have 7 regions if and only if we have 4 intersection points. This holds for other values as well when the number of regions is maximized.



Now let us think about a modified version of the problem. Suppose that each zigs has an angle of 90°. We know from the previous example that we can have at most 7 regions with 2 zigs, and those zigs must intersect at 4 distinct points. When each of the two zigs is at 90°, no matter how hard we try, it is impossible to get more than 3 intersection points, which gives a maximum of 6 regions. There will always be at least one line for each zig that will keep diverging from another line of the other zig.



The dashed lines do not intersect and diverge from each other

The reasoning is simple: two 90°s add up to 180°, in order to have 4 intersection points, at least one of the zigs need to have an angle $< 90°$. We can go the other way around: when the angle of each zigs is at 90°, we will have $< (\frac{180}{90} = 2)$ zigs that will give the maximum number of regions. For problem 17, the angle is 30° and we will have $< (\frac{180}{30} = 6)$ zigs that can obtain Z_n number of regions. The maximum integer < 6 is 5.

Chapter 2

Problem 11

$$
\begin{aligned}
&\sum_{0\le k<n} (a_{k+1} - a_k)b_k \\
&= \sum_{0\le k<n} (a_{k+1}b_k - a_k b_k) \\
&= \sum_{0\le k<n} a_{k+1}b_k - \sum_{0\le k<n} a_k b_k \\
&= \sum_{0\le k<n} a_{k+1}b_k - \sum_{1\le k<n+1} a_k b_k - (a_0 b_0 - a_n b_n) \\
&= \sum_{0\le k<n} a_{k+1}b_k - \sum_{1\le k+1<n+1} a_{k+1} b_{k+1} + a_n b_n - a_0 b_0 \\
&= \sum_{0\le k<n} a_{k+1}b_k - \sum_{0\le k<n} a_{k+1} b_{k+1} + a_n b_n - a_0 b_0 \\
&= \sum_{0\le k<n} (a_{k+1}b_k - a_{k+1} b_{k+1}) + a_n b_n - a_0 b_0 \\
&= a_n b_n - a_0 b_0 - \sum_{0\le k<n} a_{k+1}(b_{k+1} - b_k)
\end{aligned}
$$

Problem 12

If we can find an inverse function of $p(k)$ whose domain is defined for the set of all integers, then the range of $p(k)$ will contain the set of all integers. Let,

$$
\begin{aligned}
p(k) &= k + (-1)^k c = y \qquad (9) \\
\implies &= y + c = k + \underbrace{\left(1 + (-1)^k\right)}c
\end{aligned}
$$

Here,

$$
\left(1 + (-1)^k\right) = \begin{cases} 0 & k \text{ odd} \\ 2 & k \text{ even} \end{cases}
$$

So, $y + c$ and k have the same parity: they are either both even or both odd. So we can write: $(-1)^{y+c} = (-1)^k$. From (9):

$$
\begin{aligned}
y &= k + (-1)^k c \\
\implies y &= k + (-1)^{y+c} c \\
\implies k &= y - (-1)^{y+c} c
\end{aligned}
$$

Therefore, $q(y) = y - (-1)^{y+c}c$ is defined for the set of all integers. Hence the range of $p(k)$ contains the set of all integers.

Problem 14

$$\begin{aligned} S_n &= \sum_{k=1}^{n} k2^k \\ &= \sum_{k=1}^{n}\sum_{j=1}^{k} 1 \times 2^k \\ &= \sum_{j=1}^{n}\sum_{k=j}^{n} 2^k \\ &= \sum_{j=1}^{n} 2^{n+1} - 2^j \\ &= n2^{n+1} - \sum_{j=1}^{n} 2^j \\ &= n2^{n+1} - (2^{n+1} - 2) \end{aligned}$$

Problem 19

Here,

$$\begin{aligned} &a2 \\ b_n &= n \\ c_n &= 3 \cdot n! \\ \therefore s_n &= \frac{a_{n-1}a_{n-2}\dots a_1}{b_nb_{n-1}\dots b_2} \times s_1 \\ &= \frac{2^{n-1}}{n!} \qquad [\text{Letting } s_1 = 1] \end{aligned}$$

Now,

$$\begin{aligned} & s_na_nT_n = s_1b_1T_0 + \sum_{k=1}^{n} s_kc_k \\ \implies & \frac{2^{n-1}}{n!} \cdot 2 \cdot T_n = 5 + \sum_{k=1}^{n} \frac{2^{k-1}}{k!} \times 3 \cdot k! \\ \implies & \frac{2^n}{n!}T_n = 5 + 3\sum_{k=1}^{n} 2^{k-1} \\ \implies & \frac{2^n}{n!}T_n = 5 + 3 \times (2^n - 1) \\ \implies & T_n = \frac{n!}{2^n}(2 + 3 \times 2^n) \\ \implies & T_n = \frac{n!}{2^{n-1}} + 3n! \end{aligned}$$

Problem 20

$$S_n = \sum_{k=0}^{n} kH_k$$

Here,

$$\begin{aligned} S_{n+1} &= \sum_{k=0}^{n+1} kH_k \\ &= \sum_{k=0}^{n} kH_k + (n+1)H_{n+1} \\ &= S_n + (n+1)H_{n+1} \qquad (10) \end{aligned}$$

Again,

$$\begin{aligned} S_{n+1} &= \sum_{k=0}^{n+1} kH_k \\ &= \sum_{1\le k\le n+1} kH_k + 0 \times H_0 \\ &= \sum_{1\le k+1\le n+1} (k+1)H_{k+1} \\ &= \sum_{0\le k\le n} (k+1)(H_k + \frac{1}{k+1}) \\ &= \sum_{k=0}^{n} kH_k + H_k + 1 \\ &= S_n + \sum_{k=0}^{n} H_k + (n+1) \qquad (11) \end{aligned}$$

From (10) and (11),

$$\begin{aligned} S_n + (n+1)H_{n+1} &= S_n + \sum_{k=0}^{n} H_k + (n+1) \\ \implies \sum_{k=0}^{n} H_k &= (n+1)(H_{n+1} - 1) \end{aligned}$$

Problem 21

$$S_n = \sum_{0 \le k \le n} (-1)^{n-k}$$

$$\begin{aligned}
S_{n+1} &= \sum_{0 \le k \le n+1} (-1)^{n-k} \\
&= (-1)^{n-(n+1)} + \sum_{0 \le k \le n} (-1)^{n-k} \\
&= -1 + S_n \tag{12}
\end{aligned}$$

$$\begin{aligned}
S_{n+1} &= \sum_{0 \le k \le n+1} (-1)^{n-k} \\
&= (-1)^{n-0} + \sum_{1 \le k \le n+1} (-1)^{n-k} \\
&= (-1)^n + \sum_{0 \le k \le n} (-1)^{n-(k+1)} \\
&= (-1)^n - \sum_{0_\le k \le n} (-1)^{n-k} \\
&= (-1)^n - S_n \tag{13}
\end{aligned}$$

From (12) and (13),

$$\begin{aligned}
-1 + S_n &= (-1)^n - S_n \\
\implies S_n &= \frac{1 + (-1)^n}{2} \tag{14}
\end{aligned}$$

Again,

$$T_n = \sum_{0 \le k \le n} (-1)^{n-k} k$$

$$\begin{aligned}
T_{n+1} &= \sum_{0 \le k \le n+1} (-1)^{n-k} k \\
&= (-1)^{n-(n+1)}(n+1) + \sum_{0 \le k \le n} (-1)^{n-k} k \\
&= -(n+1) + T_n \tag{15}
\end{aligned}$$

$$\begin{aligned}
T_{n+1} &= \sum_{0\le k\le n+1} (-1)^{n-k}k \\
&= (-1)^{n-0}\times 0 + \sum_{1\le k\le n+1} (-1)^{n-k}k \\
&= 0 + \sum_{0\le k\le n} (-1)^{n-(k+1)}(k+1) \\
&= -\sum_{0\le k\le n} (-1)^{n-k}(k+1) \\
&= -\sum_{0\le k\le n} (-1)^{n-k}k - \sum_{0\le k\le n} (-1)^{n-k} \\
&= -T_n - S_n \qquad (16)
\end{aligned}$$

From (15) and (16),

$$\begin{aligned}
-(n+1) + T_n &= -T_n - S_n \\
\implies T_n &= \frac{1+n-S_n}{2} \qquad (17)
\end{aligned}$$

Finally,

$$U_n = \sum_{0\le k\le n} (-1)^{n-k}k^2$$

$$\begin{aligned}
U_{n+1} &= \sum_{0\le k\le n+1} (-1)^{n-k}k^2 \\
&= -(n+1)^2 + \sum_{0\le k\le n} (-1)^{n-k}k^2 \\
&= -(n+1)^2 + U_n \qquad (18)
\end{aligned}$$

$$\begin{aligned}
U_{n+1} &= \sum_{0\le k\le n+1} (-1)^{n-k}k^2 \\
&= 0 + \sum_{1\le k\le n+1} (-1)^{n-k}k^2 \\
&= \sum_{0\le k\le n} (-1)^{n-(k+1)}(k+1)^2 \\
&= -\sum_{0\le k\le n} (-1)^{n-k}(k^2+2k+1) \\
&= -\sum_{0\le k\le n} (-1)^{n-k}k^2 - 2\sum_{0\le k\le n} (-1)^{n-k}k - \sum_{0\le k\le n} (-1)^{n-k} \\
&= -U_n - 2T_n - S_n \qquad (19)
\end{aligned}$$

From (18) and (19),

$$\begin{aligned}
-(n+1)^2 + U_n &= -U_n - 2T_n - S_n \\
\implies U_n &= \frac{(n+1)^2 - 2T_n - S_n}{2} \qquad (20)
\end{aligned}$$

Problem 22

Proof of *Lagrange's Identity:*

$$\sum_{1\le j<k\le n} (a_j b_k - a_k b_j)^2 = \left(\sum_{k=1}^{n} {a_k}^2\right)\left(\sum_{k=1}^{n} {b_k}^2\right) - \left(\sum_{k=1}^{n} a_k {b_k}^2\right)$$

Let,

$$\begin{aligned}
S &= \sum_{1\le j<k\le n} (a_j b_k - a_k b_j)^2 \quad ◹ \\
S &= \sum_{1\le k<j\le n} (a_k b_j - a_j b_k)^2 \quad ◺ \qquad \text{[Swapping } j \leftrightarrow k\text{]} \\
\therefore 2S &= \sum_{1\le j,k\le n} (a_k b_j - a_j b_k)^2 - \sum_{1\le j=k\le n} (a_k b_j - a_j b_k)^2 \quad ▧ \\
&= \sum_{1\le j,k\le n} (a_k b_j - a_j b_k)^2 - 0 \\
&= \sum_j \sum_k (a_k^2 b_j^2 - 2a_j a_k b_j b_k + a_j^2 b_k^2)[1\le j\le n][1\le k\le n] \\
&= \sum_j b_j^2[1\le j\le n] \sum_k a_k^2[1\le k\le n] - 2\sum_j a_j b_j[1\le j\le n] \sum_k a_k b_k[1\le k\le n] \\
&+ \sum_j a_j^2[1\le j\le n] \sum_k b_k^2[1\le k\le n] \\
&= \sum_k b_k^2[1\le k\le n] \sum_k a_k^2[1\le k\le n] - 2\sum_k a_k b_k[1\le k\le n] \sum_k a_k b_k[1\le k\le n] \\
&+ \sum_k a_k^2[1\le k\le n] \sum_k b_k^2[1\le k\le n]
\end{aligned}$$

$$\begin{aligned}
&= \sum_{1\le k\le n} b_k^2 \sum_{1\le k\le n} a_k^2 - 2\sum_{1\le k\le n} a_k b_k \sum_{1\le k\le n} a_k b_k + \sum_{1\le k\le n} a_k^2 \sum_{1\le k\le n} b_k^2 \\
&= 2\left(\sum_{1\le k\le n} a_k^2\right)\left(\sum_{1\le k\le n} b_k^2\right) - 2\left(\sum_{1\le k\le n} a_k b_k\right)^2 \\
\implies S &= \left(\sum_{1\le k\le n} a_k^2\right)\left(\sum_{1\le k\le n} b_k^2\right) - \left(\sum_{1\le k\le n} a_k b_k\right)^2
\end{aligned}$$

With a similar approach, we can prove:

$$\sum_{1\le j<k\le n} (a_j b_k - a_k b_j)(A_j B_k - A_k B_j) = \left(\sum_{1\le k\le n} a_k A_k\right)\left(\sum_{1\le k\le n} b_k B_k\right) - \left(\sum_{1\le k\le n} a_k B_k\right)\left(\sum_{1\le k\le n} A_k b_k\right)$$

Problem 23

$$\begin{aligned}
S &= \sum_{k=1}^{n} \frac{2k+1}{k(k+1)} \\
&= \sum_{k=1}^{n} \left(\frac{1}{k} + \frac{1}{k+1} \right) \\
&= \sum_{k=1}^{n} \frac{1}{k} + \sum_{k=1}^{n} \frac{1}{k+1} \\
&= H_n + \sum_{1 \le k-1 \le n} \frac{1}{(k-1)+1} \quad \text{Replace } k \to k-1 \\
&= H_n + \sum_{2 \le k \le n+1} \frac{1}{k} \\
&= H_n + \sum_{1 \le k \le n} \frac{1}{k} - 1 + \frac{1}{n+1} \\
&= 2H_n - 1 + \frac{1}{n+1}
\end{aligned}$$

Problem 24

$$
\begin{aligned}
S &= \sum_{0\le k<n} \frac{H_k}{(k+1)(k+2)}\\
&= \sum_{0\le k\le n-1} H_k \left(\frac{1}{k+1} - \frac{1}{k+2}\right)\\
&= 0\cdot\left(\frac{1}{1}-\frac{1}{2}\right) + \left(\frac{1}{1}\right)\cdot\left(\frac{1}{2}-\frac{1}{3}\right) + \left(\frac{1}{1}+\frac{1}{2}\right)\cdot\left(\frac{1}{3}-\frac{1}{4}\right) + \left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}\right)\cdot\left(\frac{1}{4}-\frac{1}{5}\right) + \ldots\\
&= \frac{1}{1}\left(\frac{1}{2}-\frac{1}{3}+\frac{1}{3}-\frac{1}{4}+\frac{1}{4}-\frac{1}{5}+\ldots+\frac{1}{n}-\frac{1}{n+1}\right)\\
&+ \frac{1}{2}\left(\frac{1}{3}-\frac{1}{4}+\frac{1}{4}-\frac{1}{5}+\ldots+\frac{1}{n}-\frac{1}{n+1}\right)\\
&+ \frac{1}{3}\left(\frac{1}{4}-\frac{1}{5}+\ldots+\frac{1}{n}-\frac{1}{n+1}\right)\\
&+ \cdots\\
&+ \frac{1}{n-1}\left(\frac{1}{n}-\frac{1}{n+1}\right)\\
&= \frac{1}{1}\left(\frac{1}{2}-\frac{1}{n+1}\right) + \frac{1}{2}\left(\frac{1}{3}-\frac{1}{n+1}\right) + \frac{1}{3}\left(\frac{1}{4}-\frac{1}{n+1}\right) + \cdots + \frac{1}{n-1}\left(\frac{1}{n}-\frac{1}{n+1}\right)\\
&= \left(\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\ldots+\frac{1}{(n-1)\cdot n}\right) - \frac{1}{n+1}\left(\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n-1}\right)\\
&= \sum_{1\le k\le n-1} \frac{1}{k(k+1)} - \frac{1}{n+1}\left(H_n - \frac{1}{n}\right)\\
&= \sum_{1\le k\le n-1} \left(\frac{1}{k} - \frac{1}{k+1}\right) - \frac{1}{n+1}\left(H_n - \frac{1}{n}\right)\\
&= \left(\sum_{1\le k\le n} \frac{1}{k} - \frac{1}{n}\right) - \left(\sum_{1\le k-1\le n-1} \frac{1}{(k-1)+1}\right) - \frac{1}{n+1}\left(H_n - \frac{1}{n}\right)\\
&= \left(H_n - \frac{1}{n}\right) - \left(\sum_{2\le k\le n} \frac{1}{k}\right) - \frac{1}{n+1}\left(H_n - \frac{1}{n}\right)\\
&= \left(H_n - \frac{1}{n}\right) - \left(\sum_{1\le k\le n} \frac{1}{k} - 1\right) - \frac{1}{n+1}\left(H_n - \frac{1}{n}\right)\\
&= \left(H_n - \frac{1}{n} - H_n + 1\right) - \frac{1}{n+1}\left(H_n - \frac{1}{n}\right)\\
&= 1 - \frac{1}{n} + \frac{1}{n(n+1)} - \frac{H_n}{n+1}\\
&= 1 - \frac{1}{n+1} - \frac{H_n}{n+1}\\
&= 1 - \frac{H_n+1}{n+1}
\end{aligned}
$$

Bonus Problem

This stemmed from a failed attempt to Problem 24.

$$\begin{aligned}
S &= 0\cdot\left(\frac{1}{1}-\frac{1}{2}\right)+\frac{1}{1}\cdot\left(\frac{1}{2}-\frac{1}{3}\right)+\frac{1}{2}\cdot\left(\frac{1}{3}-\frac{1}{4}\right)+\frac{1}{3}\cdot\left(\frac{1}{4}-\frac{1}{5}\right)+\dots\\
&= 0+\frac{1}{1\cdot 2}-\frac{1}{1\cdot 3}+\frac{1}{2\cdot 3}-\frac{1}{2\cdot 4}+\frac{1}{3\cdot 4}-\frac{1}{3\cdot 5}+\dots\\
&= \left(\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\dots\right)-\left(\frac{1}{1\cdot 3}+\frac{1}{2\cdot 4}+\frac{1}{3\cdot 5}+\dots\right)\\
&= \sum_{1\le k<n}\frac{1}{k(k+1)}-\sum_{1\le k<n}\frac{1}{k(k+2)}\\
&= \sum_{1\le k<n}\frac{1}{k(k+1)(k+2)}\\
&= \sum_{1\le k<n}\left(\frac{1}{2k}-\frac{1}{k+1}+\frac{1}{2(k+2)}\right)\\
&= \frac{1}{2}\left(\sum_{1\le k\le n}\frac{1}{k}-\frac{1}{n}\right)-\left(\sum_{1\le k-1<n}\frac{1}{(k-1)+1}\right)+\frac{1}{2}\left(\sum_{1\le k-2<n}\frac{1}{(k-2)+2}\right)\\
&= \frac{1}{2}\left(H_n-\frac{1}{n}\right)-\left(\sum_{2\le k\le n}\frac{1}{k}\right)+\frac{1}{2}\left(\sum_{3\le k\le n+1}\frac{1}{k}\right)\\
&= \frac{1}{2}\left(H_n-\frac{1}{n}\right)-\left(\sum_{1\le k\le n}\frac{1}{k}-1\right)+\frac{1}{2}\left(\sum_{1\le k\le n}\frac{1}{k}+\frac{1}{n+1}-1-\frac{1}{2}\right)\\
&= \frac{1}{2}\left(H_n-\frac{1}{n}\right)-(H_n-1)+\frac{1}{2}\left(H_n+\frac{1}{n+1}-1-\frac{1}{2}\right)\\
&= 1-\frac{1}{2n}+\frac{1}{2(n+1)}-\frac{3}{4}\\
&= \frac{1}{4}-\frac{1}{2n(n+1)}
\end{aligned}$$

Problem 25

Distributive Law	$\sum_{k\in\mathrm{K}} ca_k = c\sum_{k\in\mathrm{K}} a_k \longleftrightarrow \prod_{k\in\mathrm{K}} a_k^c = \left(\prod_{k\in\mathrm{K}} a_k\right)^c$
Associative Law	$\sum_{k\in\mathrm{K}}(a_k+b_k) = \sum_{k\in\mathrm{K}} a_k + \sum_{k\in\mathrm{K}} b_k \longleftrightarrow \prod_{k\in\mathrm{K}}(a_k b_k) = \left(\prod_{k\in\mathrm{K}} a_k\right)\left(\prod_{k\in\mathrm{K}} b_k\right)$
Commutative Law	$\sum_{k\in\mathrm{K}} a_k = \sum_{p(k)\in\mathrm{K}} a_{p(k)} \longleftrightarrow \prod_{k\in\mathrm{K}} a_k = \prod_{p(k)\in\mathrm{K}} a_{p(k)}$
Iversonian Notation	$\sum_{k\in\mathrm{K}} a_k = \sum_{k} a_k[k\in\mathrm{K}] \longleftrightarrow \prod_{k\in\mathrm{K}} a_k = \prod_{k} {a_k}^{[k\in\mathrm{K}]}$

Problem 26

Let,

$$\begin{aligned}
P &= \prod_{1\le j\le k\le n} a_j a_k \quad \text{◹} \\
P &= \prod_{1\le k\le j\le n} a_k a_j \quad \text{◺} \qquad j \leftrightarrow k \\
\therefore P^2 &= \left(\prod_{1\le j,k\le n} a_j a_k\right)\left(\prod_{1\le j=k\le n} a_j a_k\right) \quad \text{⧅} \quad \text{[Diagonal elements are multiplied twice]} \\
&= \left(\prod_{1\le j,k\le n} a_j a_k\right)\left(\prod_{1\le k\le n} a_k^2\right)
\end{aligned}$$

The left product could be though of as multiplying each elements of the following matrix:

$$\begin{bmatrix}
a_1a_1 & a_1a_2 & a_1a_3 & \dots & a_1a_n \\
a_2a_1 & a_2a_2 & a_2a_3 & \dots & a_2a_n \\
a_3a_1 & a_3a_2 & a_3a_3 & \dots & a_3a_n \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_na_1 & a_na_2 & a_na_3 & \dots & a_na_n
\end{bmatrix}$$

Each element a_k shows up $2n$ times (n times in one row and n times in one column). After multiplying all the elements, We would end up with: $a_1^{2n}a_2^{2n}\dots a_n^{2n} = \prod_{1\le k\le n} a_k^{2n} = \left(\prod_{1\le k\le n} a_k^n\right)^2$

$$\begin{aligned}
\therefore P^2 &= \left(\prod_{1\le k\le n} a_k^n\right)^2\left(\prod_{1\le k\le n} a_k\right)^2 \\
\implies P &= \left(\prod_{1\le k\le n} a_k^n\right)\left(\prod_{1\le k\le n} a_k\right) \\
&= \left(\prod_{1\le k\le n} a_k\right)^n\left(\prod_{1\le k\le n} a_k\right)^1 \\
&= \left(\prod_{1\le k\le n} a_k\right)^{n+1}
\end{aligned}$$

Problem 29

$$\begin{aligned}
S &= \sum_{1\le k\le n} \frac{(-1)^k k}{4k^2-1}\\
&= \sum_{1\le k\le n} \frac{(-1)^k k}{(2k-1)(2k+1)}\\
&= \frac{1}{4}\sum_{1\le k\le n} (-1)^k \left(\frac{1}{2k-1}+\frac{1}{2k+1}\right)\\
&= \frac{1}{4}\left[-\left(\frac{1}{1}+\frac{1}{3}\right)+\left(\frac{1}{3}+\frac{1}{5}\right)-\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{7}+\frac{1}{9}\right)-\ldots+(-1)^n\left(\frac{1}{2n-1}+\frac{1}{2n+1}\right)\right]\\
&= \frac{1}{4}\left[-\left(\frac{1}{1}+\cancel{\frac{1}{3}}\right)+\left(\cancel{\frac{1}{3}}+\cancel{\frac{1}{5}}\right)-\left(\cancel{\frac{1}{5}}+\cancel{\frac{1}{7}}\right)+\left(\cancel{\frac{1}{7}}+\cancel{\frac{1}{9}}\right)-\ldots+(-1)^n\left(\cancel{\frac{1}{2n-1}}+\frac{1}{2n+1}\right)\right]\\
&= \frac{1}{4}\left[-1+\frac{(-1)^n}{2n+1}\right]
\end{aligned}$$

Chapter 4

Problem 2

We can represent a number in its prime-exponent representation. A prime-exponent representation is a set of the exponents of the consecutive primes that build up a number. For example, $60 = 2^3 \times 3 \times 5$, the prime-exponent representation would be $[3, 1, 1, 0, 0, 0, \ldots]$

$$\begin{aligned}\gcd(m,n) &\iff \min(m_p, n_p)\,\forall p\\ \operatorname{lcm}(m,n) &\iff \max(m_p, n_p)\,\forall p\\ \therefore \gcd(m,n)\times\operatorname{lcm}(m,n) &\iff \min(m_p,n_p)+\max(m_p,n_p)\,\forall p\end{aligned}$$

But, $\min(m_p, n_p) + \max(m_p, n_p) = m_p + n_p$

$$\therefore \gcd(m,n)\times\operatorname{lcm}(m,n) \iff m_p + n_p \quad \forall p \tag{21}$$

$$m \times n \iff m_p + n_p \quad \forall p \tag{22}$$

From equation (21) and (22),

$$\gcd(m,n)\times\operatorname{lcm}(m,n) = m \times n$$

Since $\gcd(m,n) = \gcd(n \bmod m, m)$,

$$\begin{aligned}\gcd(n \bmod m, m)\cdot\operatorname{lcm}(n \bmod m, m) &= m \times n \bmod m\\ \implies \frac{mn}{\operatorname{lcm}(m,n)}\cdot\operatorname{lcm}(n \bmod m, m) &= m \times n \bmod m\\ \implies \operatorname{lcm}(m,n) &= \frac{n}{n \bmod m}\operatorname{lcm}(n \bmod m, m)\end{aligned}$$

Problem 14

Let the prime-exponent representations of k, m, and n be the following:

$$\begin{aligned}k &\iff [k_1, k_2, k_3, \ldots]\\ m &\iff [m_1, m_2, m_3, \ldots]\\ n &\iff [n_1, n_2, n_3, \ldots]\\ km &\iff [k_1+m_1, k_2+m_2, k_3+m_3, \ldots]\\ kn &\iff [k_1+n_1, k_2+n_2, k_3+n_3, \ldots]\end{aligned}$$

Now,

$$\begin{aligned}\gcd(km, kn) &\iff \min(k_p+m_p, k_p+n_p)\,\forall p\\ &\iff k_p + \min(m_p, n_p)\,\forall p \qquad (23)\end{aligned}$$

Again,

$$k \gcd(m,n) \iff k_p + \min(m_p, n_p) \,\forall p \tag{24}$$

From equation (23) and (24),

$$\gcd(km, kn) = k \gcd(m,n)$$

Similarly,

$$\begin{aligned} \operatorname{lcm}(km, kn) &\iff \max(k_p + m_p, k_p + n_p) \,\forall p \\ &\iff k_p + \max(m_p, n_p) \,\forall p \end{aligned} \tag{25}$$

Again,

$$k \operatorname{lcm}(m,n) \iff k_p + \max(m_p, n_p) \,\forall p \tag{26}$$

From equation (25) and (26),

$$\operatorname{lcm}(km, kn) = k \operatorname{lcm}(m,n)$$

Problem 18

For this problem, we would use the following formula: there is a factorization for $x^n + 1$ when n is odd.

$$x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + x^{n-3} - \ldots + 1)$$

Suppose n is not a power of 2. Let $n = ab$, where a is an odd integer greater than 1. Then,

$$2^n + 1 = (2^b)^a + 1 = (2^b + 1)(2^{b(a-1)} - 2^{b(a-2)} + 2^{b(a-3)} + \ldots + 1)$$

$2^n + 1$ is product of 2 numbers, which leads to a contradiction. Therefore, if $2^n + 1$ is prime then n is a power of 2.

Problem 24

In radix p representation,

$$\begin{aligned} n &= n_l p^l + n_{l-1} p^{l-1} + \ldots + n_1 p + n_0 \\ \left\lfloor \frac{n}{p^r} \right\rfloor &= n_l p^{l-r} + n_{l-1} p^{l-1-r} + \ldots + n_r \end{aligned}$$

Now,

$$\begin{aligned}\epsilon(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots + \left\lfloor \frac{n}{p^{r-1}} \right\rfloor + \left\lfloor \frac{n}{p^r} \right\rfloor \\ &= n_l p^{l-1} + n_{l-1} p^{l-2} + \ldots + n_2 p + n_1 \\ &+ n_l p^{l-2} + n_{l-2} p^{l-3} + \ldots + n_2 \\ &\ldots \\ &+ n_l \\ &= n_1 + n_2(p+1) + n_3(p^2+p+1) + \ldots + n_l(p^{l-1} + \ldots + 1) \\ &= \frac{n_1(p-1) + n_2(p^2-1) + n_3(p^3-1) + \ldots + n_l(p^l - 1)}{p-1} \\ &= \frac{(n_0 + n_1 p + n_2 p^2 + n_3 p^3 + \ldots + n_l p^l) - (n_0 + n_1 + \ldots + n_l)}{p-1} \\ &= \frac{n - \upsilon_p(n)}{p-1}\end{aligned}$$

Problem 31

Let,

$$\begin{aligned} & n = 10^k a_k + 10^{k-1} a_{k-1} + \ldots + 10 a_1 + a_0 \\ \implies & n \equiv 1^k a_k + 1^{k-1} a_{k-1} + \ldots + a_1 + a_0 \pmod 3 \quad [\text{ Taking mod 3 on both sides }] \\ \implies & n \equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod 3\end{aligned}$$

Here, $3 \mid n$ if and only if $a_k + a_{k-1} + \ldots + a_1 + a_0 = 0$.

Similarly, in radix b notation $n = b^k a_k + b^{k-1} a_{k-1} + \ldots + b a_1 + a_0$ is divisible by d if and only if $b \equiv 1 \pmod d$ and $d \mid \sum_{i=1}^{k} a_i$

Problem 32

Euler's theorem:

$$n^{\varphi(m)} \equiv 1 \pmod m \quad n \perp m$$

Let S be the set of co-primes of m that are strictly below m.

$$S = \{a_1, a_2, \ldots, a_{\varphi(m)}\}$$

Here, the number of elements in S is $\varphi(m)$, since there are exactly $\varphi(m)$ co-primes of m that are below m. Now, for any $a_i \in S$,

$$\begin{aligned} a_i \perp m \text{ and } n \perp m \implies na_i \perp m \\ \therefore na_i \bmod m \in S\end{aligned}$$

Now consider the set $nS = \{na_1, na_2, \ldots, na_{\varphi(m)}\}$. We would like to show that all distinct pairs of na_i and na_j from nS are unique modulo m, that is each of na_i and na_j leave a distinct remainder when divided by m. Suppose for the sake of contradiction, they leave the same remainder:

$$na_i \equiv na_j \pmod m \implies m \mid n(a_i - a_j)$$

Since $n \perp m$,

$$m \mid (a_i - a_j)$$

Here, both a_i and a_j are less than m. Then their difference $a_i - a_j$ is also less than m. This means m divides something that is smaller than m, and this is only possible when $a_i = a_j$. This proves each distinct pair of elements from nS would leave distinct remainders. Now,

$$\begin{aligned} nS &\equiv \{na_1, na_2, \ldots, na_{\varphi(m)}\} \pmod m \\ nS &\equiv S \pmod m \qquad (27) \end{aligned}$$

Where the last equation follows from the reasoning: since each pairs of na_i and na_j from nS are distinct modulo m (that is why we proved it earlier), then taking $\{na_1, na_2, \ldots, na_\varphi(m)\}$ mod m will leave us with $\{a_1, a_2, \ldots, a_\varphi(m)\}$, although the elements maybe in different order than their original ordering. Multiplying all the elements of S from (27),

$$\begin{aligned} n^{\varphi(m)} \prod_{i=1}^{\varphi(m)} a_i &\equiv \prod_{i=1}^{\varphi(m)} a_i \pmod m \\ \implies n^{\varphi(m)} &\equiv 1 \pmod m \qquad \left[\text{Since } \prod_{i=1}^{\varphi(m)} a_i \perp m\right] \end{aligned}$$

Problem 41

For this problem, it is implicitly assumed that p is a prime number.

A. Given p mod $4 = 3$, we can write $p = 4k + 3$. Suppose for the sake of contradiction, $p \mid n^2 + 1$. Then we can write:

$$\begin{aligned} n^2 + 1 &\equiv 0 \mod p \\ \implies n^2 &\equiv -1 \mod p \\ \implies (n^2)^{\frac{p-1}{2}} &\equiv (-1)^{\frac{p-1}{2}} \mod p \\ \implies n^{p-1} &\equiv -1 \mod p \quad \left(\text{since } p = 4k+3, \frac{p-1}{2} \text{ is odd}\right) \end{aligned}$$

Which leads to a contradiction because $n^{p-1} \equiv -1 \bmod p$ according to Fermat's little theorem. So, there is no such integer n such that $p \nmid n^2 + 1$.

B. We can write $p = 4k+1$. The proof is similar as before: we assume $p \mid n^2+1$.

$$\begin{aligned} n^2+1 &\equiv 0 \mod p \\ \iff n^2 &\equiv -1 \mod p \\ \iff (n^2)^{\frac{p-1}{2}} &\equiv (-1)^{\frac{p-1}{2}} \mod p \\ \iff n^{p-1} &\equiv 1 \mod p \quad \left(\text{since } p = 4k+1, \frac{p-1}{2} \text{ is even}\right) \end{aligned}$$

Therefore, we can go backwards from here and this will lead to a modus ponens.

Problem 42

Since $\gcd(a,b) = \gcd(a, b+na)\ \forall n$, we can conclude:

$$\begin{aligned} m \perp n \text{ and } n' \perp n &\iff mn' \perp n \\ &\iff mn' + m'n \perp n \end{aligned} \tag{28}$$

Similarly,

$$\begin{aligned} m' \perp n' \text{ and } n \perp n' &\iff m'n \perp n' \\ &\iff m'n + mn' \perp n' \end{aligned} \tag{29}$$

From (28) and (29),

$$m' \perp n' \text{ and } n \perp n' \text{ and } m \perp n \iff m'n + mn' \perp nn'$$

Therefore, $\frac{m}{n} + \frac{m'}{n'} = \frac{m'n+mn'}{nn'}$ is reduced to lowest terms if and only if $n \perp n'$. By the phrase '*reduced to lowest terms*', it means the denominator and numerator in the fraction $\frac{m'n+mn'}{nn'}$ are co-prime.

Problem 46

A. According to diophantine equation, there exist integers a and b such that,

$$aj + bk = \gcd(j,k)$$

Now,

$$\begin{aligned} n^j &\equiv 1 \pmod m \\ \implies n^{aj} &\equiv 1^a \pmod m \end{aligned} \tag{30}$$

$$\begin{aligned} n^k &\equiv 1 \pmod m \\ \implies n^{bk} &\equiv 1^b \pmod m \end{aligned} \tag{31}$$

From (30) and (31),

$$\begin{aligned} n^{aj}n^{bk} &\equiv 1 \pmod m \\ \implies n^{aj+bk} &\equiv 1 \pmod m \\ \implies n^{\gcd(j,k)} &\equiv 1 \pmod m \end{aligned}$$

B. Suppose for the sake of contradiction, $2^n \equiv 1 \pmod n$. Since $n > 1$, we can factor out the twos and represent it as $n = 2^k c$, where $k > 0$. We know,

$$a \equiv b \text{ (mod } mn) \iff a \equiv b \text{ (mod } m) \text{ and } a \equiv b \text{ (mod } n) \quad \text{given } m \perp n$$

We can thus write,

$$2^n \equiv 1 \text{ (mod } 2^k c) \iff 2^n \equiv 1 \text{ (mod } 2^k) \text{ and } 2^n \equiv 1 \text{ (mod } c) \quad \text{since } 2^k \perp c$$

But $2^n \equiv 1 \text{ (mod } 2^k)$ is impossible, since there is no way to have a remainder of 1. If $n \geq k$, then $2^k \mid 2^n$ and the remainder would be 0, else the remainder would be 2^n, not 1. This leads to a contradiction, so $2^n \not\equiv 1 \text{ (mod } n)$

Problem 47

Here,

$$\begin{aligned} n^{m-1} &\equiv 1 \pmod m \\ \implies n^{m-1}(m-1)! &\equiv (m-1)! \pmod m \\ \implies (1 \cdot n)(2 \cdot n)\ldots((m-1)\cdot n) &\equiv 1 \cdot 2 \ldots (m-1) \pmod m \end{aligned}$$

Which indicates that the set $S = \{(1 \cdot n), (2 \cdot n), \ldots, ((m-1) \cdot n)\}$ is a complete residue class modulo m. This means if we take modulo m for each element of S and put them in a set, we would get $\{1, 2, \ldots, m-1\}$. Hence, the numbers from the set $\{1, 2, \ldots, m-1\}$ are co-prime to m, implying m is a prime number.

Chapter 7

Problem 1

The original problem had the following generating function:

$$T = \frac{1}{1 - \text{▯} - \text{▭}^2}$$

Since the collector pays 4\$ for each ▯ and 1\$ for each ▭, we can substitute z^4 for ▯ and z for ▭.

$$T = \frac{1}{1 - z^4 - z^2}$$

This is like the original generating function, with z being replaced by z^2. The original generating function had a solution: $[z^n]T = F_{n+1}$, where $[z^n]T$ means coefficient of z^n from the expansion of T. Since the exponent of z in each terms of the new generating function is even, there are no terms with odd powers of z. Therefore the answer is 0 if m is odd, else $F_{m/2+1}$

Problem 7

Given,

$$\begin{aligned} &g_0 = 1 \\ &g_n = g_{n-1} + 2g_{n-2} + \ldots + ng_0 \quad \text{for } n > 0 \end{aligned}$$

Here, we will follow the four steps mentioned in page *337* of the book:

(1) Expressing g_n in a single equation: The recurrence equation is defined only for $n > 0$. In order to handle the base case $g_0 = 0$, we express g_n as following:

$$g_n = g_{n-1} + 2g_{n-2} + \ldots + ng_0 + [n = 0] \tag{32}$$

(2) Express in terms of $G(z)$: For this part, we multiple both sides of equation (32) with z^n and sum over all possible values of n:

$$\begin{aligned} &\sum_n z^n g_n = \sum_n z^n g_{n-1} + \sum_n 2z^n g_{n-2} + \ldots + \sum_n nz^n g_0 + \sum_n z^n\,[n = 0] \\ \implies &\sum_n z^n g_n = \sum_n z^{n+1} g_n + \sum_n 2z^{n+2} g_n + \ldots + \sum_n nz^{n+n} g_n + \sum_n z^n\,[n = 0] \quad \text{(shifting } n\text{)} \\ \implies &\sum_n z^n g_n = z\sum_n z^n g_n + 2z^2 \sum_n z^n g_n + \ldots + nz^n \sum_n z^n g_n + \sum_{n=0} z^0 \\ \implies &G(z) = zG(z) + 2z^2G(z) + \ldots + nz^nG(z) + 1 \end{aligned}$$

(3) Solve for $G(Z)$ and express it as a ratio of two polynomials, $\frac{P(z)}{Q(z)}$. Here, the degree of $P(z)$ needs to

be smaller than that of $Q(z)$:

$$\begin{aligned}
&G(z) = zG(z) + 2z^2G(z) + \ldots + nz^nG(z) + 1 \\
\implies &G(z) = \frac{1}{1 - z - 2z^2 - \ldots - nz^n} \\
\implies &G(z) = \frac{1}{1 - z(1 + 2z + 3z^2 - \ldots - nz^{n-1})} \\
\implies &G(z) = \frac{1}{1 - z(1-z)^{-2}} \\
\implies &G(z) = \frac{(1-z)^2}{(1-z)^2 - z} \\
\implies &G(z) = \frac{1 - 2z - z^2}{1 - 3z - z^2} \\
\implies &G(z) = 1 + \frac{z}{1 - 3z - z^2}
\end{aligned}$$

(4) Find the coefficient of z^n: This coefficient is the closed form of g_n. Here, the extra 1 added with $G(z)$ does not have any contribution to the coefficient of z^n, so it is best left to be ignored. Express the rest as partial fraction and find the coefficient of z^n:

$$\begin{aligned}
\frac{z}{1 - 3z - z^2} &= \frac{z}{(1 - \phi_1 z)(1 - \phi_2 z)} \quad \text{Where, } \phi_1 = \frac{3 + \sqrt{13}}{2},\ \phi_2 = \frac{3 - \sqrt{13}}{2} \\
&= \frac{1}{\phi_1 - \phi_2}\left(\frac{1}{1 - \phi_1 z} - \frac{1}{1 - \phi_2 z}\right) \quad \text{[Decomposing into partial fractions]} \\
&= \frac{1}{\phi_1 - \phi_2}\left((1 - \phi_1 z)^{-1} - (1 - \phi_2 z)^{-1}\right)
\end{aligned}$$

Since $[x^n](1 - px)^{-1} = p^n$ (read as coefficient of x^n from $(1 - px)^{-1}$),

$$\begin{aligned}
[z^n]G(z) &= \frac{1}{\phi_1 - \phi_2}\left({\phi_1}^n - {\phi_2}^n\right) \\
&= \frac{1}{\sqrt{13}}\left({\phi_1}^n - {\phi_2}^n\right)
\end{aligned}$$

The roots ϕ_1, ϕ_2 were found using the following rule: Suppose $Q(z)$ has the form:

$$Q(z) = q_0 + q_1 z + \ldots + q_n z^n$$

Then the reflected polynomial of $Q(z)$ is denoted as:

$$Q^R(z) = q_0 z^n + q_1 z^{n-1} + \ldots + q_n$$

If $Q^R(z)$ has the roots $p_1, p_2, \ldots, p_n$, then the roots of $Q(z)$ are $\frac{1}{p_1}, \frac{1}{p_2}, \ldots, \frac{1}{p_n}$. So if we can express $Q^R(z) = q_0(p_1 - z)(p_2 - z)\ldots(p_n - z)$, then $Q(z) = q_0(1 - p_1 z)(1 - p_2 z)\ldots(1 - p_n z)$

Problem 21

We can express the generating function as:

$$\begin{aligned} G(z) &= (1 + z^{10} + z^{20} + \ldots)(1 + z^{20} + z^{40} + \ldots) \\ &= \left(1 - z^{10}\right)^{-1} \left(1 - z^{20}\right)^{-1} \\ &= \frac{1}{(1 - z^{10})(1 - z^{20})} \end{aligned}$$

A more compact generating function can be found with the substitution $z^{10} \to z$

$$G(z) = \frac{1}{(1 - z)(1 - z^2)} \tag{33}$$

Determining $[z^n]G(z)$:

$$\begin{aligned} \hat{G}(z) &= \frac{1}{(1 - z)(1 - z^2)} \\ &= \frac{1}{4(1 - z)} + \frac{1}{2(1 - z)^2} + \frac{1}{4(1 + z)} \\ &= \frac{1}{2}(1 - z)^{-2} + \frac{1}{4}\Big((1 - z)^{-1} + (1 + z)^{-1}\Big) \\ \implies [z^n]\hat{G}(z) &= \frac{1}{2}(1 + n) + \frac{1}{4}(1 + (-1)^n) \end{aligned}$$

Since $\hat{G}(z)$ is the compact representation of $G(z)$ by a power of 10, finding $[z^{500}]$ from $G(z)$ is equivalent to finding $[z^{50}]$ from $\hat{G}(z)$.

$$\therefore [z^{50}]\hat{G}(z) = 26$$

This can also be found by simple counting technique. Since,

$$\begin{aligned} \hat{G}(z) &= \frac{1}{(1 - z)(1 - z^2)} \\ &= (1 + z + z^2 + \ldots)(1 + z^2 + z^4 + \ldots) \end{aligned}$$

Here, $[z^{50}] = [z^0][z^{50}] + [z^2][z^{48}] + [z^4][z^{46}] + \ldots + [z^{50}][z^0]$. Since each of the coefficients in the expanded series is 1, the number of possible ways to get z^{50} is $\frac{50-0}{2} + 1 = 26$

Problem 35

$$\begin{aligned}
S_n &= \sum_{0<k<n} \frac{1}{k(n-k)} \\
&= \sum_{0<k<n} \left(\frac{1}{nk} + \frac{1}{n(n-k)} \right) \\
&= \sum_{0<k<n} \left(\frac{1}{nk} + \frac{1}{n(n-k)} \right) \\
&= \frac{1}{n} \sum_{0<k<n} \frac{1}{k} + \frac{1}{n} \sum_{0<k<n} \frac{1}{n-k} \\
&= \frac{1}{n} H_{n-1} + \frac{1}{n} \sum_{0<n-k<n} \frac{1}{k} \\
&= \frac{1}{n} H_{n-1} + \frac{1}{n} \sum_{0<k<n} \frac{1}{k} \\
&= \frac{2}{n} H_{n-1}
\end{aligned}$$

Practice Problems

Problem 1

Q: Find the largest positive integer n such that $(n+10) \mid (n^3+100)$.

$$\begin{aligned} n+10 &\equiv 0 \pmod{(n+10)} \\ \implies n &\equiv -10 \pmod{(n+10)} \\ \implies n^3 &\equiv -1000 \pmod{(n+10)} \\ \implies n^3+100 &\equiv -900 \pmod{(n+10)} \end{aligned}$$

Here, largest value of n such that $(n+10) \mid -900$ is 890.

Problem 2

Q: Show that the fraction $\frac{12n+1}{30n+2}$ is irreducible for all positive integers n.

Suppose the fraction is reducible, that is, there is a factor $p > 1$ such that $\gcd(12n+1, 30n+2) = p$. So, $p \mid 12n+1$ and $p \mid 30n+2$. Therefore,

$$\begin{aligned} 12n+1 &\equiv 0 \pmod{p} \\ \implies 60n+5 &\equiv 0 \pmod{p} \quad \text{Multiply by 5} \qquad (34) \\ 30n+2 &\equiv 0 \pmod{p} \\ \implies 60n+4 &\equiv 0 \pmod{p} \quad \text{Multiply by 2} \qquad (35) \end{aligned}$$

Subtracting (34) and (35),

$$1 \equiv 0 \pmod{p} \implies p \mid 1 \quad [\text{ Contradiction }]$$

Problem 3

Q: Call a number *prime looking* if it is composite but not divisible by 2, 3, or 5. The three smallest prime-looking numbers are 49, 77, and 91. There are 168 prime numbers less than 1000. How many prime-looking numbers are there less than 1000?

Let, $|S_n|$ denote the number of integers that are less than 1000 and divisible by n.

$$\begin{aligned} &| S_2 | = \left\lfloor \frac{1000}{2} \right\rfloor = 500 && | S_{2,3} | = \left\lfloor \frac{1000}{2\times 3} \right\rfloor = 166 && \\ &| S_3 | = \left\lfloor \frac{1000}{3} \right\rfloor = 333 && | S_{2,5} | = \left\lfloor \frac{1000}{2\times 5} \right\rfloor = 100 && | S_{2,3,5} | = \left\lfloor \frac{1000}{2\times 3\times 5} \right\rfloor = 33 \\ &| S_5 | = \left\lfloor \frac{1000}{5} \right\rfloor = 200 && | S_{3,5} | = \left\lfloor \frac{1000}{5\times 3} \right\rfloor = 66 && \end{aligned}$$

According to principle of inclusion-exclusion, number of integers that are either divisible by 2,3 or 5 are given by:

$$\begin{aligned} N = &\mid S_2 \mid + \mid S_3 \mid + \mid S_5 \mid - (\mid S_{2,3} \mid + \mid S_{2,5} \mid + \mid S_{3,5} \mid) + \mid S_{2,3,5} \mid \\ &= 734 \end{aligned}$$

Therefore, number of integers that are neither divisible by 2,3 and 5 is: $1000 - 734 = 266$. Note that, among the 734 integers we found earlier, 2,3 and 5 were already included in those 734 integers. From the rest 266 integers, there are $168 - |2, 3, 5| = 165$ prime numbers. We also need to subtract 1 since the number 1 itself is neither a prime nor a prime-looking number. So the number of prime-looking integers less than 1000 is: $266 - 165 - 1 = 100$.

Problem 4

Q: Let m and n be positive integers such that $\text{lcm}\,(m, n) + \text{gcd}\,(m, n) = m + n$. Prove that one of the two numbers is divisible by the other.

Let $\text{gcd}\,(m, n) = d$. Since $\text{gcd}\,(m, n) \times \text{lcm}\,(m, n) = mn$,

$$\begin{aligned} \frac{mn}{d} + d &= m + n \\ \implies (m - d)(n - d) &= 0 \end{aligned}$$

Therefore, $m = d$ or $n = d$. Since $\text{gcd}\,(m, n) = d \implies d \mid m$ and $d \mid n$, we can conclude one of the two numbers is divisible by the other.

Problem 5

Q: Show that for any positive integers a and b, the number $(36a + b)(a + 36b)$ cannot be a power of 2.

Suppose for contradiction that there exists a minimum integer k such that $(36a + b)(a + 36b) = 2^k$. This means each of the factors must be a power of 2, this is only possible when both a and b are even. This is because if either of a or b were to be odd, then at least one of the factors would be odd. Let,

$$a = 2a'b = 2b'$$

Therefore,

$$\begin{aligned} (36a + b)(a + 36b) &= 2^k \\ \implies 2^2(36a' + b')(a' + 36b') &= 2^k \\ \implies (36a' + b')(a' + 36b') &= 2^{k-2} \end{aligned}$$

But this contradicts the minimality of k. We assumed k was the minimum possible integer that satisfies $(36a + b)(a + 36b) = 2^k$, but now we are getting a smaller integer $k - 2$ that satisfies our hypothesis. Thus we arrive at a contradiction.

Problem 6

Q: Find all positive integers n such that $n! + 5$ is a perfect cube.

Check by brute-force $\forall n \leq 9$, we find that only such integer is $n = 5$. Now $\forall n \geq 10$, $100 \mid n!$ since $n!$ contains $2 \times 5 \times 10 = 100$. Now,

$$\begin{aligned} n! &\equiv 0 \pmod{100} \\ \implies n! + 5 &\equiv 5 \pmod{100} \\ \implies k^3 &\equiv 5 \pmod{100} \\ \implies k^3 &= 100c + 5 \quad c > 0 \\ \implies k^3 &= 5(20c + 1) \end{aligned}$$

In order for k^3 to be a perfect cube, there must be at least a factor of 5^3 in it. However, we can factor out only one 5, since for any value of $c > 0$, we cannot factor out any more 5s from $(20c + 1)$. This means k^3 cannot be a perfect cube, which leads to a contradiction.

Problem 7

Q: Let n be an integer greater than three. Prove that $1! + 2! + \ldots + n!$ cannot be a perfect power.

First assume $1! + 2! + \ldots + n!$ can be expressed in a perfect square. Here,

$$\begin{aligned} 1! + 2! + 3! + 4! &\equiv 3 \pmod{10} \\ 5! + 6! + \ldots + n! &\equiv 0 \pmod{10} \\ \implies 1! + 2! + 3! \ldots + n! &\equiv 3 \pmod{10} \quad \text{(Adding the upper two expressions)} \end{aligned}$$

This indicates that the last digit of $1! + 2! + 3! \ldots + n!$ is 3. But there are no integers whose even power ends with 3 (one may manually check $1^2 = 1, 2^2 = 4, \ldots, 9^2 = 81$, none of those squares end with 3). So the given expression cannot be expressed in a perfect square (A stronger conclusion can be derived: The given expression cannot be expressed in any perfect even powers).

Now assume that $1! + 2! + \ldots + n!$ can be expressed in perfect powers greater than 2. Now,

$$\begin{aligned} &1! + 2! + 3! + \ldots + 8! \\ &= 46233 \\ &= 3^2 \times 11 \times 467 \\ &= 9k_1 \quad \text{Where } k_1 = 11 \times 467 \end{aligned} \tag{36}$$

Similarly, we can factor out 27 from $n!$ when $n \geq 9$. So,

$$\begin{aligned} & 9! + 10! + \ldots + n! \\ & = 27k_2 \quad \text{Where } k_2 \text{ is some positive integer} \end{aligned} \tag{37}$$

Adding (36) and (37),

$$\begin{aligned} 1! + 2! + \ldots + n! &= 9k_1 + 27k_2 \\ &= 9(k_1 + 3k_2) \\ &= 3^2(11 \times 467 + k_2) \end{aligned}$$

Here, we can see that the expression $1! + 2! + \ldots + n!$ can have 3 s at most twice, but in order to be a perfect power greater than 2, it needs to have at least that many 3 s. This is a contradiction to our assumption, so the expression $1! + 2! + \ldots + n!$ cannot be a perfect power.

Problem 8

Q: Let p be a prime. Show that there are infinitely many positive integers n such that $p \mid 2^n - n$

Since p is a prime, applying Fermat's little theorem, we get:

$$\begin{aligned} 2^{p-1} &\equiv 1 \pmod{p} \\ \implies 2^{m(p-1)} &\equiv 1^m \pmod{p} \end{aligned}$$

If we let $m = (p-1)^{2k-1}$, we get:

$$2^{(p-1)^{2k}} \equiv 1 \pmod{p} \tag{38}$$

Now,

$$\begin{aligned} p &\equiv 0 \pmod{p} \\ \implies p - 1 &\equiv -1 \pmod{p} \\ \implies (p-1)^{2k} &\equiv (-1)^{2k} \pmod{p} \\ \implies (p-1)^{2k} &\equiv 1 \pmod{p} \end{aligned} \tag{39}$$

From (38) and (39),

$$\begin{aligned} 2^{(p-1)^{2k}} &\equiv (p-1)^{2k} \pmod{p} \\ \implies 2^n &\equiv n \pmod{p} \quad \text{Where } n = (p-1)^{2k} \\ \implies 2^n - n &\equiv 0 \pmod{p} \end{aligned}$$

Thus for different values of k in the equation $n = (p-1)^{2k}$, we would get different values of n. Thus our proof is complete.

JK, not yet. For $p = 2$, the value of n will always be 1 regardless of any positive integer value of k. We need to handle this case separately. Fortunately, this case is easy. When $p = 2$, $p \mid (2^n - n)$ for every even positive integer n. This completes the proof.

Problem 9

Q: Prove that $a^p \equiv a \bmod (p)$, where p is any prime.

Let $S = \{a, 2a, 3a, \dots, (p-1)\cdot a\}$. For each element from S, if we divide it by p and put the remainders in a set R, we would get $R = \{1, 2, 3, \dots, (p-1)\}$. The set S is thus sometimes called complete residue class modulo p, since it generates all possible reminders from $1, 2, \dots, (p-1)$ when divided by p. Now multiplying each element from S and R and taking their modulo, we get:

$$\begin{aligned}(a)\cdot(2a)\cdot(3a)\dots((p-1)\times a) &\equiv 1\cdot 2\cdot 3\dots(p-1) \pmod p\\ \implies a^{p-1}\cdot(p-1)! &\equiv (p-1)! \pmod p\\ \implies a^{p-1} &\equiv 1 \pmod p \quad [\text{Since } (p-1)! \perp p]\\ \implies a^p &\equiv a \pmod p\end{aligned}$$

Problem 10

Q: Find all prime numbers p and q for which $pq \mid (5^p - 2^p)(5^q - 2^q)$

Here,

$$\begin{aligned}5^p - 2^p &= (5-2)\big(5^{p-1} + 5^{p-2}\cdot 2 + 5^{p-3}\cdot 2^2 + \dots + 5\cdot 2^{p-2} + 2^{p-1}\big)\\ &= 3\big(5^{p-1} + 5^{p-2}\cdot 2 + 5^{p-3}\cdot 2^2 + \dots + 5\cdot 2^{p-2} + 2^{p-1}\big)\end{aligned}$$

Similarly,

$$\begin{aligned}5^q - 2^q &= 3\big(5^{q-1} + 5^{q-2}\cdot 2 + 5^{q-3}\cdot 2^2 + \dots + 5\cdot 2^{q-2} + 2^{q-1}\big)\\ \therefore (5^p - 2^p)(5^q - 2^q) &= 3^2\big(5^{p-1} + 5^{p-2}\cdot 2 + \dots + 2^{p-1}\big)\big(5^{q-1} + 5^{q-2}\cdot 2 + \dots + 2^{q-1}\big)\end{aligned}$$

Here, $pq \mid (5^p - 2^p)(5^q - 2^q)$ if we let $p = 3, q = 3$. Now, consider the case when only $p = 3$.

$$\begin{aligned}(5^p - 2^p)(5^q - 2^q) &= (5^3 - 2^3)(5^q - 2^q)\\ &= 3^2 \times 13(5^q - 2^q)\end{aligned}$$

Here, $pq \mid (5^p - 2^p)(5^q - 2^q)$ if we let $p = 3, q = 13$. Since the cases are symmetric for, we can also conclude that the division is possible when $p = 13, q = 3$. Therefore, the possible values are: $(p, q) = (3, 3), (3, 13), (13, 3)$

Problem 11

Since $\gcd(a, b) = \gcd(a - kb, b)$ for any integer k, we can write:

$$\begin{aligned}
&\gcd((n+1)! + 1, n! + 1) \\
&= \gcd((n+1)! + 1 - (n+1)(n! + 1), n! + 1) \\
&= \gcd((n+1)! + 1 - (n+1)! - (n+1), n! + 1) \\
&= \gcd(-n, n! + 1) \\
&= \gcd(n, n! + 1)
\end{aligned}$$

Here, $n! + 1 \perp n$, therefore $\gcd(n, n! + 1) = 1$.

Problem 12

Q: Find the smallest positive integer whose cube ends in 888.

Let the number be x. By trial and error for the ones digit: $1^3 = 1, 2^3 = 8, 3^3 = 27, \ldots, 9^3 = 729$, we see that only possible choice for the ones digit is 2 if x^3 is to end in 8. Since the ones digit of x is 2, we can write $x = 10k + 2$. Now,

$$\begin{aligned}
x &= 10k + 2 \\
\implies x^3 &= 1000k^3 + 600k^2 + 120k + 8
\end{aligned}$$

Since the ones digit of x^3 is 8, the leftover part $1000k^3 + 600k^2 + 120k$ needs to end with 880. In other words, $\frac{1000k^3+600k^2+120k}{10} = 100k^3 + 60k^2 + 12k$ needs to end with 88. Now,

$$100k^3 + 60k^2 + 12k \equiv 12k \equiv 8 \pmod{10}$$

We can write this because $100k^3$ and $60k^2$ are both divisible by 10, so the remainder part must come from $12k$, and this remainder part has to end with an 8. So k must end with either 4 or 9. Manually checking some values,

$$\begin{aligned}
12 \times 4 = 48 &\implies x^3 = (42)^3 = 74088 \\
12 \times 9 = 108 &\implies x^3 = (92)^3 = 778688 \\
12 \times 14 = 168 &\implies x^3 = (142)^3 = 2863288 \\
12 \times 19 = 228 &\implies x^3 = (192)^3 = 7077888
\end{aligned}$$

Therefore $x = 192$.

Problem 13

Q: Let $p \geq 3$ be a prime, and let $\{a_1, a_2, \ldots, a_{p-1}\}$ and $\{b_1, b_2, \ldots, b_{p-1}\}$ be two sets of complete residue classes modulo p. Prove that $a_1b_1, a_2b_2, \ldots, a_{p-1}b_{p-1}$ is not a complete set of residue classes modulo p.

Since the sets are complete residue classes modulo p (which means the elements of the set produce all possible remainders $1, 2, \ldots, (p-1)$ when divided by p), according to Wilson's theorem, we get:

$$\begin{aligned} a_1 \cdot a_2 \ldots a_{p-1} &\equiv 1 \cdot 2 \ldots (p-1) \pmod{p} \\ &\equiv (p-1)! \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned} \tag{40}$$

Similarly,

$$b_1 \cdot b_2 \ldots b_{p-1} \equiv -1 \pmod{p} \tag{41}$$

Multiplying (40) and (41),

$$a_1b_1 \cdot a_2b_2 \ldots a_{p-1}b_{p-1} \equiv 1 \pmod{p}$$

However, it is important to note that only the product of integers that generate all possible remainders $1, 2, \ldots, (p-1)$ is congruent to -1 modulo p. In this case, the product $a_1b_1 \cdot a_2b_2 \ldots a_{p-1}b_{p-1}$ does not satisfy this congruence, indicating that the set $\{a_1b_1, a_2b_2, \ldots, a_{p-1}b_{p-1}\}$ does not encompass all the possible remainders modulo p. Therefore, this set cannot be considered a complete set of residue classes modulo p.

Problem 14

Q: Let $n > 1$ be an odd integer. Prove that $n \nmid 3^n + 1$.

Here, the integer 3^n is always odd for any value of $n > 1$. Therefore, $3^n + 1$ is always even, hence $n \nmid 3^n + 1$. This proof can also be visualized in a different way: let us write the first few values of the integers in base 3 notation:

Base 10	Base 3	$\sum$ Digits of base 3
1	1	1
2	2	2
3	10	1
4	11	2
5	12	3
6	20	2
7	21	3
8	22	4
9	100	1
10	101	2
11	102	3
12	110	2
13	111	3
14	112	4
15	120	3

Here, we see that for odd integers, the sum of digits of the base 3 notation is always odd, and for even integers, the sum of digits of the base 3 notation is always even. Now the integer $3^n + 1$ can be written as $1000 \ldots 0001$ in base 3 notation, where the most significant bit 1 is followed by $n - 1$ zeroes, then followed by a single 1 at the rightmost side. In base 3 notation, the only non-zero digits in $3^n + 1$ are 1 and 1, and their sum is 2, indicating that $3^n + 1$ is always an even integer. However, n is always an odd integer, and an odd integer can never divide an even integer. Thus $n \nmid 3^n + 1$.