CSE 301

Tanjeem Azwad Zaman Student ID: 1805006

May 13, 2023

Chapter 1

NB. In general, T_n represents the n^{th} term in a series. The series is defined according to the context given, and n is usually a non-negative integer.

P5: A "Venn diagram" with three overlapping circles is often used to illustrate the eight possible subsets associated with three given sets. Can the sixteen possibilities that arise with four given sets be illustrated by four overlapping circles?

Ans: No. It is not possible to do so. Because:

- A circle can intersect another circle at a maximum of two points. Thus creating two new regions per pair of intersection points. Let T_n be the maximum number of regions from n intersecting circles.
- This gives the recursive definition to be:
  - **Base Case:** $T_1 = 2$
  - **Recursive Definition:** $T_n = T_{n-1} + 2(n-1)$ for $n > 1$
- With a closed form as $T_n = 2 + n(n-1)$ [Can be proven with induction]
- This gives us $T_4 = 14 < 16$, thus proving the claim as impossible.

P6: Some of the regions defined by n lines in the plane are infinite, while others are bounded. What's the maximum possible number of bounded regions?

Ans:

- We manually look at some some (n, T_n) pairs, and find $(1,0), (2,0), (3,1), (4,3), (5,6)/cdots$
- Thus the recursive definition looks like: [T_n= max bounded regions by n lines]
  - **Base Case:** $T_2 = 0$
  - **Recursive Definition:** $T_n = T_{n-1} + (n-2)$
- We propose a closed form as $T_n = (n-1)(n-2)/2$

Proof By induction:

- **Base Case:** $T_2 = 1 \cdot 0/2 = 0$
- **Inductive Hypothesis:** Let $T_k = T_{k-1} + (k-2)$ be true for $k \leq n$
- **Inductive Step:** We must show that the closed form holds for T_{n+1}
  - $T_{n+1} = T_n + (n-1) = (n-1)(n-2)/2 + (n-1) = (n-1)(n-2+2)/2 = ((n+1)-1)((n+1)-2)/2$
  - This proves the inductive step and thus completes our proof.

P10: Q_n be the minimum number of moves needed to transfer a tower of n disks from A to B if all moves must be clockwise - that is, from A to B, or from B to the other peg, or from the other peg to A. Also let R_n be the minimum number of moves needed to go from B back to A under this restriction. Prove that:

$$Q_n = \begin{cases} 0, & \textbf{if } n = 0 \\ 2R_{n-1} + 1, & \textbf{if } n > 0 \end{cases}$$

$$R_n = \begin{cases} 0, & \textbf{if } n = 0 \\ Q_n + Q_{n-1}, +1 & \textbf{if } n > 0 \end{cases}$$

Ans: Let third peg be C and A-B-C be in clockwise order

A. Proof of:

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

- Move $n-1$ discs anticlockwise from A to C in R_{n-1} moves
- Move n^{th} disc from A to B in 1 move (clockwise)
- Move $n-1$ discs anticlockwise from C to B in R_{n-1} moves
- Thus total moves $= R_{n-1} + 1 + R_{n-1} = 2R_{n-1} + 1$
- Thus, $Q_n = 2R_{n-1} + 1$, for $n > 0$ ***(Proved)***

B. Proof of:

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

- Move top $n-1$ discs anticlockwise from B to A in R_{n-1} moves
- Move n_{th} clockwise from B to C in 1 move
- Move top $n-1$ discs anticlockwise from A to C in R_{n-1} moves
- Move n_{th} clockwise from C to A in 1 move
- Move top $n-1$ discs clockwise from C to A in Q_{n-1} moves
- Total moves $= R_{n-1} + 1 + R_{n-1} + 1 + Q_{n-1} = (2R_{n-1} + 1) + Q_{n-1} + 1 = Q_n + Q_{n-1} + 1$ **(QED)**

P11a: A Double Tower of Hanoi contains $2n$ disks of n different sizes, two of each size. As usual, we're required to move only one disk at a time, without putting a larger one over a smaller one. How many moves does it take to transfer a double tower from one peg to another, if disks of equal size are indistinguishable from each other?

Ans: Let A_n be the minimum number of moves required to shift $2n$ discs from A to C (with helper B) where order doesn't matter (is actually reversed for bottom 2 discs).

- **Base case:** For $n = 1$, $A_1 = 2$
- Move top $2(n-1)$ from A to B in A_{n-1} moves
- Move Bottom 2 from A to C in 2 moves
- Move top $2(n-1)$ from B to C in A_{n-1} moves
- **Recursive Definition:** $A_n = 2A_{n-1} + 2$
- **Closed Form:** $A_n = 2^{n+1} - 2$ [can easily be proved by Induction]

P11b: What if we are required to reproduce the original top-to-bottom order of all the equal-size disks in the original arrangement?

Ans: Let B_n be the minimum number of moves required to shift $2n$ discs from A to C (with helper B) where order is the same.

- **Base case:** $B_1 = 4$ (move 2 from A to B [reverse] then from B to C [2x reverse = in order])
- Move top $2(n-1)$ from A to C in A_{n-1} moves (Reverse bottom Order)
- Move Bottom 2 from A to B in 2 moves
- Move top $2(n-1)$ from C to A in A_{n-1} moves (Reverse bottom Order again, thus correcting order)
- Move Bottom 2 from B to C in 2 moves
- Move top $2(n-1)$ from A to C in B_{n-1} moves (Maintain bottom order)
- **Recursive Definition:** $B_n = B_{n-1} + 2A_{n-1} + 4$
- **Closed Form:** $A_n = 2^{n+2} - 5$ [can be proved by Induction]

P13: What's the maximum number of regions definable by n zig-zag lines?

Ans: Let Z_n denote the max number of regions created by n zigzags.

- First consider the lines to be normal straight lines. Let, L_n denote the maximum number of regions made by n intersecting straight lines. As proved before, $L_1 = 2; L_n = L_{n-1} + n$; and closed form $L_n = n(n+1)/2 + 1$
- Then convert each line into very thin zigzags.
- Zigzags intersecting can produce a maximum of 8 new bounded regions per intersection point, not considered in the normal line intersection above.
- Z_n = old regions + regions from normal line PoV + 8· Zigzag intersections
- Thus $Z_n = Z_{n-1} + n + 8(n-1) = Z_{n-1} + 9n - 8$ with a base case of $Z_1 = 2$
- Which has a closed form of $Z_n = (9/2)n^2 - (7/2)n + 1$ [can be proved by induction]

P14: How many pieces of cheese can you obtain from a single thick piece by making five straight slices? (The cheese must stay in its original position while you do all the cutting, and each slice must correspond to a plane in 3D.) Find a recurrence relation for P_n, the maximum number of 3-D dimensional regions that can be defined by n different planes

Ans: Let C_n denote the max number of 3-D regions created by n slices.

- **Base Case:** $C_1 = 2$
- n_{th} slice creates new 3-D regions = number of 2-D regions on the plane of n_{th} slice created by the lines of intersection between that slice and previous other $n-1$ slices.
- Thus, $C_n = C_{n-1} + L_{n-1} = C_{n-1} + n(n-1)/2 + 1$
- Thus, (n, C_n) pairs stand as follows: $(1,2), (2,4), (3,8), (4,15), (5,26) \cdots$
- Max 3D regions for 5 slices = 26 **(Ans)**

P17: If W_n is the minimum number of moves needed to transfer a tower of n disks from one peg to another when there are four pegs instead of three, show that

$$W_{(n(n+1))/2} \leq W_{(n(n-1))/2} + T_n$$

Here $T_n = 2^n - 1$ is the ordinary three-peg number.) Use this to find a closed form $f(n)$ such that $W_{(n(n+1))/2} \leq f(n)$

Ans: We are to find an upper bound. And move from A to D with B,C as intermediates.

- We find a recursive definition for W_{n+m}
- We move upper m discs from A to an intermediate (say B) in W_m moves using 4 pegs
- We move the bottom n discs from A to D using the other intermediate (C) in T_n moves (using available 3 pegs)
- We then again move the m discs in peg B to D using 4 pegs in W_m moves
- This at most $2W_m + T_n$ moves are needed to move $(m + n)$ discs

$$W_{m+n} \leq 2W_m + T_n$$

- let $m = 1 + 2 + \cdots + n - 1 = n(n-1)/2$, then $m = 1 + 2 + \cdots + n = (n+1)n/2$
- Then the required form is obtained

$$\begin{aligned} W_{(n(n+1))/2} &\leq W_{(n(n-1))/2} + T_n \\ W_{(n(n+1))/2} - 1 &\leq W_{(n(n-1))/2} + 2^n - 2 \end{aligned}$$

- Dividing by 2^n and taking $Y_n = W_{(n(n+1)/2)} - 1/2^n$ we get

$$\begin{aligned} & (W_{(n(n+1))/2} - 1)/2^n \leq (W_{(n(n-1))/2} - 1)/2^{n-1} + 1 \\ \implies & Y_n \leq Y_{n-1} + 1 = n - 1 \ (Base: \ Y_1 = 0) \\ \implies & (W_{(n(n+1))/2} - 1)/2^n \leq n - 1 \\ \implies & W_{(n(n+1))/2} \leq (n-1)2^n + 1 \end{aligned}$$

P19: Is it possible to obtain Z_n regions with n bent lines when the angle at each zig is $30°$?

Ans: No, it is impossible to do so.

- The bisectors of two bent lines (each bent at and angle α) must intersect each other and produce an angle θ such that $\alpha < \theta < 180 - \alpha$
- in our case, $\alpha = 30°$, so possible range of θ is $(30, 150)$. Thus we can fit at most $150/30 = 5$ zigs before the 6th zig crosses the $150°$ upper limit. So at most 5 zigs can produce max regions by intersection, when each of their angles is $30°$
- So 11 zigs is impossible.

P21: Suppose there are 2n people in a circle; the first n are "good guys" and the last n are "bad guys." Show that there is always an integer m (depending on n) such that, if we go around the circle executing every m^{th} person, all the bad guys are first to go. (For example, when n = 3 we can take m = 5; when n = 4 we can take m = 30.)

Ans:

- This can be easily accomplished by picking $m = lcm(n + 1, n + 2, \cdots, 2n)$
- if this is done, in n iterations, starting from $k = 2n^{th}$ down to the $(n + 1)^{th}$ person will be eliminated one by one after m/k full circles around the remaining people in each iteration.
- Thus all the n bad guys will be eliminated first.

Chapter 2

P11: The general rule for summation by parts is equivalent to

$$\sum_{0\le k<n}(a_{k+1}-a_k)b_k = a_nb_n - a_0b_0 - \sum_{0\le k<n} a_{k+1}(b_{k+1}-b_k),\ for\ n\ge 0$$

Prove this formula directly by using the distributive, associative, and commutative laws.

Ans:

$$\begin{aligned}
LHS &= \sum_{0\le k<n}(a_{k+1}-a_k)b_k \\
&= \sum_{0\le k<n} a_{k+1}b_k - \sum_{0\le k<n} a_kb_k \\
&= \sum_{0\le k<n} a_{k+1}b_k - (\sum_{0\le k<n} a_kb_k + a_nb_n - a_nb_n) \\
&= \sum_{0\le k<n} a_{k+1}b_k - (\sum_{1\le k<n} a_kb_k + a_nb_n + a_0b_0 - a_nb_n) \\
&= \sum_{0\le k<n} a_{k+1}b_k - (\sum_{1\le k<n+1} a_kb_k) + a_nb_n - a_0b_0 \\
&= \sum_{0\le k<n} a_{k+1}b_k - (\sum_{0\le k<n} a_{k+1}b_{k+1}) + a_nb_n - a_0b_0 \\
&= -\sum_{0\le k<n} a_{k+1}(b_{k+1}-b_k) + a_nb_n - a_0b_0 = RHS\ \textbf{(Proved)}
\end{aligned}$$

P12: Show that the function $p(k) = k + (-1)^k c$ is a permutation of the set of all integers, whenever c is an integer.

Ans:

- This function maps all even integers $2k$ to $2k+1$; $k \in \mathbb{Z}$
- And all odd integers $2m+1$ to $2m$; $m \in \mathbb{Z}$
- Since the set of integers is infinite, these end up mapping to all even and odd integers seperately, making up a permutation of $\mathbb{Z}$ itself

P14: 4 Evaluate $\sum_{1\le k\le n} k2^k$ by rewriting it as the multiple sum $\sum_{1\le j\le k\le n} 2^k$

Ans:

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

P15: Evaluate $Cu_n = \sum_{1\le k\le n} k^3$

Ans:

$$\begin{aligned}
Cu_n + Sq_n &= \sum_{1\le k\le n} k^3 + k^2 = 2\sum_{1\le k\le n} k\cdot(k(k+1)/2) = 2\sum_{1\le k\le n}\sum_{1\le j\le k} jk \\
&= [(\sum_{1\le j\le n} j)^2 + (\sum_{1\le j\le n} j^2)] \qquad [Since \sum_{1\le j\le k\le n}]a_ja_k = (1/2)((\sum_{1\le k\le n} a_k)^2 + \sum_{1\le k\le n} a_k^2)] \\
&= (n(n+1)/2)^2 + Sq + n
\end{aligned}$$

$$\implies Cu_n = (n(n+1)/2)^2$$

P19: Use a summation factor to solve the recurrence

$$T_0 = 5$$
$$2T_n = nT_n - 1 + 3 \cdot n!$$

Ans:

- Comparing with $a_nT_n = b_nT_{n-1} + c_n$, we get $a_n = 2, b_n = n, c_n = 3n!$
- Again, $s_n = \frac{a_{n-1}a_{n-2}\cdots a_1}{b_n b_{n-1}\cdots b_2} s_1 = \frac{2^{n-1}}{n!} \cdot 2 = \frac{2^n}{n!}$ [let $s_1 = 2$]
- $T_n = \frac{1}{s_n a_n}[s_1 b_1 T_0 + \sum_{1\le k\le n} s_k c_k] = \frac{n!}{2^n}(5 + 3\sum_{1\le k\le n} 2^{k-1}) = \frac{n!}{2^n}(5 + 3(2^n - 1))$ $= 3n! + n!/2^{n-1}$ ***(Ans)***

P20: Try to evaluate $\sum_{0\le k\le n} kH_k$ by the perturbation method, but deduce the vapue of $\sum_{0\le k\le n} H_k$ instead

Ans:

- Perturbation gives:

$$s_{n+1} = S_n + (n+1)H_{n+1} = \sum_{1\le k\le n+1} kH_k = \sum_{0\le k\le n} (k+1)H_{k+1} = \sum_{0\le k\le n} (k+1)(H_k + \frac{1}{k+1})$$
$$= \sum_{0\le k\le n} kH_k + \sum_{0\le k\le n} H_k + \sum_{0\le k\le n} 1$$
$$S_n + (n+1)H_{n+1} = S_n + \sum_{0\le k\le n} H_k + n + 1 \implies \sum_{0\le k\le n} H_k = (n+1)(H_{n+1} - 1) \quad \textbf{\textit{(Proved)}}$$

P21: Evaluate using perturbation method $[n \ge 0]$:

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

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

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

Ans:

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

$$S_{n+1} = \sum_{0\le k\le n+1} (-1)^{n+1-k}$$
$$= \sum_{0\le k\le n} (-1)^{n+1-k} + (-1)^{n+1-(n+1)}$$
$$= 1 - S_n \qquad -(1)$$
$$Again,\ S_{n+1} = \sum_{0\le k\le n+1} (-1)^{n+1-k}$$
$$= (-1)^{n+1} + \sum_{1\le k\le n+1} (-1)^{n+1-k}$$
$$= (-1)^{n+1} + \sum_{0\le k\le n} (-1)^{n-k}$$
$$= (-1)^{n+1} + S_n \qquad -(2)$$
$$(1),(2) \implies 2S_n = 1 - (-1)^{n+1}$$
$$\implies S_n = (1 - (-1)^{n+1})/2 \quad i.e. \quad S_n = [n\ is\ even]$$

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

$$\begin{aligned}
T_{n+1} &= \sum_{0\le k\le n+1}(-1)^{n+1-k}k \\
&= \sum_{0\le k\le n}(-1)^{n+1-k}k + (-1)^{n+1-(n+1)}(n+1) \\
&= n+1-T_n \qquad\qquad -(1) \\
\textit{Again, } T_{n+1} &= \sum_{0\le k\le n+1}(-1)^{n+1-k}k \\
&= (-1)^{n+1}\cdot 0 + \sum_{1\le k\le n+1}(-1)^{n+1-k}k \\
&= 0 + \sum_{0\le k\le n}(-1)^{n-k}(k+1) \\
&= \sum_{0\le k\le n}(-1)^{n-k}(k) + \sum_{0\le k\le n}(-1)^{n-k} \\
&= T_n + S_n \qquad -(2) \\
(1),(2) &\implies 2T_n = n+1-S_n \\
&\implies T_n = (n+1-S_n)/2 \quad \textit{i.e.} \quad T_n = (n+[n\ is\ odd])/2
\end{aligned}$$

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

$$\begin{aligned}
U_{n+1} &= \sum_{0\le k\le n+1}(-1)^{n+1-k}k^2 \\
&= \sum_{0\le k\le n}(-1)^{n+1-k}k^2 + (-1)^{n+1-(n+1)}(n+1)^2 \\
&= (n+1)^2 - U_n \qquad\qquad -(1) \\
\textit{Again, } U_{n+1} &= \sum_{0\le k\le n+1}(-1)^{n+1-k}k^2 \\
&= (-1)^{n+1}\cdot 0^2 + \sum_{1\le k\le n+1}(-1)^{n+1-k}k^2 \\
&= 0 + \sum_{0\le k\le n}(-1)^{n-k}(k+1)^2 \\
&= \sum_{0\le k\le n}(-1)^{n-k}k^2 + \sum_{0\le k\le n}(-1)^{n-k}(2k) + \sum_{0\le k\le n}(-1)^{n-k} \\
&= U_n + 2T_n + S_n \qquad -(2) \\
(1),(2) &\implies 2T_n = (n+1)^2 - 2T_n - S_n \\
&\implies U_n = ((n+1)^2 - (n+1-S_n) - S_n)/2 \\
&\implies U_n = n(n+1)/2
\end{aligned}$$

P22: i. Prove Lagrange's identity (without using induction):

$$\sum_{1\le j<k\le n}(a_jb_k - a_kb_j)^2 = (\sum_{1\le k\le n}a_k^2)(\sum_{1\le k\le n}b_k^2) - (\sum_{1\le k\le n}a_kb_k)^2$$

ii. Prove, in fact, an identity for the more general double sum

$$\sum_{1\le j<k\le n}(a_jb_k - a_kb_j)(A_jB_k - A_kB_j)$$

Ans:

i Proof of $\sum_{1\le j<k\le n}(a_jb_k - a_kb_j)^2 = (\sum_{1\le k\le n} a_k^2)(\sum_{1\le k\le n} b_k^2) - (\sum_{1\le k\le n} a_kb_k)^2$

$$
\begin{aligned}
Let,\ S_n &= \sum_{1\le j<k\le n}(a_jb_k - a_kb_j)^2 \\
Now,\ \sum_{1\le j,k\le n}(a_jb_k - a_kb_j)^2 &= 2S_n - \sum_{1\le j=k\le n}(a_jb_k - a_kb_j)^2 = 2S_n + 0 \\
\therefore S_n &= \frac{1}{2}\sum_{1\le j,k\le n}(a_jb_k - a_kb_j)^2 \\
&= \frac{1}{2}\sum_{1\le j\le n}\sum_{1\le k\le n}(a_jb_k)^2 - 2a_jb_ka_kb_j + (a_kb_j)^2 \\
&= \frac{1}{2}[(\sum_{1\le j\le n} a_j^2)(\sum_{1\le k\le n} b_k^2) + (\sum_{1\le k\le n} a_k^2)(\sum_{1\le j\le n} b_j^2) - 2(\sum_{1\le j\le n} a_jb_j)(\sum_{1\le k\le n} a_kb_k) \\
&= \frac{1}{2}[2(\sum_{1\le k\le n} a_k^2)(\sum_{1\le k\le n} b_k^2) - 2(\sum_{1\le k\le n} a_kb_k)^2] \\
\implies S_n &= (\sum_{1\le k\le n} a_k^2)(\sum_{1\le k\le n} b_k^2) - (\sum_{1\le k\le n} a_kb_k)^2 \qquad \textbf{\textit{(Proved)}}
\end{aligned}
$$

ii Derivation of $\sum_{1\le j<k\le n}(a_jb_k - a_kb_j)(A_jB_k - A_kB_j)$

$$
\begin{aligned}
Let,\ T_n &= \sum_{1\le j<k\le n}(a_jb_k - a_kb_j)(A_jB_k - A_kB_j) \\
Now,\ \sum_{1\le j,k\le n}(a_jb_k - a_kb_j)(A_jB_k - A_kB_j) &= 2T_n - \sum_{1\le j=k\le n}(a_jb_k - a_kb_j)(A_jB_k - A_kB_j) = 2T_n + 0 \\
\therefore T_n &= \frac{1}{2}\sum_{1\le j,k\le n}(a_jb_k - a_kb_j)(A_jB_k - A_kB_j) \\
&= \frac{1}{2}\sum_{1\le j\le n}\sum_{1\le k\le n}(a_jb_kA_jB_k - a_jb_kA_kB_j - a_kb_jA_jB_k + a_kb_jA_kB_J) \\
&= \frac{1}{2}[(\sum_{1\le j\le n} a_jA_j)(\sum_{1\le k\le n} b_kB_K) + (\sum_{1\le k\le n} a_kA_k)(\sum_{1\le j\le n} b_jB_j) \\
&\qquad - (\sum_{1\le j\le n} a_jB_j)(\sum_{1\le k\le n} A_kb_k) - (\sum_{1\le j\le n} A_jb_j)(\sum_{1\le k\le n} a_kB_k) \\
&= \frac{1}{2}[2(\sum_{1\le k\le n} a_kA_k)(\sum_{1\le k\le n} b_kB_k) - 2(\sum_{1\le k\le n} a_kB_k)\sum_{1\le k\le n} A_kb_k)] \\
\implies T_n &= (\sum_{1\le k\le n} a_kA_k)(\sum_{1\le k\le n} b_kB_k) - (\sum_{1\le k\le n} a_kB_k)(\sum_{1\le k\le n} A_kb_k) \qquad \textbf{\textit{(Proved)}}
\end{aligned}
$$

P23: Evaluate the sum $\sum_{1\le k\le n}(2k+1)/k(k+1)$

Ans:

$$
\begin{aligned}
&\sum_{1\le k\le n}(2k+1)/k(k+1) \\
&= \sum_{1\le k\le n}[\frac{1}{k} + \frac{1}{k+1}] \\
&= 2\sum_{1\le k\le n}\frac{1}{k} + \frac{1}{n+1} - 1 \quad = 2H_n - \frac{n}{n+1}
\end{aligned}
$$

P25: The notation $\prod_{k\in K} a_k$ means the product of the numbers a_k for all $k \in K$. What laws does this Q-notation satisfy, analogous to the distributive, associative, and commutative laws that hold for $\sum$?

Ans: There are the following rules for products:

i. $\prod a^c = (\prod a)^c$ [***Distributive***]

ii. $\prod a_k b_k = (\prod a_k)(\prod b_k)$ [***Associative***]

iii. $\prod a^c = (\prod a)^c$ [***Commutative***]

iv. $\prod_{1\le i\le k} c = \prod c^k$

v. $\prod_{k\in K} a_k = \prod a_k^{[k\in K]}$

P26: Express the double product $\prod_{1\le j\le k\le n} a_j a_k$ in terms of the single product $\prod_{1\le k\le n} a_k$ by manipulating $\prod$ notation

Ans:

$$
\begin{aligned}
Let,\ P &= \prod_{1\le j\le k\le n} a_j a_k \\
P\cdot P &= \prod_{1\le j,k\le n} a_j a_k \cdot \prod_{1\le j=k\le n} a_j a_k \\
&= (\prod_{1\le j\le n} a_j)(\prod_{1\le k\le n} a_k)(\prod_{1\le k\le n} a_k^2) \\
&= (\prod_{1\le k\le n} a_k^n)^2 \cdot (\prod_{1\le k\le n} a_k^2) \\
P^2 &= (\prod_{1\le k\le n} a_k^{n+1})^2 \\
\implies P &= \prod_{1\le k\le n} a_k^{n+1} \quad \textbf{\textit{(Proved)}}
\end{aligned}
$$

P29: Evaluate the sum $\sum_{1\le k\le n}(-1)^k k/4k^2-1$

Ans:

$$
\begin{aligned}
&\sum_{1\le k\le n} (-1)^k k/4k^2-1 \\
&= \sum_{1\le k\le n} (-1)^k \frac{1}{4}\left(\frac{1}{2k+1}+\frac{1}{2k-1}\right) \\
&= \frac{1}{4}\left(-1-\frac{1}{3}+\frac{1}{3}+\frac{1}{5}\cdots+(-1)^{n-1}\frac{1}{2n-3}+(-1)^{n-1}\frac{1}{2n-1}+(-1)^n\frac{1}{2n-1}+(-1)^n\frac{1}{2n+1}\right) \\
&= \frac{1}{4}\left((-1)^n\frac{1}{2n+1}-1\right)
\end{aligned}
$$

P30: Find the number of ways to represent 1050 as a sum of consecutive positive integers.

Ans: We try to find a generalized formula.

- Let N be the given number.
- Let $N = m + m + 1 + \cdots + n$ be a general representation.

- Thus $N = \frac{1}{2}(n(n+1) - m(m-1)) = \frac{1}{2}(n^2 + n - m^2 - m) = \frac{1}{2}(n+m)(n-m+1)$
- $\therefore 2N = (n+m)(n-m+1)$
- since $n + m \not\equiv n - m + 1$ and LHS is even, thus we need to break 2N in two parts of opposite parity. ***This means the total number of representations is the total number of unique odd factors of 2N***.
- Thus, $ans = \prod_k (p_k+1)$ where $N = 2^x \cdot \prod_k q_k^{p_k}$ where q_k is a prime not equal to 2, and $q_i \neq q_j \iff i \neq j$
- for our specific example, $2 \cdot 1050 = 2^2 \cdot 3 \cdot 5^2 \cdot 7$ and $ans = (1+1) \cdot (2+1) \cdot (1+1) = 12$

Chapter 4 (Extra)

P1: What is the largest positive integer n for which $n^3 + 100$ is divisible by $n + 10$?

Ans:

$$
\begin{aligned}
Let \quad & k = n + 10 \\
& \therefore n^3 = (k-10)^3 = k^3 - 30k^2 + 300k - 1000 \\
\implies & n^3 + 100 = k^3 - 30k^2 + 300k - 900 \\
\implies & n^3 + 100 = k(k^2 + 30k + 300) - 900
\end{aligned}
$$

Now, $k \mid k(k^2 + 30k + 300)$
Thus, largest k that divides $n^3 + 100 = k(k^2 + 30k + 300) - 900$ is **900** *(Ans)*

P2: Show that the fraction $\frac{12n+1}{30n+2}$ is irreducible for all positive integers n.

Ans:

$$
\begin{aligned}
& 30n + 2 \equiv 6n + 1 \pmod{12n+1} \\
\implies & 12n + 1 \equiv 6n \pmod{6n+1} \\
\implies & 6n + 1 \equiv 1 \pmod{6n} \\
\implies & gcd(30n+2, 12n+1) = 1 \qquad [\textit{by the Euclidean alogrithm}]
\end{aligned}
$$

Therefore, the given fraction is irreducible for all positive integers n ***(Proved)***

P3: 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?

Ans:

$$
\begin{aligned}
Let \quad A_0 &= \left\lfloor \frac{999}{2} \right\rfloor + \left\lfloor \frac{999}{3} \right\rfloor + \left\lfloor \frac{999}{5} \right\rfloor - \left\lfloor \frac{999}{6} \right\rfloor - \left\lfloor \frac{999}{10} \right\rfloor - \left\lfloor \frac{999}{15} \right\rfloor + \left\lfloor \frac{999}{30} \right\rfloor \\
&= 733 \qquad (\textit{numbers divisible by } 2,\ 3 \textit{ or } 5\ , \textit{by inclusion} - \textit{exclusion principle}) \\
A_1 &= A_0 - (168 - 3) = 101 \qquad (\textit{remove primes except } 2,\ 3,\ 5) \\
A_2 &= A_1 - 1 = 100 \qquad (1 \textit{ is not a prime}) \\
\therefore \ & \boldsymbol{ans} = 100
\end{aligned}
$$

P4: Let m and n be positive integers such that $lcm(m,n) + gcd(m,n) = m + n$. Prove that one of the two numbers is divisible by the other.

Ans:

$$
\begin{aligned}
&Let \quad gcd(m,n) = g \\
&\quad \therefore m = gm',\ n = gn',\ lcm(m,n) = gm'n' \qquad [where\ m' \perp n'] \\
&\quad \therefore lcm(m,n) + gcd(m,n) = gm'n' + g = g(m'n' + 1) \\
&\quad \therefore m + n = g(m'n' + 1) \qquad [Given] \\
&\implies g(m' + n') = g(m'n' + 1) \\
&\implies m' + n' - m'n' + 1 = 0 \\
&\implies m'(1 - n') - 1(1 - n') = (m' - 1)(1 - n') \\
&\quad \therefore if\ m' = 1, then\ m = g,\ and\ m \mid n \\
&again\ if\ n' = 1, then\ n = g,\ and\ n \mid m
\end{aligned}
$$

Thus, in either case, we see that one of the numbers m,n is divisible by the other. ***(Ans)***

P5: Show that for any positive integers a and b, the number $(36a+b)(a+36b)$ cannot be a power of 2.

Ans:

$$
\begin{aligned}
&Let, \quad (36a + b)(36b + a)\ be\ a\ power\ of\ 2 \\
&\quad \therefore (36a + b)(36b + a) = 2^m \qquad [m \in \mathbb{Z}^+] \\
&\quad \therefore (36a + b) = 2^n\ and\ (36b + a) = 2^l \qquad [n, l \in \mathbb{Z}^+\ and\ a, b \neq 0] \\
&\quad \therefore a \equiv b \equiv 0(\mod 2) \\
&Let \quad a = 2a',\ b = 2b' \qquad [a', b' \in \mathbb{Z}^+] \\
&\quad \therefore (36a + b)(36b + a) = 4(36a' + b')(36b' + a') = 2^m \\
&\implies (36a' + b')(36b' + a') = 2^{m-2} = 2^{m'} \qquad [m \in \mathbb{Z}^+]
\end{aligned}
$$

The same argument can be applied to the statement $(36a+b)(36b+a) = 2^m$ an infinite number of times, thus leading to no solution.
Therefore, the expression $(36a+b)(36b+a)$ cannot be a power of 2 for positive a, b [*by contradiction*] ***(Proved)***

P6: Find all positive integers n for which $n! + 5$ is a perfect cube.

Ans:

$$
\begin{aligned}
n^6 &\equiv 1 \pmod 7 \qquad [if\ n \perp 7, By\ FLT] \\
again, n^6 &\equiv 0 \pmod 7 \qquad [if 7 \mid n] \\
\therefore n^6 &\equiv 0, 1 \pmod 7 \\
\implies n^3 &\equiv 0, \pm 1 \pmod 7 \\
now,\ for\ n &\geq 7 \\
n! &\equiv 0 \pmod 7 \\
n! + 5 &\equiv 5 \pmod 7 \\
Thus, n! + 5 &\not\equiv 0, \pm 1 \pmod 7 \\
And, n! + 5\ &can't\ be\ a\ perfect\ cube\ when\ n \geq 7
\end{aligned}
$$

By exhaustive searching $n \leq 6$, we find $n = 5$ gives $n! + 5 = 125$, which is 5^3. Thus $n = 5$ is the only solution.

P7: Let n be an integer greater than three. Prove that $1! + 2! + \cdots + n!$ cannot be a perfect power.

Ans:

$$1! + 2! + \cdots + 8! \text{ is a multiple of } 3^2 \text{ and not } 3^3$$

$$\text{Again}, \forall n \geq 9,\ 3^3 \mid n!$$

$$\text{Thus}, \forall n \geq 9,\ 3^3 \nmid \sum_{i=1}^{n} i! \text{ but } 3^2 \mid \sum_{i=1}^{n} i!$$

$$\text{Thus}, \forall\ n \geq 3,\ \sum_{i=1}^{n} i! \text{ can at most be a perfect square}$$

Manually checking the possibilities from $n = 3$ to $n = 8$ we see that only for $n = 3$, $\sum_{i=1}^{n} i! = 9$ is a perfect square.
Thus the answer is 3;

P8: Let p be a prime. Show that there are infinitely many positive integers such that $p \mid 2^n - n$

Ans: $p = 2$ divides $2^n - n$ for all $n \equiv 0 \pmod 2$
Now, let p be any odd prime

$$\begin{aligned}
& p - 1 \equiv -1 \pmod p \\
\implies & (p-1)^2 \equiv 1 \pmod p \\
\implies & ((p-1)^2)^k \equiv 1 \pmod p \\
\implies & (p-1)^{2k} \equiv 1 \pmod p \\
\text{Again}, & 2^{p-1} \equiv 1 \pmod p \quad [\text{By FLT}] \\
& (2^{p-1})^m \equiv 2^{(p-1)m} \equiv 1^m \equiv 1 \pmod p \\
\text{now, let } & m = (p-1)^{2k-1} \\
\text{thus}, & 2^{(p-1)m} \equiv 2^{(p-1)(p-1)^{2k-1}} \equiv 1 \pmod p \\
\implies & 2^{((p-1)^{2k}} \equiv 1 \equiv (p-1)^{2k} \pmod p \\
\implies & 2^n \equiv n \pmod p \quad \text{where } n = (p-1)^{2k}
\end{aligned}$$

P9: Prove that $a^p \equiv a \pmod p$, where p is any prime.

Ans: Case 1: $a \not\perp p$

$$\text{Then, } p \mid a \quad \text{and } a^p \equiv a \equiv 0 \pmod p$$

Case 2: $a \perp p$ Then, residue class of p contains $0, 1, 2 \cdots (p-1)$
Multiplying by $a \in \mathbb{Z}^+$, the class $0a, 1a, 2a \cdots (p-1)a$ maps to the original residue class $0, 1, 2 \cdots (p-1)$
Taking product of all the terms except 0, we have,

$$\begin{aligned}
& a.2a.3a.\cdots.(p-1)a \equiv 1.2.\cdots(p-1) \pmod p \\
\implies & (p-1)!a^{p-1} \equiv (p-1)! \pmod p \\
\implies & a^{p-1} \equiv 1 \pmod p \quad [\text{since } \forall i < \text{prime } p,\ i \nmid p] \\
\implies & a^p \equiv a \pmod p \quad [\text{multiply by } a] \quad \textbf{\textit{(Proved)}}
\end{aligned}$$

P10: Find all prime numbers p and q for which pq divides the product $(5^p - 2^p)(5^q - 2^q)$.

Ans: Both p and q coprime to 2 and 5
Case:1 Without loss of generality, assume $p \mid 5^p - 2^p$

$$\implies 5^p \equiv 2^p \pmod{p}$$
$$\implies 5.5^{p-1} \equiv 2.2^{p-1} \pmod{p}$$
$$\implies 5.1 \equiv 2.1 \pmod{p} \quad [By/; FLT]$$
$$\implies p \mid 5 - 2 = 3, \quad \therefore p = 3$$
$$Now, 5^p - 2^p = 5^3 - 2^3 = 117 = 3^2.13$$
$$Again, pq \mid (5^p - 2^p)(5^q - 2^q) = (3^2)(13)(5^q - 2^q) \implies 3q \mid (3^2)(13)(5^q - 2^q) \implies q \mid (3)(13)(5^q - 2^q)$$

Leaving (p,q) = (3,3) and (3,13) as solutions when $q \mid (3)(13)$
And by symmetry we have (13,3) as a solution when $q \mid 5^q - 2^q$.

Case 2: $p \mid 5^q - 2^q$ and $p \nmid 5^p - 2^p$, and Vice-versa

$$5^{p-1} \equiv 2^{p-1} \equiv 1 \pmod{p}$$
$$\therefore 5^{gcd(q,p-1)} \equiv 2^{gcd(q,p-1)} \pmod{p}$$

Case 2.1: gcd(q,p-1) = 1
Then, $5 \equiv 2 \pmod{p}$ which gives us $p = 3$, and $q = 3, 13$ as above
Case 2.2: gcd(q,p-1) ¿ 1 and gcd(p,q-1) ¿ 1
Then, $q \mid p - 1$ and $p \mid q - 1$ (as p,q are primes)
Thus, $p > q > p$ which is a contradiction.

Therefore the solutions are (3,3), (3,13) and (13,3)

P11: Evaluate $gcd(n! + 1, (n + 1)! + 1)$

Ans: Let, gcd be g and $k = n!$

$$g \mid k + 1 \quad and g \mid (n + 1)k + 1$$
$$\implies k \equiv (n + 1)k \equiv -1 \pmod{g}$$
$$\implies (n + 1)k \equiv -1 \implies n + 1 \equiv 1 \implies n \equiv 0 \pmod{g} \implies g \mid n \implies g \mid n!$$
$$Again, g \mid n! + 1$$

Thus, $g = 1$ ***(Ans)***

P12: Find the smallest positive integer whose cube ends in 888

Ans: Let x be the smallest integer s.t $x^3 \equiv 888 \pmod{1000}$

$$x = (10y + e) \implies x^3 = 1000y^3 + 300y^2e + 30ye^2 + e^3$$
$$[where\ y, e \in \mathbb{Z}^+ \ and\ e\ in\ \{0, 2, 4, 6, 8\}$$
$$x^3 \equiv e^3 \equiv 8 \pmod{10} \implies e = 2 \implies x^3 = 1000y^3 + 600y^2 + 120y + 8$$
$$Now,\ x_1 = \left\lfloor \frac{x^3}{10} \right\rfloor = 100y^3 + 60y^2 + 12y$$
$$now,\ x_1 \equiv 12y \equiv 2y \equiv 8 \pmod{10} \implies y\ ends\ in\ 4\ or\ 9$$

Manually trying out values of y as 4,9,14,19 we see $y = 19$ gives $x = 192$ and $x^3 = 7077888$
Thus our answer is 192 ***(Ans)***

P13: Let $p \geq 3$ be a prime, and let $a_1, a_2, \cdots, a_{p-1}$ and $b_1, b_2, , b_{p-1}$ be two sets of complete residue classes *modulo p*. Prove that $a_1b_1, a_2b_2, , a_{p-1}b_{p-1}$ is not a complete set of residue classes *modulo p*

Ans:

$$(p-1)! \equiv a_1 \cdot a_2 \cdots a_{p-1} \equiv b_1 \cdot b_2 \cdots b_{p-1} \equiv -1 \pmod p \qquad [By\ Wilson's\ Theorem]$$
$$\implies a_1 \cdot a_2 \cdots a_{p-1} \cdot b_1 \cdot b_2 \cdots b_{p-1} \equiv a_1b_1 \cdot a_2b_2 \cdots a_{p-1}b_{p-1} \equiv 1 \pmod p$$
$$now, 1 \not\equiv -1 \pmod p\ [if\ p \geq 3] \implies a_1b_1 \cdot a_2b_2 \cdots a_{p-1}b_{p-1} is\ not\ a\ residue\ class \qquad [By\ Wilson's\ Theorem\ ]$$

P14: Let $n > 1$ be an odd integer. Prove that n does not divide $3^n + 1$

Ans:

$$Let, n \mid 3^n + 1\ and\ p\ be\ the\ smallest\ prime\ factor\ of\ n$$
$$3^n \equiv -1 \pmod p \implies (3^n)^2 \equiv (-1)^2 \pmod p \implies 3^{2n} \equiv 1 \equiv 3^{p-1} \pmod p\ [By\ FLT]$$
$$gcd(2n, p-1) = 2 \qquad [p-1\ is\ even]$$
$$\implies 3^{gcd(2n,p-1)} \equiv 1 \pmod p \implies 3^2 \equiv 1 \pmod p \implies p \mid 3^2 - 1 \implies p \mid 8 \implies p = 2 \qquad [which\ is\ a\ contradiction]$$

Thus $n \nmid 3^n + 1$, for odd $n > 1$ ***(Proved)***

Chapter 4

P2: Prove that $gcd(m, n) \cdot lcm(m, n) = m \cdot n$, and use this identity to express $lcm(m, n)$ in terms of $lcm(n \bmod m, m)$, when $n \bmod m \neq 0$

Ans: Let, $gcd(m, n) = g$; then $m = gm'$ and $n = gn'$ where $m' \perp n'$; $lcm(m, n) = gm'n'$
now, RHS $= m \cdot n = gm' \cdot gn' = g^2m'n'$
LHS $= lcm(m, n) \cdot gcd(m, n) = gm' \cdot gn' = g^2m'n' =$ RHS ***(Proved)***

$$\therefore gcd(m, n) \cdot lcm(m, n) = m \cdot n \implies gcd(m, n) = \frac{m \cdot n}{lcm(m,n)}$$

again, $gcd(m, n) = gcd(n \bmod m) = g$
now, $gcd(n \bmod m) \cdot lcm(n \bmod m) = m \cdot (n \bmod m)$

$$\therefore lcm(n \bmod m) = \frac{m \cdot (n \bmod m)}{gcd(n \bmod m)} = \frac{m \cdot (n \bmod m)}{\frac{m \cdot n}{lcm(m,n)}} = \frac{m \cdot (n \bmod m)(lcm(m,n))}{m \cdot n}$$

P14(a): Prove or disprove $gcd(km, kn) = kgcd(m, n)$

$$Let, gcd(m, n) = g;\ then, m = gm';\ n = gn' \qquad [where\ m' \perp n',\ i.e\ gcd(m', n') = 1,\ lcm(m', n') = m'n']$$
$$Now, LHS = gcd(km, kn) = gcd(kgm', kgn') = kg \cdot gcd(m', n') = kg \cdot 1 = k \cdot gcd(m, n) = RHS$$ **(Proved)**

P14(b): Prove or disprove $lcm(km, kn) = klcm(m, n)$

$$Now, LHS = lcm(km, kn) = lcm(kgm', kgn') = kg \cdot lcm(m', n') = kg \cdot m'n' = k \cdot lcm(m, n) = RHS$$ **(Proved)**

P18: Show that if $2^n + 1$ is prime then n is a power of 2

Ans: Let, $n = mq$ where $m = 2^k\ and k, q \in \mathbb{Z}^+ \cup \{0\}\ and\ q > 1$ if q is odd, then,

$$2^n + 1 = 2^{mq} + 1 = (2^m)^q + 1^q = (2^m + 1)(2^{n-m} - 2^{n-2m} + \cdots - 2^m + 1)$$

which is clearly not a prime since there is a factor $(2^m + 1)$ Thus, n cannot be written as $n = mq$ where there is an odd $q > 1$, thus n must be a power of 2 ***(Proved)***

P24: Express $\epsilon_p(n!)$ in terms of $V_p(n)$, the sum of the digits in the radix p

Ans: Let m_i^{th} digit be d_i. Then this d_i contributes the following to $\epsilon_p(n!)$

$$d_i p^{m_i-1} + d_i p^{m_i-2} + \cdots + d_i p + d_i = d_i \frac{p^{m_i}-1}{p-1}$$

Now, $\epsilon_p(n!)$ = Sum of all such contributions from $d_i s$ =

$$\sum_i d_i \frac{p^{m_i}-1}{p-1} = \frac{\sum_i d_i p^{m_i} - \sum_i d_i}{p-1} = \frac{n - V_p(n)}{p-1}$$

P30: Prove the following statement (the Chinese Remainder Theorem): Let $m_1, \cdots, m_r$ be integers with $m_j \perp m_k$ for $1 \leq j < k \leq r$; let $m = m_1 \cdots m_r$; and let $a_1, \cdots, a_r, A$ be integers. Then there is exactly one integer a such that $a \equiv a_k (mod\ m_k)$ for $1 \leq k \leq r$ and $A \leq a < A + m$.

Ans:
There are m integers between $[A, A+m)$
They will all have different remainders $mod\ m$ and will thus make up a residue class
Again, each m_i has exactly m_i distinct elements in its residue class.
And thus, number of distinct n-tuples of the form

$$(x\ mod\ m_1, x\ mod\ m_2, \cdots x\ mod\ m_r) = m_1 m_2 \cdots m_r = m$$

Thus exactly one such x must yield a tuple equal to $(a_1, a_2 \cdots a_r)$ ***[Proved]***

P31: A number in decimal notation is divisible by 3 if and only if the sum of its digits is divisible by 3. Prove this well-known rule, and generalize it.

Ans:

$$\begin{aligned}
& 10 \equiv 1\ (mod\ 3) \\
\iff & 10^k \equiv 1^k \equiv 1\ (mod\ 3) \\
\iff & 10^k d_k \equiv d_k\ (mod\ 3) \\
\iff & \sum_k 10^k d_k \equiv sum_k d_k\ (mod\ 3) \\
\therefore & n \equiv \sum_k d_k\ (mod\ 3)
\end{aligned}$$

Thus, a number is divisible by 3 if sum of it's digits is divisible by 3 ***(Proved)***

Generalized: A number in radix b will be divisible by another number d iff sum of its digits are divisible by d, only when $b \equiv 1\ (mod\ d)$b b

P32: Prove Euler's theorem

Euler's Theorem: if $a \perp m$ then, $a^{\phi(m)} \equiv 1\ (mod\ m)$
Proof:
Let $\{k_1, k_2 \cdots k_{\phi(m)}\}$ be a reduced residue system $mod\ m$
$\{ak_1, ak_2 \cdots ak_{\phi(m)}\}$ is also a reduced residue system $mod\ m$
$\therefore k_1 k_2 \cdots k_{\phi(m)} \equiv ak_1 ak_2 \cdots ak_{\phi(m)}\ (mod\ m)$
$\implies k_1 k_2 \cdots k_{\phi(m)} \equiv a^{\phi(m)} k_1 k_2 \cdots k_{\phi(m)}\ (mod\ m)$
$\implies a^{\phi(m)} \equiv 1\ (mod\ m)$ ***(Proved)***

P38: Prove that if $a \perp b$ and $a > b$ then gcd$(a^m - b^m, a^n - b^n) = a^{gcd(m,n)} - b^{gcd(m,n)}$ [where $0 \leq m < n$]

Ans:

$$(a^n - b^n) = (a^m - b^m)(a^{n-m}b^0 + a^{n-2m}b^m + \cdots + a^{nmodm}b^{n-m-nmodm}) + b^{m\lfloor n/m \rfloor}(a^{nmodm} - b^{nmodm})$$

Here, $a^n - b^n \equiv b^{m\lfloor n/m \rfloor}(a^{nmodm} - b^{nmodm})\ (mod\ (a^m - b^m))$
Again, $(a^m - b^m) \perp b^{m\lfloor n/m \rfloor}$ so $b^{m\lfloor n/m \rfloor}$ not a factor of $gcd(a^m - b^m, a^n - b^n)$
Therefore, $gcd(a^m - b^m, a^n - b^n) = gcd(a^{nmodm} - b^{nmodm}, a^m - b^m)$ [analogous to the euclidean algorithm]
Therefore, finally we get, $gcd(a^m - b^m, a^n - b^n) = gcd(a^0 - b^0, a^{gcd(m,n)} - b^{gcd(m,n)}) = a^{gcd(m,n)} - b^{gcd(m,n)}$
(Proved)

P41a: Show that if $p\ mod\ 4 = 3$, there is no integer n such that p divides $n_2 + 1$

Ans:

$$p \equiv 3\ (mod\ 4) \implies p - 1 \equiv 2\ (mod\ 4) \implies (p-1)/2 \equiv 1\ (mod\ 2) \implies \text{(p-1)/2 is odd}$$

Proof by Contradiction:

$$let, p \mid n^2 + 1 \iff n^2 \equiv -1\ (mod\ p) \iff (n^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}\ (mod\ p) \iff n^{p-1} \equiv -1\ (mod\ p)$$

$$but, n^{p-1} \equiv 1\ (mod\ p), \text{by FLT, which is a contradiction, thus completing the proof.}$$

P41b: But show that if $p\ mod\ 4 = 1$, there is such an integer.

Ans:

$$p \equiv 1\ (mod\ 4) \implies p - 1 \equiv 0\ (mod\ 4) \implies (p-1)/2 \equiv 0\ (mod\ 2) \implies \text{(p-1)/2 is even}$$

$$let, n = ((p-1)/2)! \implies n \equiv (-1)^{(p-1)/2} \prod_{1 \leq k \leq \frac{p-1}{2}} (p-k) = 1 \cdot \frac{(p-1)!}{(\frac{p-1}{2})!} = \frac{(p-1)!}{n}$$

$$\implies n^2 \equiv (p-1)! \equiv -1\ (mod\ p) \quad [By\ Wilson's\ Theorem]$$

Thus, $p \mid n^2 + 1$ when n = $(\frac{p-1}{2})!$ ***(Proved)***

P42: Consider two fractions m/n and m'/n' in lowest terms. Prove that when the sum $m/n + m'/n'$ is reduced to lowest terms, the denominator will be nn' if and only if $n \perp n'$. (In other words, $(mn' + m'n)/nn'$ will already be in lowest terms if and only if n and n' have no common factor.)

Ans: $m/n + m'/n' = (mn' + m'n)/nn'$ and $k \perp l \iff k \perp (l + ak)$

$$m \perp n\ and\ n' \perp n \iff mn' \perp n \iff mn' + nm' \perp n$$
$$m' \perp n'\ and\ n' \perp n \iff mn' \perp n' \iff mn' + nm' \perp n'$$
$$m \perp n\ and\ m' \perp n'\ and\ n' \perp n \iff mn' + nm' \perp nn' \quad \textbf{\textit{(Proved)}}$$

P46a: Prove that if $n^j \equiv 1$ and $n^k \equiv 1 \quad (mod\ m)$, then $n^{gcd(j,k)} \equiv 1$

Ans: Let, $jj' - kk' = gcd(j,k) \implies jj' = gcd(j,k) + kk'$

$$n^j \equiv n^{jj'} \equiv 1,\ and\ n^k \equiv n^{kk'} \equiv 1\ (mod\ m)$$
$$n^{jj'} \equiv n^{gcd(j,k)+kk'} \equiv n^{kk'} \cdot n^{gcd(j,k)} \equiv n^{gcd(j,k)} \equiv 1\ (mod\ m)\ \textbf{\textit{(Proved)}}$$

P46b: Show that $2^n \not\equiv 1 \pmod n$, if $n > 1$.

Ans: Let $n = pq$ where p is the smallest prime factor of n. Thus $gcd(p-1, n) = 1$
Proof by contradiction:

$$\begin{aligned} &Let, 2^n \equiv 1 \ (mod\ n) \implies 2^n \equiv 1 \ (mod\ p) \\ &Again, 2^{p-1} \equiv 1 \ (mod\ p) \\ &\therefore 2^{gcd(p-1,n)} \equiv 1 \ (mod\ p) \quad [by\ 46a] \\ &\implies 2 \equiv 1 \ (mod\ p) \quad [which\ is\ a\ Contradiction] \end{aligned}$$

Chapter 7

P1: An eccentric collector of 2 × n domino tilings pays \$4 for each vertical domino and \$1 for each horizontal domino. How many tilings are worth exactly \$m by this criterion?

Ans:

- Let V be a vertical tile and H be two stacked horizontal tiles
- If T is collection of all possible tilings for a $2xn$ board, then $T = \frac{1}{1-V-H}$ with a generating function of $G(z) = \frac{1}{1-z-z^2}$ where $[z^n]G(z) = F_{n+1}$ where F_n is the nth Fibonacchi number starting from $F_1 = F_2 = 1$
- Since each vertical domino costs 4 and a pair of horizontal costs 2, The cost generating function becomes $C(z) = \frac{1}{1-z^4-z^2}$ which is just $G(z^2)$
- Thus, cost for 2 x n tiling, $[z^n]C(z) = \begin{cases} 0, & \text{if } n \text{ odd} \\ [z^n/2]G(z) = F_{n/2+1}, & \text{if } n \text{ is even} \end{cases}$

P7: Solve the recurrence:

$$\begin{aligned} &g_0 = 1; \\ &g_n = g_{n-1} + 2g_{n-2} + \cdots + ng_0, \textbf{for } n > 0 \end{aligned}$$

Ans:

- The combined equation becomes

$$\begin{aligned} g_n &= g_{n-1} + 2g_{n-2} + \cdots + ng_0 + [n=0] \\ &\implies \sum z^n g_n = \sum z^n g_{n-1} + \sum z^n 2g_{n-2} + \cdots + \sum z^n n g_0 + \sum z^n [n=0] \\ &\implies \sum z^n g_n = \sum z^{n+1} g_n + \sum z^{n+2} 2g_n + \cdots + \sum z^{2n} n g_n + \sum z^n [n=0] \\ &\implies G(z) = G(z)(z + 2z^2 + 3z^3 \cdots) + 1 = \frac{z}{(1-z)^2} G(z) + 1 \\ &\implies G(z)(1 - \frac{z}{(1-z)^2}) = 1 \implies G(z) = \frac{1 - 2z + z^2}{1 - 3z + z^2} = 1 + \frac{z}{1 - 3z + z^2} \end{aligned}$$

- Comparing with $G(z) = T(z) + S(z)$ and $S(z) = \frac{P(z)}{Q(z)}$, we get
  - $T(z) = 1$
  - $P(z) = z$
  - $Q(z) = 1 - 3z + z^2$
- $Q^R = 1 - 3z + z^2$ and roots of Q^R are $\rho_1 = \frac{3+\sqrt{5}}{2}$ and $\rho_2 = \frac{3-\sqrt{5}}{2}$

- $Q' = 2z - 3$
- $a = \frac{-\rho + P(1/\rho)}{Q'(1/\rho)} = \frac{-\rho + 1/\rho}{2/\rho - 3} = \frac{\rho}{3 - 2\rho}$
- $a_1 = 1/\sqrt{5}$, $a_2 = -1/\sqrt{5}$
- $[z^n]G(z) = a_1\rho_1^n + a_2\rho_2^n = \frac{1}{\sqrt{5}}\left[\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right]$ ***(Ans)***

P8: What is $[z^n](ln(1-z))^2/(1-z)^{m+1}$?

Ans:

- Let $P(n) = (1-z)^{n+1}$
- Now, $\frac{d}{dn}P(n) = ln|1-z|(1-z)^{n+1}$
- $\frac{d^2}{dn^2}P(n) = (ln|1-z|)^2(1-z)^{n+1}$
- $P(n) = (1-z)^{n+1} = \sum_k \binom{n+k}{k} z^k$
- Differentiating, $\frac{d}{dn}P(n)$

$$\begin{aligned}
&\frac{d}{dn}\sum_k \binom{n+k}{k} z^k \\
&= \sum_k z^k/k!\ \frac{d}{dn}[(n+1)(n+2)\cdots(n+k)] \\
&= \sum_k z^k/k!\ \cdot \frac{(n+k)!}{n!} \cdot \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+k}\right) \\
&= \sum_k z^k \binom{n+k}{k} \cdot \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+k}\right)
\end{aligned}$$

- Differentiating again, $\frac{d^2}{dn^2}P(n)$

$$\begin{aligned}
&\frac{d}{dn}\sum_k z^k \binom{n+k}{k} \cdot \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+k}\right) \\
&= \sum_k z^k \left[\left(\frac{d}{dn}\binom{n+k}{k}\right) \cdot \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+k}\right) + \binom{n+k}{k} \cdot \left(\frac{d}{dn}\left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+k}\right)\right)\right] \\
&= \sum_k z^k \left[\binom{n+k}{k} \cdot \left(\frac{1}{n+1} + \frac{1}{n+2} + \cdots + \frac{1}{n+k}\right)^2 - \binom{n+k}{k} \cdot \left(\frac{1}{(n+1)^2} + \frac{1}{(n+2)^2} + \cdots + \frac{1}{(n+k)^2}\right)\right] \\
&= \sum_k z^k \binom{n+k}{k} [(H_{x+k} - H_k)^2 - (H^{(2)}_{x+k} - H^{(2)}_k)]\ \textbf{\textit{(Ans)}}
\end{aligned}$$

P21: A robber holds up a bank and demands $500 in tens and twenties. He also demands to know the number of ways in which the cashier can give him the money. Find a generating function G(z) for which this number is $[z^{500}]G(z)$, and a more compact generating function G'(z) for which this number is $[z^{50}]G'(z)$.

Ans:

- The thief demands 10 and 20 denominations. From the concept of coin change, we can express the generating function as $G(z) = \frac{1}{(1-z^{10})(1-z^{20})}$

- This can also be expressed as $G(z^{10})$ where, $G(z) = \frac{1}{(1-z)(1-z^2)}$
- (a) using partial fractions
  - now $G'(z) = \frac{1}{(1-z)(1-z^2)} = \frac{1}{2}\frac{1}{(1-z)^2} + \frac{1}{4}\frac{1}{1+z} + \frac{1}{4}\frac{1}{1+z}$
  - expanding we get, $\frac{1}{2}(1 + 2z + 3z^2 + \cdots) + \frac{1}{4}(1 - z + z^2 \cdots) + \frac{1}{4}(1 + z + z^2 \cdots)$
  - thus, $[z^n]G'(n) = \frac{1}{2}(n+1) + \frac{1}{4}(1 + (-1)^n)$
  - $[z^{500}]G(z) = [z^{50}]G'(z) = \frac{50+1}{2} + \frac{1+1}{4} = 26$
- (b) using a different method:
  - $G'(z) = \frac{1}{(1-z)(1-z^2)} = \frac{1+z}{(1-z^2)^2} = (1+z)(1 + 2z^2 + 3z^4 + 4z^6 \cdots)$
  - $(2n)^{th}$ and $(2n+1)^{th}$ power will have a coefficient of (n+1)
  - As per question 2n=50, so ways = (25+1) = 26 ***(Ans)***

P35: Evaluate the sum $\sum_{0<k<n} 1/k(n-k)$ in two ways:

a Expand the summand in partial fraction

b Treat the sum as a convolution and use generating functions

Ans:

a. Using partial fractions:

$$\sum_{0<k<n} 1/k(n-k)$$
$$= \sum_{0<k<n} \frac{1}{kn} + \sum_{0<k<n} \frac{1}{n(n-k)}$$
$$= \frac{1}{n}\left(\sum_{0<k<n} \frac{1}{k} + \sum_{0<k<n} \frac{1}{n-k}\right) \quad = \frac{1}{n}\left(\sum_{0<k<n} \frac{1}{k} + \sum_{0<n-l<n} \frac{1}{l}\right) \textbf{ [let n-k = l]}$$
$$= \frac{1}{n}\left(\sum_{0<k<n} \frac{1}{k} + \sum_{0<l<n} \frac{1}{l}\right)$$
$$= \frac{2}{n}H_{n-1}$$