Contents

Hasan Masum: 1805052@ugrad.cse.buet.ac.bd

1 Chapter-1: Recurrent Problems

1.1 Problem 1(1.5)

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?

Solution:

Let T_n be the number of subsets illustrated by n overlapping circles. Now,

$$T_1 = 2$$

$$T_2 = 4 = 2 + 1 \times 2 = T_1 + 1 \times 2$$

$$T_3 = 8 = 4 + 2 \times 2 = T_2 + 2 \times 2$$

$$\vdots$$

$$T_n = T_{n-1} + (n-1) \times 2$$

So for 4 overlapping circles,

$$T_4 = T_3 + (4-1) \times 2 = 8 + 6 = 14$$

We can see 4 overlapping circles at max can illustrate 14 possibilities (subsets). Therefore, sixteen possibilities that arise with four given sets can't be illustrated by four overlapping circles.

1.2 Problem 2(1.6)

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?

Solution:

Let, R_n be the maximum number of bounded regions by n lines.

Now,

$$R_2 = 0$$

$$R_3 = 1 = 0 + (3 - 2) = R_2 + (3 - 2)$$

$$R_4 = 3 = 1 + (4 - 2) = R_3 + (4 - 2)$$

$$R_5 = 6 = 3 + (5 - 3) = R_4 + (5 - 2)$$

$$\vdots$$

$$R_n = R_{n-1} + (n - 2)$$

So, Recurrence for the bounded region by n lines,

$$R_n = \begin{cases} 0 \text{ if } n \le 2\\ R_n + (n-2), \text{ if } n > 2 \end{cases}$$

Now,

$$R_n = R_{n-1} + (n-2)$$

$$= R_{n-2} + (n-1-2) + (n-2)$$

$$= R_2 + 1 + 2 + \dots + (n-1-2)(n-2)$$

$$= 0 + 1 + 2 + \dots + (n-1-2)(n-2)$$

$$= \frac{(n-2)(n-2+1)}{2}$$

$$= \frac{(n-2)(n-1)}{2}$$

1.3 Problem 3(1.10)

Let 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

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

You need not solve these recurrences

Solution:

Let, three disks are A, B and C. All the moves are cloclewice.

To move n disks from A to B, we need -

- R_{n-1} moves to transfer (n-1) smaller disks to C clockwise.
- \bullet 1 move to transfer the largest dish to B
- And Finally R_{n-1} moves more to transfer (n-1) smaller disks to B clocliwise.

So,
$$Q_n = R_{n-1} + 1 + R_{n-1} = 2R_{n-1} + 1$$
, if $n > 0$

Therefore,

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

Again to move n disks from B to A in clockwise direction, we need -

- R_{n-1} moves to transfer (n-1) smaller disks to A
- 1 Move to transfer the largest disk to B
- Q_{n-1} moves to transfer (n-1) smaller disks to B
- 1 move to transfer the largest disk to A
- R_{n-1} moves again to transfer (n-1) smaller disks to A

So,

$$R_n = R_{n-1} + 1 + Q_{n-1} + 1 + R_{n-1}$$
$$= (2R_{n-1} + 1) + Q_{n-1} + 1$$
$$\therefore R_n = Q_n + Q_{n-1} + 1 \text{ when } n > 0$$

Therefore,

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

1.4 Problem 4(1.11-a)

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?

Solution

Let D_n be the number of moves required for a double tower of Hanoi problem. For A Double Tower of Hanoi instead of moving the smallest n-1 disk to the intermediate peg, we need to move 2(n-1) of them

in D_{n-1} moves. Also now there are two largest disks that we have to the destination peg. Finally, we have to move 2(n-1) dist to the destination in D_{n-1} moves more.

Therefore, $D_n = 2D_{n-1} + 2$.

We know the number of moves required for an original tower of Hanoi problem with n disk is, $T_n = 2^n - 1$ Now if we consider moving two same-sized disks as a single move, we can get the number of moves required for 2n disk by multiplying T_n by 2.

That is,

$$D_n = 2T_n$$
$$= 2(2^n - 1)$$
$$= 2^{n+1} - 2$$

1.5 Problem 5(1.13)

What's the maximum number of regions definable by n zig-zag lines, each of which consists of two parallel infinite half-lines joined by a straight segment?



Solution:

After a little thought, we realize that a zig zag is like three intersecting lines. Three intersecting line creates 7 regions. But one zig zag only creates 2 regions. So we lose 5 a region per zig zag. We know number of regions generated by n lines is, $L_n = \frac{n(n+1)}{2} + 1$

So, number of regions definable by n zig-zay has is,

$$ZZ_n = L_{3n} - 5n$$

$$= \frac{3n(3n+1)}{2} + 1 - 5n$$

$$= \frac{9n^2 + 3n}{2} + 1 - 5n$$

$$= \frac{9}{2}n^2 + \frac{3}{2}n - 5n + 1$$

$$= \frac{9}{2}n^2 - \frac{7}{2}n + 1$$

2 Chapter-2: Sums

2.1 Problem 1(2.11)

Solution:

$$\begin{split} L.H.S &= \sum_{0 \leq k < n} \left(a_{k+1} - a_k \right) b_k \\ &= \sum_{0 \leq k < n} a_{k+1} b_k - \sum_{0 \leq k < n} a_k b_k \\ &= \sum_{0 \leq k < n} a_{k+1} b_k - \sum_{1 \leq k+1 \leq n} a_{k+1} b_{k+1} - a_0 b_0 + a_n b_n \\ &= \sum_{0 \leq k < n} a_{k+1} b_k - \sum_{0 \leq k \leq n-1} a_{k+1} b_{k+1} - a_0 b_0 + a_n b_n \\ &= a_n b_n - a_0 b_0 + \sum_{0 \leq k < n} a_{k+1} b_k - \sum_{0 \leq k < n} a_{k+1} b_{k+1} \\ &= a_n b_n - a_0 b_0 - \sum_{0 \leq k < n} a_{k+1} \left(b_{k+1} - b_k \right) \\ &= R \cdot H \cdot S \end{split}$$

2.2 Problem 2(2.12)

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

Solution:

Let,

Let,
$$p(k) = n \in \mathbb{N}$$

$$\Rightarrow k + (-1)^k c = n \dots(i)$$

$$\Rightarrow k + (-1)^k c + c = n + c$$

$$\Rightarrow k + \{(-1)^k + 1\} c = n + c$$

Now,

$$(-1)^{k+\{(-1)^k+1\}c} = (-1)^{n+c}$$

$$\Rightarrow (-1)^k \cdot (-1)^{\{(-1)^k+1\}c} = (-1)^{n+c}$$

$$\Rightarrow (-1)^k \cdot (-1)^{\text{even}} = (-1)^{n+c}$$

$$\Rightarrow (-1)^k = (-1)^{n+c}$$

From (i),

$$n = k + (-1)^k c$$

$$\Rightarrow n = k + (-1)^{n+c} c$$

$$\Rightarrow k = n - (-1)^{n+c} c$$

So, whenever c is an integer, the value of k above will give $p(k) = n \in \mathbb{N}$. Therefore, the function $p(k) = k + (-1)^k c$ is a permutation of the set of all integers; whenever c is an integer.

2.3 Problem 3(2.14)

Solution:

$$\sum_{k=1}^{n} k 2^{k} = \sum_{k=1}^{n} \left(\sum_{j=1}^{k} 1\right)^{k}$$

$$= \sum_{k=1}^{n} \sum_{j=1}^{k} 2^{k}$$

$$= \sum_{1 \le j \le k \le n} 2^{k}$$

$$= \sum_{1 \le j \le n} \sum_{j \le k \le n} 2^{k}$$

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

$$= \sum_{1 \le j \le n} \left(2^{n+1} - 1 - 2^{j} + 1\right)$$

$$= \sum_{1 \le j \le n} 2^{n+1} - \sum_{1 \le j \le n} 2^{j}$$

$$= 2^{n+1} \sum_{1 \le j \le n} 1 - \left(\sum_{0 \le j \le n} 2^{j} - 1\right)$$

$$= n2^{n+1} - \left(2^{n+1} - 1 - 1\right)$$

$$= n2^{n+1} - \left(2^{n+1} - 2\right)$$

2.4 Problem 4(2.19)

Use a summation factor to solve the recurrence

$$T_0 = 5$$
 $2T_n = nT_{n-1} + 3 \cdot n!, \quad \text{for } n > 0.$

Solution:

Given recurrence,

$$T_0 = 5$$
$$2T_n = nT_{n-1} + 3 \cdot n!$$

Comparing with $a_n T_n = b_n T_{n-1} + c_n$, we get

$$a_n = 2, b_n = n \text{ and } c_n = 3 \cdot n!$$

So, the summation factor,

$$s_n = \frac{a_{n-1}a_{n-2}\cdots a_1}{b_nb_{n-1}\cdots b_2}$$
$$= \frac{2\cdot 2\cdots 2}{n(n-1)\cdots 2}$$
$$= \frac{2^{n-1}}{n!}$$

Therefore,

$$T_n = \frac{1}{s_n a_n} \left(s_1 b_1 T_0 + \sum_{k=1}^n s_k c_k \right)$$

$$= \frac{1}{s_n a_n} \left(\frac{2^{1-1}}{1!} \cdot 1 \cdot 5 + \sum_{k=1}^n \frac{2^{k-1}}{k!} \cdot 3 \cdot k! \right)$$

$$= \frac{1}{\frac{2^{n-1}}{n!}} \cdot 2 \left(\frac{n!}{2^n} \left(5 + 3 \sum_{k=1}^n 2^{k-1} \right) \right)$$

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

$$= \frac{n!}{2^n} (2 + 3 \cdot 2^n)$$

$$= n! (2^{1-n} + 3)$$

2.5 Problem 5(2.20)

Solution:

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

Now,

$$S_{n+1} = \sum_{k=0}^{n+1} kH_k$$

$$\Rightarrow S_{n+1} = 0 \cdot H_0 + \sum_{k=1}^{n+1} kH_k$$

$$\Rightarrow S_{n+1} = \sum_{1 \le k+1 \le n+1} (k+1)H_{k+1}$$

$$\Rightarrow S_{n+1} = \sum_{0 \le k \le n} (k+1)(H_k + \frac{1}{k+1})$$

$$\Rightarrow S_{n+1} = \sum_{0 \le k \le n} (1 + kH_k + H_k)$$

$$\Rightarrow S_{n+1} = \sum_{0 \le k \le n} 1 + \sum_{0 \le k \le n} kH_k + \sum_{0 \le k \le n} H_k$$

$$\Rightarrow S_n + (n+1)H_{n+1} = (n+1) + S_n + \sum_{0 \le k \le n} H_k$$

$$\Rightarrow \sum_{0 \le k \le n} H_k = (n+1) - (n+1)H_{n+1}$$

$$= (n+1)(1 - H_{n+1})$$

2.6 Problem 6(2.21)

Solution: Let $S_n = \sum_{k=0}^{n} (-1)^{n-k}$

Now,

$$S_{n+1} = \sum_{k=0}^{n+1} (-1)^{n+1-k}$$

$$\Rightarrow \sum_{k=0}^{n} (-1)^{n+1-k} + (-1)^{n+1-(n+1)} = (-1)^{n+1-0} + \sum_{k=1}^{n+1} (-1)^{n+1-k}$$

$$\Rightarrow \sum_{k=0}^{n} (-1)^{n-k} \cdot (-1)^{1} + (-1)^{0} = (-1)^{n+1} + \sum_{1 \le k+1 \le n+1} (-1)^{n+1-(k+1)}$$

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

$$\Rightarrow -S_n + 1 = (-1)^{n+1} + S_n$$

$$\Rightarrow 2S_n = 1 + (-1)^{n+1}$$

$$\Rightarrow S_n = \frac{1 + (-1)^{n+1}}{2}$$

Again let, $T_n = \sum_{k=0}^n (-1)^k k$

Now,

$$T_{n+1} = \sum_{k=0}^{n+1} (-1)^k k$$

$$\Rightarrow T_{n+1} = (-1)^{n+1-0} \cdot 0 + \sum_{k=1}^{n+1} (-1)^{n+1-k} k$$

$$\Rightarrow \sum_{k=0}^{n} (-1)^{n+1-k} k + (-1)^{n+1-(n+1)} \cdot (n+1) = \sum_{1 \le k+1 \le n+1} (-1)^{n+1-(k+1)} (k+1)$$

$$\Rightarrow \sum_{k=0}^{n} (-1)^{n-k} \cdot k \cdot (-1)^1 + (n+1) = \sum_{0 \le k \le n} (-1)^{n-k} (k+1)$$

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

$$\Rightarrow -T_n + (n+1) = T_n + S_n$$

$$\Rightarrow 2T_n = (n+1) - S_n$$

$$\Rightarrow 2T_n = (n+1) - S_n$$

$$\Rightarrow T_n = \frac{(n+1) - S_n}{2}$$

$$= \frac{(n+1) - \frac{1+(-1)^{n+1}}{2}}{2}$$

$$= \frac{2(n+1) - (1+(-1)^{n+1})}{4}$$

$$= \frac{2n+2-1-(-1)^{n+1}}{4}$$

$$= \frac{2n+1+(-1)^{n+1}}{4}$$

2.7 Problem 7(2.23)

Evaluate the sum $\sum_{k=1}^{n} (2k+1)/k(k+1)$ using partial fraction.

Solution:

Here,

$$\frac{2k+1}{k(k+1)} = \frac{2 \cdot 0 + 1}{k(0+1)} + \frac{2 \cdot (-1) + 1}{(-1)(k+1)}$$
$$= \frac{1}{k} + \frac{1}{k+1}$$

Now,

$$\sum_{k=1}^{n} \frac{2k+1}{k(k+1)} = \sum_{k=1}^{n} \left(\frac{1}{k} + \frac{1}{k+1}\right)$$

$$= \sum_{k=1}^{n} \frac{1}{k} + \sum_{k=1}^{n} \frac{1}{k+1}$$

$$= H_n + \sum_{1 \le k \le n} \frac{1}{k+1}$$

$$= H_n + \sum_{1 \le k \le n+1} \frac{1}{k}$$

$$= H_n + \sum_{1 \le k \le n+1} \frac{1}{k}$$

$$= H_n + \sum_{1 \le k \le n} \frac{1}{k} + \frac{1}{n+1} - \frac{1}{1}$$

$$= H_n + H_n + \frac{1}{n+1} - 1$$

$$= 2H_n - \frac{n}{n+1}$$

2.8 Problem 8(2.29)

Evaluate the sum $\sum_{k=1}^{n} (-1)^k/(4k^2-1)$ using partial fraction.

Solution:

Here,

$$\begin{split} \frac{k}{4k^2 - 1} &= \frac{k}{(2k - 1)(2k + 1)} \\ &= \frac{1/2}{(2k - 1)(2 \cdot \frac{1}{2} + 1)} + \frac{-1/2}{(2 \cdot \frac{-1}{2} - 1)(2k + 1)} \\ &= \frac{1}{4} \left(\frac{1}{2k - 1} + \frac{1}{2k + 1} \right) \end{split}$$

$$\begin{split} \sum_{k=1}^{n} \frac{(-1)^k}{4k^2 - 1} &= \sum_{k=1}^{n} \frac{(-1)^k}{4} \left(\frac{1}{2k - 1} + \frac{1}{2k + 1} \right) \\ &= \frac{1}{4} \left(\sum_{k=1}^{n} \frac{(-1)^k}{2k - 1} + \sum_{k=1}^{n} \frac{(-1)^k}{2k + 1} \right) \\ &= \frac{1}{4} \left(\frac{(-1)^1}{2 \cdot 1 - 1} + \sum_{k=2}^{n} \frac{(-1)^k}{2k - 1} + \frac{(-1)^n}{2n + 1} + \sum_{k=1}^{n-1} \frac{(-1)^k}{2k + 1} \right) \\ &= \frac{1}{4} \left(\frac{(-1)^n}{2n + 1} - 1 + \sum_{k=1+2}^{n} \frac{(-1)^{k+1}}{2k + 2 - 1} + \sum_{k=1}^{n-1} \frac{(-1)^k}{2k + 1} \right) \\ &= \frac{1}{4} \left(\frac{(-1)^n}{2n + 1} - 1 + \sum_{k=1-2-1}^{n-1} \frac{(-1)^k \cdot (-1)^1}{2k + 1} + \sum_{k=1}^{n-1} \frac{(-1)^k}{2k + 1} \right) \\ &= \frac{1}{4} \left(\frac{(-1)^n}{2n + 1} - 1 - \sum_{k=1}^{n-1} \frac{(-1)^k}{2k + 1} + \sum_{k=1}^{n-1} \frac{(-1)^k}{2k + 1} \right) \\ &= \frac{1}{4} \left(\frac{(-1)^n}{2n + 1} - 1 \right) \end{split}$$

3 Chapter-4: Number theory

3.1 Problem 1

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

Solution:

$$n^{3} + 100 = n^{3} + 10^{3} - 900$$
$$= (n+10)(n^{2} - 10 \cdot n + 10^{2}) - 900$$
$$= (n+10)(n^{2} - 10n + 100) - 900$$

Here n + 10 is a factor of $n^3 + 100$ if and only if n + 10 is a factor of 900. That is $(n + 1) \cdot k = 900$ for some integer k. If we take k = 1, then n + 10 = 900 and n = 890. So, the largest positive integer n for which $n^3 + 100$ is divisible by n + 10 is 890.

3.2 Problem 2

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

Here

Solution:

$$\begin{split} \gcd(12n+1,30n+2) &= \gcd(12n+1,(30n+2) mod(12n+1)) \\ &= \gcd(12n+1,(30n+2)-2(12n+1)) \\ &= \gcd(12n+1,6n) \\ &= \gcd(6n,(12n+1) mod 6n) \\ &= \gcd(6n,(12n+1)-2(6n)) \\ &= \gcd(6n,1) \\ \Rightarrow \gcd(12n+1,30n+2) &= 1 \end{split}$$

So 12n+1 and 30n+2 are co-prime. Therefore the fraction $\frac{12n+1}{30n+2}$ is irreducible for all positive integers n.

3.3 Problem 3

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?

Solution:

Let A, B, C be the number of numbers less than 1000 that are divisible by 2, 3, 5 respectively. Then, by inclusion-exclusion principle, the number of numbers that are divisible by at least one of 2, 3, 5 is,

$$\begin{split} n(A \cup B \cup C) &= n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C) \\ &= \left\lfloor \frac{1000}{2} \right\rfloor + \left\lfloor \frac{1000}{3} \right\rfloor + \left\lfloor \frac{1000}{5} \right\rfloor - \left\lfloor \frac{1000}{2 \times 3} \right\rfloor - \left\lfloor \frac{1000}{3 \times 5} \right\rfloor - \left\lfloor \frac{1000}{5 \times 2} \right\rfloor + \left\lfloor \frac{1000}{2 \times 3 \times 5} \right\rfloor \\ &= 500 + 333 + 200 - 166 - 100 - 66 + 33 \\ &= 734 \end{split}$$

Therefore the number of numbers that are not divisible by 2, 3, 5 is,

$$n(A^c \cap B^c \cap C^c) = n(U) - n(A \cup B \cup C)$$
$$= 1000 - 734$$
$$= 266$$

Given that there are 168 prime numbers less than 1000. So, the number of prime-looking numbers less than 1000 is,

$$n(A^c \cap B^c \cap C^c) - n$$
(prime numbers less than 1000) = 266 - 168
= 98

3.4 Problem 4

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.

Solution:

Let gcd of m, n be g.

We know that, $gcd(m, n) \cdot lcm(m, n) = mn$

Now,

$$lcm(m,n) + gcd(m,n) = m + n$$

$$\Rightarrow \frac{mn}{g} + g = m + n$$

$$\Rightarrow mn + g^2 = gm + gn$$

$$\Rightarrow g^2 - gn = gm - mn$$

$$\Rightarrow g(g - n) = m(g - n)$$

$$\Rightarrow g(g - n) - m(g - n) = 0$$

$$\Rightarrow (g - m)(g - n) = 0$$

$$\Rightarrow g = m \text{ or } g = n$$

So if g = m, then m divides n. If g = n, then n divides m. Therefore, one of the two numbers is divisible by the other.

3.5 Problem 5

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

Solution:

We will prove it by contradiction.

Let, $(36a + b) = 2^m$...(i)

and $(a + 36b) = 2^n$...(ii)

Subtracting (ii) from (i), we get,

$$35a - 35b = 2^{m} - 2^{n}$$

$$\Rightarrow 35(a - b) = 2^{n}(2^{m-n} - 1)$$

Here 2^n is even and $2^{m-n} - 1$ is odd. So, $2^n(2^{m-n} - 1)$ is odd. 35 is odd. So (a - b) must be even. Therefore,

$$35 = 2^{m-n} - 1$$
$$\Rightarrow 36 = 2^{m-n}$$

But 36 is not a power of 2. So, our assumption is wrong.

Therefore, for any positive integers a and b, the number (36a + b)(a + 36b) cannot be a power of 2.

3.6 Problem 6

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

Solution:

Let, $n! + 5 = k^3$

For $n \ge 10$, 100\n!. So, $n! + 5 \equiv 5 \pmod{100}$

Therefore, $k^3 \equiv 5 \pmod{100}$, which is not possible since k^3 will have only one factor of 5.

Therefore n is less than 10.

For n = 1, n! + 5 = 6 which is not a perfect cube.

For n = 2, n! + 5 = 7 which is not a perfect cube.

For n = 3, n! + 5 = 11 which is not a perfect cube.

For n = 4, n! + 5 = 29 which is not a perfect cube.

For n = 5, $n! + 5 = 125 = 5^3$ which is a perfect cube.

For n = 6, n! + 5 = 725 which is not a perfect cube.

For n = 7, n! + 5 = 5045 which is not a perfect cube.

For n = 8, n! + 5 = 40325 which is not a perfect cube.

For n = 9, n! + 5 = 362885 which is not a perfect cube.

Therefore, the only positive integer n for which n! + 5 is a perfect cube is 5.

3.7 Problem 7

Prove that $a^p \equiv a \pmod{p}$, where p is any prime

Solution:

Base case: For a = 1, $a^p = 1^p = 1 \equiv 1 \pmod{p}$

Inductive step: Assume $a^p \equiv a \pmod{p}$ is true. We have to prove that $(a+1)^p \equiv a+1 \pmod{p}$.

$$(a+1)^{p} = \binom{p}{0}a^{p} + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \dots + \binom{p}{p-1}a^{1} + \binom{p}{p}a^{0}$$

$$= a^{p} + pa^{p-1} + \dots + 1$$

$$= (a^{p} + 1) + p \cdot (a^{p-1} + \dots)$$

$$= (a^{p} + 1) + pK$$

where $K = (a^{p-1} + ...)$

Now,

$$(a+1)^p \pmod{p} = [(a^p+1) + pK] \pmod{p}$$

= $[(a^p+1) \pmod{p} + (pK) \pmod{p}] \pmod{p}$
= $[a^p \pmod{p} + 1 \pmod{p} + 0] \pmod{p}$
= $(a+1) \pmod{p}$

Therefore, $(a+1)^p \equiv a+1 \pmod{p}$ is true.

Therefore, by principle of mathematical induction, $a^p \equiv a \pmod{p}$ is true for all positive integers a and prime p.

3.8 Problem 8

Evaluate gcd(n! + 1, (n + 1)! + 1)

Solution:

$$\gcd(n!+1,(n+1)!+1) = \gcd((n+1)!+1,n!+1)$$

$$= \gcd(n!+1,((n+1)!+1) \mod (n!+1))$$

$$= \gcd(n!+1,(n+1)!+1-n\cdot (n!+1))$$

$$= \gcd(n!+1,n!+1-n)$$

$$= \gcd(n!+1-n,(n!+1) \mod (n!+1-n))$$

$$= \gcd(n!+1-n,n!+1-1\cdot (n!+1-n))$$

$$= \gcd(n!+1-n,n)$$

$$= \gcd(n!+1-n,n)$$

$$= \gcd(n,(n!+1-n) \mod n)$$

$$= \gcd(n,(n!+1-n) - (n-1)!\cdot n)$$

$$= \gcd(n,1-n)$$

$$= \gcd(n,1-n)$$

$$= \gcd(n,1-n-(-1)\cdot n)$$

$$= \gcd(n,1)$$

$$= 1$$