CS21201 DISCRETE STRUCTURES
Tutorial 3 : Induction and Proof Techniques

August 2025

1. Consider the permutations of 1,2,3,4. For example, 1432 has one *ascent* 14 (as $1 < 4$) and two *descents* 43 and 32. 1423, similarly, has two ascents (14 and 23) and one descent (42). Let $\pi_{m,k}$ denote the number of permutations of 1,2,3...,m with k ascents. Prove that :

$$\pi_{m,k} = (k+1)\pi_{m-1,k} + (m-k)\pi_{m-1,k-1}$$

2. (a) Suppose $a, b, k \in \mathbb{Z}^+$ and k is not a power of 2. Then prove that if $a^k + b^k \neq 2$ then $a^k + b^k$ is composite.

3. Let $A = \{a1, a2, a3, a4, a5\} \subseteq \mathbb{Z}^+$. Prove that A contains a non-empty subset S such that the sum of the elements in S is a multiple of 5. Here it is possible to have a sum with only one summand.

4. For $n \in \mathbb{Z}^+$, let H_n denote the nth Harmonic number.
   That is $H_n = \sum_{i=1}^{n} \frac{1}{i}$.
   (a) Prove that for all $n \in \mathbb{Z}^+$, $1 + (\frac{n}{2}) \leq H_{2^n}$
   (b) Prove that for all $n \in \mathbb{Z}^+$,

$$\sum_{j=1}^{n} j.H_j = \frac{n(n+1)}{2} H_{n+1} - \frac{n(n+1)}{4}$$

5. For any $n \in \mathbb{Z}^+$, we say that n is a perfect integer if 2n = sum of all positive divisors of n. For example, 2.6 = 1+2+3+6 so 6 is a perfect number.
   If $2^m - 1$ is prime for a positive integer m, prove that $2^{m-1}(2^m - 1)$ is a perfect integer.

6. For all positive integers n, show that there exists a prime greater than n.

7. Using the Principle of Mathematical Induction, prove the following :
   (a) $\forall n \geq 4$ the nth Catalan Number satisfies $C_n \leq 2^{2n-4}$
   (b) If H_n is the nth Harmonic number (see Q4) then prove that $\forall n \geq 1$

$$ln(n+1) \leq H_n \leq ln(n) + 1$$

8. Prove the following using the principle of mathematical induction or other techniques you know :
(a) $\forall n \in \mathbb{Z}^+, 3 \mid 7^n - 4^n$
(b) $\forall n \in \mathbb{Z}^+$, n is a perfect square if and only if n has odd number of positive divisors.

9. Let F_n be the nth Fibonacci Number.
(a) Prove that for all integers m,n with $m \geq 1$ and $n \geq 0$ we have

$$F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$$

(b) For $m, n \in \mathbb{Z}^+$, prove that if $m \mid n$ then $F_m \mid F_n$
(c) Prove or disprove with a counterexample, the converse of (b)
(d) Prove that $gcd(F_m, F_n) = F_{gcd(m,n)}, \forall m, n \geq 1$

10. Let $n \in \mathbb{Z}^+$. Consider all non-empty subsets of $\{1, 2, 3, ...n\}$ that *do not contain consecutive integers*. Let S_n denote the sum of squares of the products of the elements in these subsets.
Prove that $S_n = (n+1)! - 1, \forall n \geq 1$.

For example, for n = 5, all the valid subsets are :
$\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{3, 5\}, \{1, 3, 5\}$.
The sum of squares of products
$= 1^2 + 2^2 + ... + 5^2 + (1.3)^2 + (1.4)^2 + ... + (1.3.5)^2 = 719 = 5! - 1$.

1 Solutions

1. Let $x = (x_1, x_2, x_3, ...x_m)$ be a permutation of 1,2,...m with k ascents (and thus m-k-1) descents. There are two cases :

   (a) If $m = x_m$ or if m occurs in $x_i m x_{i+2}$ for $1 \leq i \leq m-2$ with $x_i > x_{i+2}$, then the removal of m results in a permutation of 1,2,3,...m-1 with k-1 ascents, for a total of $(1+(m-k-1))\pi_{m-1,k-1} = (m-k)\pi_{m-1,k-1}$ permutations.

   (b) If $m = x_1$ or if m occurs in $x_i m x_{i+2}$ for $1 \leq i \leq m-2$ with $x_i < x_{i+2}$, then the removal of m results in a permutation of 1,2,3,...m-1 with k ascents, for a total of $(k+1)\pi_{m-1,k}$ permutations.

   Since cases (a) and (b) are disjoint and account for all possibilities, we have $\pi_{m,k} = (m-k)\pi_{m-1,k-1} + (k+1)\pi_{m-1,k}$

2. (a) Recall that

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2$$

$$a^5 + b^5 = (a+b)(a^4 - a^3 b + a^2 b^2 - ab^3 + b^4)$$

$$a^p + b^p = (a+b)\sum_{i=1}^{p} a^{p-i}(-b)^{i-1}$$

with p being an odd prime.

Since k is not a power of 2, we can write it as $k = r.p$ where p is an odd prime and $r \geq 1$. Thus

$$a^k + b^k = (a^r)^p + (b^r)^p = (a^r + b^r)\sum_{i=1}^{p} a^{r(p-i)}(-b)^{r(i-1)}$$

Thus $a^r + b^r \mid a^k + b^k$ with $a^r + b^r \geq 2$ and with the assignment $a = 1, b = 1$ forbidden (so that $a^r + b^r \neq a^k + b^k$), thus it is clear that $a^k + b^k$ will be composite.

3. For $1 \leq i \leq 5$, it follows from the division algorithm that

$$a_i = 5q_i + r_i, \quad 0 \leq r_i \leq 4.$$

So now we shall consider the remainders: r_1, r_2, r_3, r_4, r_5. It is obvious that if a selection of the remainders adds to a multiple of 5, then the sum of the corresponding elements of A will also sum to a multiple of 5. (Note that for the remainders we need not have five distinct integers.)

(a) If $r_i = 0$ for some $1 \leq i \leq 5$, then $5 \mid a_i$ and we are finished. Therefore we shall assume from this point on that $r_i \neq 0$ for all $1 \leq i \leq 5$.

(b) If $1 \leq r_1 = r_2 = r_3 = r_4 = r_5 \leq 4$, then

$$a_1 + a_2 + \cdots + a_5 = 5(q_1 + q_2 + \cdots + q_5) + 5r_1,$$

and the result follows. Consequently we now narrow our attention to the cases where at least two different nonzero remainders occur.

Case 1: (There are at least three 4's). Here the possibilities to consider are (i) $4+1$; (ii) $4+4+2$; and (iii) $4+4+4+3$ — these all lead to the result we are seeking.

Case 2: (We have one or two 4's). If there is at least one 1, or at least one 2 and one 3, then we are done. Otherwise we get one of the following possibilities: (i) $4+2+2+2$; or (ii) $4+3+3$.

Case 3: (Now there are no 4's and at least one 3). Then we either have (i) $3+2$; (ii) $3+1+1$; or (iii) $3+3+3+1$.

Case 4: (Now we have only 1's and 2's as summands). The final possibilities are (i) $2+1+1+1$ and (ii) $2+2+1$

Thus, in every possible scenario it is possible to get a subset to remainders whose sum is divisible by 5.

4. (a) Once again we start at $n = 0$. Here we find that

$$1 = 1 + (0/2) \leq H_1 = H_{2^0},$$

so this first case is true. Assuming the truth for $n = k \in \mathbb{N}$ we obtain the induction hypothesis

$$1 + \frac{k}{2} \leq H_{2^k}.$$

Turning now to the case where $n = k + 1$ we find

$$H_{2^{k+1}} = H_{2^k} + \frac{1}{2^k + 1} + \frac{1}{2^k + 2} + \cdots + \frac{1}{2^k + 2^k},$$

$$= H_{2^k} + \frac{1}{2^k + 1} + \frac{1}{2^k + 2} + \cdots + \frac{1}{2^k + 2^k},$$

$$= H_{2^k} + 2^k \cdot \frac{1}{2^k + 2^k} = H_{2^k} + \frac{1}{2} \geq 1 + \frac{k}{2} + \frac{1}{2} = 1 + \frac{k+1}{2}.$$

The result now follows for all $n \geq 0$ by the Principle of Mathematical Induction.

(b) Starting with $n = 1$ we find that

$$\sum_{j=1}^{1} jH_j = H_1 = 1 = \frac{(2)(1)}{2} \cdot \frac{3}{2} - \frac{(2)(1)}{4} = \frac{(2)(1)}{2} H_2 - \frac{(2)(1)}{4}.$$

Assuming the truth of the given statement for $n = k$, we have

$$\sum_{j=1}^{k} jH_j = \left[\frac{(k+1)k}{2}\right] H_{k+1} - \frac{(k+1)k}{4}$$

For $n = k + 1$ we now find that

$$\sum_{j=1}^{k+1} jH_j = \sum_{j=1}^{k} jH_j + (k+1)H_{k+1}$$

$$= \left[\frac{(k+1)k}{2}\right] H_{k+1} - \frac{(k+1)k}{4} + (k+1)H_{k+1}$$

$$= (k+1)\left(1 + \frac{k}{2}\right) H_{k+1} - \frac{(k+1)k}{4}$$

$$= (k+1)\left(1 + \frac{k}{2}\right)\left(H_{k+2} - \frac{1}{k+2}\right) - \frac{(k+1)k}{4}$$

$$= \left[\frac{(k+2)(k+1)}{2}\right] H_{k+2} - \frac{(k+1)(k+2)}{2(k+2)} - \frac{(k+1)k}{4}$$

$$= \left[\frac{(k+2)(k+1)}{2}\right] H_{k+2} - \frac{1}{4}\left[2(k+1) + k(k+1)\right]$$

$$= \left[\frac{(k+2)(k+1)}{2}\right] H_{k+2} - \frac{(k+2)(k+1)}{4}$$

Consequently, by the Principle of Mathematical Induction, it follows that the given statement is true for all $n \in \mathbb{Z}^+$.

5. The divisors of $2^{m-1}(2^m-1)$, where 2^m-1 is a prime, are $1, 2, 2^2, 2^3, ..., 2^{m-1}$ and $(2^m-1), 2(2^m-1), 2^2(2^m-1), ..., 2^{m-1}(2^m-1)$. Thus, the sum of divisors $= 2^m - 1 + (2^m-1)(2^m-1) = 2.2^{m-1}(2^m-1)$, thus the given integer is a perfect number.

6. Assume that there is no prime $> n$. Then we have a finite set of primes, called $P = \{p_1, p_2, p_3, ...p_k\}$ for some $k \in \mathbb{Z}^+$. Consider a number $c = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k} + 1$ where $\alpha_i \in \mathbb{Z}^+$ and $c > n$ by taking arbitrarily large α_i.

   Now, $c \notin P \implies c$ is composite. But $c = 1 \mod p_i$ for all $i \in \{1, 2, ...k\}$. Thus no prime number divides c $\implies$ c is not composite. This is a contradiction, it means that there must be primes greater than n, as we have constructed one such prime number ourselves.

7. (a) **Solution:**

   [**Basis**] For $n = 4$,
   $$C_4 = 14 \leq 2^{8-4} = 16.$$

   [**Induction**] Assume that
   $$C_n \leq 2^{2n-4}.$$

   Then
   $$C_{n+1} = \frac{1}{n+2}\binom{2n+2}{n+1} = \frac{1}{n+2} \cdot \frac{(2n+2)(2n+1)}{(n+1)^2}\binom{2n}{n} = \frac{2(2n+1)}{n+2} C_n.$$

   Now,
   $$(2n+1) \leq 2(n+2).$$

   Therefore,
   $$C_{n+1} = \frac{2(2n+1)}{n+2} C_n \leq 4C_n \leq 2^{2(n+1)-4}$$

   Thus the induction hypothesis holds and the given proposition is proven true.

(b) The harmonic numbers

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

satisfy

$$\ln(n+1) \leq H_n \leq \ln n + 1, \quad \forall n \geq 1.$$

Solution:
[**Basis**]

$$\ln(1+1) = \ln(2) \leq H_1 = 1 \leq \ln 1 + 1 = 1.$$

[**Induction**] Assume the condition holds for H_n.

$$H_{n+1} = H_n + \frac{1}{n+1} \leq 1 + \ln n + \frac{1}{n+1}.$$

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

$$= 1 + \ln(n+1) + \frac{1}{n+1} + \ln\left(1 - \frac{1}{n+1}\right).$$

$$= 1+\ln(n+1)+\frac{1}{n+1}-\frac{1}{n+1}-\frac{1}{2(n+1)^2}-\frac{1}{3(n+1)^3}\cdots \quad (n \geq 1).$$

$$= 1 + \ln(n+1) - \left[\frac{1}{2(n+1)^2} + \frac{1}{3(n+1)^3} + \cdots\right].$$

$$\leq 1 + \ln(n+1).$$

Similarly,

$$H_{n+1} = H_n + \frac{1}{n+1} \geq \ln(n+1) + \frac{1}{n+1}.$$

$$H_{n+1} \geq \ln(n+1) + \frac{1}{n+1} - \ln(n+2) + \ln(n+2).$$

$$H_{n+1} \geq \ln\left(\frac{n+1}{n+2}\right) + \frac{1}{n+1} + \ln(n+2).$$

$$= -\ln\left(1 + \frac{1}{n+1}\right) + \frac{1}{n+1} + \ln(n+2).$$

$$H_{n+1} \geq \frac{1}{n+1} - \left(\frac{1}{n+1} - \frac{1}{2(n+1)^2} + \frac{1}{3(n+1)^3} - \cdots\right) + \ln(n+2).$$

$$\geq \ln(n+2).$$

Thus the induction hypothesis holds and the given proposition is proven true.

8. (a) For $n = 0$ we have

$$7^n - 4^n = 7^0 - 4^0 = 1 - 1 = 0,$$

and $3 \mid 0$. So the result is true for this first case.
Assuming the truth for $n = k$ we have $3 \mid (7^k - 4^k)$. Turning to the case for $n = k+1$ we find that

$$7^{k+1} - 4^{k+1} = 7(7^k) - 4(4^k) = (3+4)(7^k) - 4(4^k) = 3(7^k) + 4(7^k - 4^k).$$

Since $3 \mid 3$ and $3 \mid (7^k - 4^k)$ (by the induction hypothesis), it is clear that

$$3 \mid \left[3(7^k) + 4(7^k - 4^k)\right],$$

that is,

$$3 \mid (7^{k+1} - 4^{k+1}).$$

It now follows by the Principle of Mathematical Induction that

$$3 \mid (7^n - 4^n) \quad \text{for all } n \in \mathbb{N}.$$

(b) If $n \in \mathbb{Z}^+$ and n is a perfect square, then

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where p_i is prime and e_i is a positive even integer for all $1 \leq i \leq k$. Hence

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

is a product of odd integers. Therefore the number of positive divisors of n is odd.
Conversely, if $n \in \mathbb{Z}^+$ and n is not a perfect square, then

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where each p_i is prime and e_i is odd for some $1 \leq i \leq k$. Therefore $(e_i + 1)$ is even for some $1 \leq i \leq k$, so

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

is even and n has an even number of positive divisors.

9. Find the solution below :

10. Find the solution below :

8a) $(F_0 = 0, F_1 = 1, F_2 = 1 \ldots)$

Using Induction on m:

For $m=1$: $F_{n+1} = F_1 F_{n+1} + F_0 F_n$

For $m=2$: $F_{n+2} = F_{n+1} + F_n$

$= F_2 F_{n+1} + F_1 F_n$.

Suppose the statement is true for some m & $m+1$ [and for all n]

Then $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$

& $F_{m+n+1} = F_{m+1} F_{n+1} + F_m F_n$ are true.

Adding these 2 eqns gives:

$$F_{m+n+2} = F_{m+n+1} + F_{m+n} = (F_{m+1} + F_m) F_{n+1} + (F_m + F_{m-1}) F_n$$

$$= F_{m+2} F_{n+1} + F_{m+1} F_n$$

$\Rightarrow$ Induction hypotheses holds true

8b) Let $n = qm$.

For $q = 1$, $n = m \Rightarrow n \mid m$ & $F_m \mid F_n$.

Suppose $F_m \mid F_{qm}$. (by induction hypothesis, on q)

Then, $F_{(q+1)m} = F(m + qm) = F_m F_{qm+1} + F_{m-1} F_{qm}$

(from (a))

Thus, $F_m \mid F_m F_{qm+1}$ and $F_m \mid F_{m-1} F_{qm}$

(as $F_m \mid F_{qm}$ by induction hypothesis)

$\Rightarrow F_m \mid F_{(q+1)m}$

$\Rightarrow$ induction hypothesis holds true.

8c) The converse can be disproved easily.

Take $m = 2$, $n = 3$

Then $m \nmid n$, but $F_2 \mid F_3$ (as $1 \mid 2$).

8d) [Basis] For $m=1, n=1$

$$\gcd(F_1, F_1) = F_1 = 1 = F_{\gcd(1,1)}$$

[Induction] (Assume $m+n > 2$)

Without loss of generality, assume that $m \geq n$.

$$F_m = F_{m-n+n} = F_{m-n+1} F_n + F_{m-n} F_{n-1}$$

(from (a)).

Claim: F_{n-1} is coprime to F_n.

Proof: $F_n = F_{n-1} + F_{n-2}$. Assume that $\exists\, d$ s.t. $d \mid F_n, F_{n-1}$

Then d must divide F_{n-2}.

Continuing recursively, $d \mid (F_1 = 1) \Rightarrow d = 1$.

$\Rightarrow F_n, F_{n-1}$ are coprime.

Since F_n, F_{n-1} are coprime & F_{m-n+1}, F_{m-n} are coprime, we can assume that

if $\exists\, d$ s.t $d \mid F_n$ and $d \mid F_{m-n}$,

then d must divide F_m.

$\therefore$ the pairs (f_m, f_n) and (f_{m-n}, f_n) have the same set of common divisors, hence they have the same gcd.

$\therefore \gcd(F_m, F_n) = \gcd(F_{m-n}, F_n)$.

Now, by induction (strong), we have $\gcd(F_{m-n}, F_n)$

$$= F_{\gcd(m-n,\, n)}$$

But, the pairs $(m-n, n)$ and (m, n) have the same common divisors and hence the same GCDs.

Thus, $\gcd(F_m, F_n) = F_{\gcd(m-n,n)} = F_{\gcd(m,n)}$

Thus Proved

3.

→ Proceed by generalized weak induction on n with $n_0 = 1$, $k = 2$.

[Basis] We need two base cases. For $n = 1$, we have $S_1 = 1^2 = 1$ and $(1+1)! - 1 = 1$. For $n = 2$, $S_2 = 1^2 + 2^2 = 5$ and $(2+1)! - 1 = 6 - 1 = 5$

[Induction] Assume that $S_{n-1} = n! - 1$ and $S_{n-2} = (n-1)! - 1$ for some $n \geq 3$. All non-empty subsets of $\{1, 2, 3, \ldots n\}$ that do not contain consecutive integers can be classified in three groups

1.) Non-empty subsets of $\{1, 2, 3, \ldots n-1\}$ that do not contain consecutive integers.

2.) A non-empty subset with the desired property that contains n and one or more elements from $\{1, 2, 3, \ldots n-1\}$. Since these subsets are not allowed to contain consecutive integers, the elements other than n must come from $\{1, 2, 3 \ldots n-2\}$

3.) The subset $\{n\}$

By induction, $S_n = S_{n-1} + n^2 S_{n-2} + n^2$:

$$= (n! - 1) + n^2((n-1)! - 1) + n^2$$
$$= n! + n^2 \times (n-1)! - 1 = (n-1)!\,(n + n^2) - 1$$
$$= (n+1)! - 1$$