CS21201 Discrete Structures
Solutions
Proof Techniques, Induction

---

1. Prove that every positive integer greater than one can be factored as a product of primes. [Hint: Prove this using well-ordering theorem]

1.

→ Let S be the set of all integers (>1) that can't be factored as product of primes.
Assume S is not empty.
If $S \neq \phi \Rightarrow \exists$ a least element $a \in S$ [well ordering]
$\Rightarrow a$ is not prime [prime is a product of itself otherwise it can't be in S]
$\Rightarrow a$ must be a product of two int x, y s.t. $1 < x, y < a$.
Since $x, y < a$ [least element in S]
$\Rightarrow x, y \notin S$
$\Rightarrow x$ can be written as a product of primes
~~of primes~~ $x = p_1 p_2 \cdots p_k$
y " " $y = q_1 q_2 \cdots q_l$
$\Rightarrow a = xy = p_1 \cdots p_k q_1 \cdots q_l$ which is a contradiction

2. Prove that every positive integer can be written as a product of prime factors, and this product is unique up to the reordering of factors (also known as the Fundamental Theorem of Arithmetic). [Hint: Prove this using Principle of Mathematical Induction]

2. Strong Induction on +ve integers

[Basis] $n = 1$: Empty product of prime factors [unique]

[Induction] : Every +ve integer $k \leq n$ case uniquely [upto reordering] written as a product of prime factors.

Consider $n+1$.

If $n+1$ is prime, it can only be written as a product of $n+1$ with nothing else $\Rightarrow$ unique.

If $n+1$ is not a prime, since $n \geq 1$, it must be composite

Let a, b be integers > 1 such that $ab = n+1$

By Strong Induction hypothesis $a = p_1 \ldots p_t$

$b = q_1 \ldots q_s$ $\quad p_i, q_j$ are primes

$\Rightarrow n+1 = p_1 \ldots p_t q_1 \ldots q_s$

Relabeling this as $n+1 = p_1 \cdot p_2 \cdots p_r$; all p_i's are primes

We need to show that this is unique

Suppose, we have a second factorization of $n+1 = q_1 \ldots q_r$

$n+1 = p_1 \cdots p_r = q_1 \cdots q_r$

C-1: $p_1 = q_1$: Let $k = \frac{n+1}{p_1} = \frac{n+1}{q_1} = p_2 \cdots p_r = q_2 \cdots q_r$

$k < n+1 \Rightarrow$ By strong induction, k has a unique factorization

$\Rightarrow p_1 \cdots p_r$ is same as $q_1 \cdots q_r$

C-2: $p_1 \neq q_1$: Without loss of generality let $p_1 > q_1$

$\Rightarrow c = p_1 - q_1 < n+1$

$\Rightarrow c = s_1 s_2 \ldots s_u$ [Strong Induction hypothesis]

$\Rightarrow q_1$ can't be a factor of c, otherwise $p_1 = c + q_1$ is divisible by q_1 but p_1 is a prime

Define $m = c\,p_2 p_3 \cdots p_r = s_1 \cdots s_u\, p_2 \cdots p_r$

$m = (p_1 - q_1)\, p_2 \cdots p_r = n+1 - q_1 p_2 \cdots p_r$

$\Rightarrow$ $m < n+1$ $\Rightarrow$ by strong ind. hyp

$m = s_1 \cdots s_u\, p_2 \cdots p_r$ is unique

On the other hand,

$m = n+1 - q\,p_2 \cdots p_r$

$= q_1 (q_2 \cdots q_r - p_2 \cdots p_r)$

$\Rightarrow$ q_1 is a prime factor of m

Since q_1 is not a factor of c, $q_1 \neq s_i$

$\Rightarrow q_1 = p_j$ for some $2 \le j \le r$

then let $k = \frac{n+1}{p_j} = \frac{n+1}{q_1}$

$\Rightarrow$ The product of remaining p_i $(i \neq j)$ is a prime factorization of $k = q_2 \cdots q_r$

$k < n+1 \Rightarrow$ this must be unique

$\Rightarrow$ Thus, in either case, the prime factorization of $n+1$ is unique. [upto reordering]

3. Prove that √n is irrational if and only if n is not a perfect square.

3.

→ [⇒] if $\sqrt{n}$ is irrational ⇒ n is not a perf. square

Contrapositive : n is a perfect sq. ⇒ $\sqrt{n}$ is rational

let $n = k^2$ for some $k \in \mathbb{Z}$

⇒ $\sqrt{n} = \sqrt{k^2} = k$

⇒ $\sqrt{n} \in \mathbb{Z}$,

⇒ $\sqrt{n}$ is rational

[⇐] if n is not a perfect sq. ⇒ $\sqrt{n}$ is irrational

Assume, n is not a perfect sq. & $\sqrt{n}$ is rational

⇒ $\sqrt{n} = \frac{p}{q}$ where p, q are coprime & $q \neq 0$
$p, q \in \mathbb{Z}$

⇒ $n = \frac{p^2}{q^2}$ ⇒ $nq^2 = p^2$

⇒ $q^2 | p^2$ ⇒ $q = 1$ (since p & q are coprime)

⇒ $n = p^2$ ⇒ n is a perfect square

This is a contradiction & ∴ $\sqrt{n}$ is irrational

4. Using mathematical induction, prove that $2^n < n! < 2^{n\log_2 n}$, $\forall\, n >= 4$.

4.

→ [Basis] $n = 4$ ⇒ $2^4 = 16 < 4! = 24 < 2^{4\log_2 4} = 256$

[Induction] Suppose, $2^n < n! < 2^{n\log_2 n}$ for some $n \geq 4$

we have, $(n+1)! = (n+1) \times n! > (n+1) \times 2^n >$
$2 \times 2^n = 2^{n+1}$

& $(n+1)! = (n+1) \times n! < (n+1) \cdot 2^{n\log_2 n}$
$= (n+1) \cdot n^n \leq (n+1)^{n+1}$
$= 2^{(n+1)\log_2 (n+1)}$

5. Let a,b be two positive integers, and d = gcd(a,b) = ua + vb with u, v ∈ $\mathbb{Z}$. Prove that u and v can be so chosen that $|u| < \frac{b}{d}$ and $|v| \le \frac{a}{d}$.

5.

→ By extended GCD, we always have a representation of the form $1 = u\left(\frac{a}{d}\right) + v\left(\frac{b}{d}\right)$ for some integers u, v.

Write $u = q\left(\frac{b}{d}\right) + r$ with $0 \le r < \frac{b}{d}$ (Euclidean Division).

We have,

$$1 = \left(q\left(\frac{b}{d}\right) + r\right)\left(\frac{a}{d}\right) + v\left(\frac{b}{d}\right)$$

$$= r\left(\frac{a}{d}\right) + s\left(\frac{b}{d}\right),$$

where $s = v + q\left(\frac{a}{d}\right)$.

If $r = 0$, $s = \frac{d}{b} \le 1 \le \frac{a}{d}$.

If $r > 0$, $|s| = \frac{d}{b}\left(r\left(\frac{a}{d}\right) - 1\right) < \left(r\left(\frac{d}{b}\right)\right)\frac{a}{d} < \frac{a}{d}$

6. You have coins of two integral denominations a,b > 1 with gcd(a,b) = 1. Prove that any integer amount n ≥ (a−1)(b−1) can be changed by coins of these two denominations. $[\exists x, y > 0,\ n = xa + yb]$

Solution:

Because a and b are relatively prime, there exist integers x_0 and y_0 (not necessarily both ≥ 0) such that $ax_0 + by_0 = 1$. Thus, (multiplying through by n), we find that there exist integers x_1, y_1 such that $ax_1 + by_1 = n$.

Infinitely many solutions of the equation $ax + by = n$ are given by $x = x_1 - tb,\ y = y_1 + ta$, where t ranges over the integers.

Let t be the smallest positive integer such that $y_1 + ta \ge 0$. We show that $x_1 - tb \ge 0$. We have

$a(x_1 - tb) + b(y_1 + ta) = n \ge (a - 1)(b - 1)$,

thus,

$a(x_1 - tb) \ge (a - 1)(b - 1) - b(y_1 + ta)$.

But $y_1 + ta \le a - 1$, else we could decrement t. Thus

$a(x_1 - tb) \ge (a - 1)(b - 1) - b(a - 1) = -(a - 1) > -a$,

and therefore $x_1 - tb > -1$, so that $x_1 - tb \ge 0$. So, we have produced the required non-negative solution.

7. Let a,b be as in the last question. Prove that the amount (a−1)(b−1)−1 cannot be changed by coins of denominations a and b.

Solution:
Let the max number which cannot be represented using a and b denominations be x.

Now, notice that we can denote the number $x + a = pa + yb$, for some p >= 0 & y >=0. Since x can't be represented as : (some positive number) * a + (some positive number)*b , p = 0, So, $x + a = yb$ and $x + b = za$, for some y and z.
This implies $a(z + 1) = b(y + 1)$.
Since a and b are coprimes, $z = nb - 1$ and $y = na - 1$, where n is an integer.
This gives $x = nab - a - b$.
If n>1, let n=j+k, where j>0 and k>0.
$x = jab + kab - a - b \Rightarrow x = a(jb - 1) + b(ka - 1)$, which cannot be true.
Therefore, n=1 and $x = ab - a - b = (a - 1)(b - 1) - 1$.

8. Let F_n denote the n-th Fibonacci number.
   a. Prove that for all integers m,n with m ≥ 1 and n ≥ 0, we have $F_{m+n} = F_m F_{n+1} + F_{m-1} F_n$.
   b. Let m,n ∈ ℕ. Prove that if m|n, then $F_m | F_n$.
   c. What about the converse of Part (b)?
   d. Prove $gcd(F_m, F_n) = F_{gcd(m,n)} \forall m, n \geq 1$.

8.
(a.)
→ 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 (& for all n) :

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

$F_{m+n+1} = F_{m+1} \cdot F_{n+1} + F_m F_n$

Adding these two equations gives

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

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

(b)

→ Write $n = qm$.

For $q = 1$; $n = m \Rightarrow n | m$ & $f_m | f_n$

Suppose $f_m | f_{qm}$

$F_{(q+1)m} = f_{m+qm} = f_m f_{qm+1} + f_{m-1} f_{qm}$ ((2.))

Since $f_m f_{qm+1}$ is a multiple of f_m

& $f_{m-1} f_{qm}$ is a multiple of f_m

$\Rightarrow f_{(q+1)m}$ is a multiple of f_m.

(c)

→ Can be disproved by taking $m=2$, $n=3$

8.

d.) [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 $m \geq n$.

$F_m = F_{m-n+1} F_n + F_{m-n} F_{n-1}$ (using (a.))

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

Proof: $F_n = F_{n-1} + F_{n-2}$

Assume $\exists d$ s.t. $d \mid F_n, F_{n-1}$,

So, d must divide F_{n-2}

Repeating this recursively,

d divides $F_1 = 1$

$\therefore d = 1$

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. $d \mid F_n$ & $d \mid F_{m-n}$ then $d \mid F_m$

$\therefore$ The pairs $(F_m, F_n), (F_{m-n}, F_n)$ have same set of common divisors & hence have the same GCD.

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

Now, by Induction (Strong), $gcd(F_{m-n}, F_n) = F_{gcd(m-n, n)}$

However the pairs $(m-n, n)$ & (m, n) have the same common divisors & hence the same gcds.

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

9. Using the principle of mathematical induction, prove the following statements.
   a. $\forall n \geq 4$, the nth-Catalan number satisfies $C_n \leq 2^{2n-4}$.

Solution: [Basis] for $n = 4$, $C_4 = 14 \leq 2^{8-4} = 16$

[Induction] Assume, $C_n \leq 2^{2n-4}$

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

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

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

b. The harmonic numbers $H_n = \frac{1}{1} + \frac{1}{2} + \ ... + \frac{1}{n}$ satisfy

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

Solution: [Basis] $ln(1 + 1) = ln(2) \leq H_1 = 1 \leq ln1 + 1 = 1$

[Induction] Assume the condition holds for H_n

$$\begin{aligned} H_{n+1} &= H_n + \frac{1}{n+1} \leq 1 + ln\, n + \frac{1}{n+1} \\ &= 1 + ln(n + 1) + \frac{1}{n+1} + (ln\, n - ln\,(n + 1)) \\ &= 1 + ln(n + 1) + \frac{1}{n+1} + ln(1 - \frac{1}{n+1}) \\ &= 1 + ln(n + 1) + \frac{1}{n+1} - \frac{1}{n+1} - \frac{1}{2(n+1)^2} - \frac{1}{3(n+1)^3} ... \quad (n \geq 1) \\ &= 1 + ln(n + 1) - [\frac{1}{2(n+1)^2} + \frac{1}{3(n+1)^3}...] \\ &\leq 1 + ln(n + 1) \end{aligned}$$

Similarly,

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

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

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

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

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

10. For all positive integers n, show that there exists a prime > n.

1.

→ Assume there exists no prime $> n$.

$\therefore$ we have a finite set of primes. Let the set be $P = \{p_1, p_2, \dots p_k\}$ for some $k \in N$.

Consider a number $c = p_1 * p_2 * p_3 \dots p_k + 1$

$\Rightarrow c \notin P \Rightarrow c$ is composite

However, we have $c = 1 \pmod{p_i}\ \forall\ i \in [1, k]$.

$\Rightarrow$ no prime numbers divide c

$\Rightarrow c$ is not composite

We arrive at a contradiction

*Correction: $c = p_1^{\alpha_1} . p_2^{\alpha_2} . p_3^{\alpha_3} .... p_k^{\alpha_k} + 1$, $\alpha_i \in N$, $c > n$ for arbitrarily large α_i

11. Let x be a non-zero real number such that $x + \frac{1}{x}$ is an integer. Prove by induction on n that $x^n + \frac{1}{x^n}$ is an integer for all n ≥ 1.

2.

→ [Basis] For $n = 1$, the statement is obvious (it is a part of the hypothesis). For $n = 2$, we use the fact that

$$\Rightarrow \left(x + \frac{1}{x}\right)^2 = x^2 + \frac{1}{x^2} + 2 \text{ is an integer}$$

$$\Rightarrow x^2 + \frac{1}{x^2} \text{ is an integer.}$$

[Induction] For $n \geq 3$, assume $x^{n-1} + \frac{1}{x^{n-1}}$, $x^{n-2} + \frac{1}{x^{n-2}}$ are integers.

We have,

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

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

Hence, $x^n + \frac{1}{x^n}$ is also an integer.

12. Let n be a positive integer. Consider all non-empty subsets of {1,2,3,...,n} that do not contain consecutive integers. Let S_n denote the sum of the squares of the products of the elements in these subsets.

For example, for n = 5, these subsets are

$$\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 4\}, \{2, 5\}, \{3, 5\}, \{1, 3, 5\}$$

Therefore S_5 is equal to:

$$1^2 + 2^2 + 3^2 + 4^2 + 5^2 + (1 * 3)^2 + (1 * 4)^2 + (1 * 5)^2 + (2 * 4)^2 + (2 * 5)^2 + \\ + (3 * 5)^2 + (1 * 3 * 5)^2 = 719$$

Prove that $S_n = (n + 1)! - 1$ for all $n \geq 1$.

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

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

13. Show by induction that $\forall n \in \mathbb{N}$,

$$f(n) = \sum_{k=0}^{n} \binom{n+k}{k} \frac{1}{2^k} = 2^n$$

4.

→ $f(n) = \sum_{k=0}^{n} \binom{n+k}{k} \frac{1}{2^k} = 2^n$

[Basis] $n = 1$:

$f(1) = \sum_{k=0}^{1} \binom{k+1}{k} \frac{1}{2^k} = {}^{1}C_{0} \cdot \frac{1}{2^0} + {}^{2}C_{1} \cdot \frac{1}{2^1}$

$= 1 + 1 = 2^1$

[Induction]

$f(n+1) = \sum_{k=0}^{n+1} \binom{n+k+1}{k} \frac{1}{2^k}$

$= \sum_{k=0}^{n+1} \left(\binom{n+k}{k} + \binom{n+k}{k-1} \right) \frac{1}{2^k}$

$f(n+1) = \left(f(n) + \binom{2n+1}{n+1} \frac{1}{2^{n+1}} \right) + \sum_{k=0}^{n} \binom{n+1+k}{k} \frac{1}{2^{k+1}}$

$f(n+1) = f(n) + \frac{f(n+1)}{2} + \frac{1}{2^{n+2}} \left(2 \binom{2n+1}{n+1} - \binom{2n+2}{n+1} \right)$

Now, $\binom{2n+2}{n+1} = \frac{2n+2}{n+1} \binom{2n+1}{n} = 2 \binom{2n+1}{n+1}$

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

$f(n+1) = 2 \cdot f(n) = 2^{n+1}$.

14. Are there three consecutive positive integers whose product is a perfect square - that is, do there exist $m, n \in \boldsymbol{Z}^{+}$ with $m * (m + 1) * (m + 2) = n^2$?

5.

→ We know that $\gcd(m, m+1) = 1 = \gcd(m+1, m+2)$

For any prime p, if $p \mid (m+1)$ then $p \nmid m$ & $p \nmid (m+2)$. Let $m * (m+1) * (m+2) = n^2$.

~~Furthermore~~, If $p \mid (m+1)$, $p \mid n^2$

$\Rightarrow p \mid n$

$\Rightarrow p^2 \mid n^2$

$\Rightarrow p^2 \mid m+1$ $\left(\because p \nmid m \text{ \& } p \nmid (m+2) \right)$

This is true for all prime divisors of $(m+1)$. So $(m+1)$ is a perfect square.

$\therefore$ $m * (m+2)$ is a perfect square.

However, $m * (m+2)$ is such that $m^2 < m^2 + 2m <$
$m^2 + 2m + 1 = (m+1)^2$.

$\Rightarrow$ $m * (m+2)$ lies b/w two consecutive perfect squares

$\Rightarrow$ $m * (m+2)$ is not a perfect square

We arrive at a contradiction. There are no three consecutive positive integers whose product is a perfect square.