

MATH 74, FALL 2004, HOMEWORK 4 SOLUTIONS

BENJAMIN JOHNSON

Due September 29

Assignment: 1.3.6(1)(3), 1.3.7, 1.4.2, 1.4.13, 1.4.19

1.3.6(1) What is $\sum_{j=1}^n j(j!)$? The easiest way to answer this question and to provide proof is to recognize the above expression as a telescoping sum, and then use the telescoping sum formula. We have

$$\begin{aligned}j(j!) &= ((j+1) - 1)(j!) \\ &= (j+1)(j!) - 1(j!) \\ &= (j+1)! - j!\end{aligned}$$

Hence

$$\begin{aligned}\sum_{j=1}^n j(j!) &= \sum_{j=1}^n [(j+1)! - j!] \text{ (by algebra, steps shown above)} \\ &= (n+1)! - 1 \text{ (by the telescoping sum formula)}\end{aligned}$$

Now that we have discovered a closed-form formula, we could do an additional proof by induction; however it is not really necessary because we have already proved the telescoping sum formula. The above suffices as a proof that $\sum_{j=1}^n j(j!) = (n+1)! - 1$.

The above is not the only way to solve this problem. One common method is to simply evaluate the expression $\sum_{j=1}^n j(j!)$ for the first several values of n , (0, 1, 5, 23, 119, 719, ...), and then guess a pattern, by recognizing that these numbers are all close to the numbers in the range of the factorial function. If you use this method to discover the correct formula, then you need to prove that your formula is valid by using induction.

1.3.6(3) No luck doing this one with telescoping sums. We just have to figure out a pattern with a few examples and then prove our result using induction. Let x and y be any fixed numbers. Then

$$\begin{aligned}x^0 - y^0 &= 0 \\ x^1 - y^1 &= x - y \\ x^2 - y^2 &= (x - y)(x + y) \\ x^3 - y^3 &= (x - y)(x^2 + xy + y^2) \\ x^4 - y^4 &= (x - y)(x^3 + x^2y + xy^2 + y^3) \\ x^5 - y^5 &= (x - y)(x^4 + x^3y + x^2y^2 + xy^3 + y^4)\end{aligned}$$

Observe that the pattern is $x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1})$. Writing this expression as a formal sum, we get $x^n - y^n = (x - y) \sum_{j=0}^{n-1} (x^{n-1-j}y^j)$. We'll prove this result holds for every $n \in \mathbb{N}$ by induction on n .

Proof. Let $P(n)$ say $x^n - y^n = (x - y) \sum_{j=0}^{n-1} (x^{n-1-j} y^j)$.

- (1) $P(n)$ is a predicate in the variable n . (Recall that we said x and y were fixed at the beginning of this discussion. Otherwise, we'd need to worry about putting quantifiers around x and y .)
- (2) $P(0)$ says $x^0 - y^0 = \sum_{j=0}^{0-1} (x^{0-1-j} y^j)$. The left side of this expression is 0 by basic algebra, and the right side is 0 by our convention involving summation. So $P(0)$ is true.
- (3) Let $n \in \mathbb{N}$, and assume $P(n)$ is true. Then $x^n - y^n = (x - y) \sum_{j=0}^{n-1} (x^{n-1-j} y^j)$. We need to show $P(n+1)$ is true. $P(n+1)$ says $x^{n+1} - y^{n+1} = (x - y) \sum_{j=0}^n (x^{n-j} y^j)$. We have

$$\begin{aligned}
 x^{n+1} - y^{n+1} &= x^{n+1} - xy^n + xy^n - y^{n+1} \text{ (add and subtract } xy^n\text{)} \\
 &= x(x^n - y^n) + y^n(x - y) \text{ (distributivity of } \cdot \text{ over } +\text{)} \\
 &= x \left[(x - y) \sum_{j=0}^{n-1} (x^{n-1-j} y^j) \right] + y^n(x - y) \text{ (by our induction hypothesis)} \\
 &= (x - y) \left[x \sum_{j=0}^{n-1} (x^{n-1-j} y^j) + y^n \right] \text{ (commutativity of } \cdot \text{, distributivity)} \\
 &= (x - y) \left[\sum_{j=0}^{n-1} (x^{n-j} y^j) + y^n \right] \text{ (multiplying } x \text{ through the sum)} \\
 &= (x - y) \left[\sum_{j=0}^n (x^{n-j} y^j) \right] \text{ (since } y^n = x^{n-n} y^n\text{)}
 \end{aligned}$$

So $P(n+1)$ is true. So $(\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1))$ is true. So by induction, $(\forall n \in \mathbb{N})(P(n))$ is true, i.e. $(\forall n \in \mathbb{N})(x^n - y^n = (x - y) \sum_{j=0}^{n-1} (x^{n-1-j} y^j))$. □

- 1.3.7(a) We need to prove that if $p(x) = \sum_{j=0}^n c_j x^j$ is a polynomial with integer coefficients (i.e. if all the c_j 's are integers), then $(\forall a \in \mathbb{N})((x-a)$ is a factor of $p(x)$ over the integers $\Leftrightarrow p(a) = 0$). We'll prove both directions of the implication directly. No need to use induction here.

Proof. Let $a \in \mathbb{N}$.

(\Rightarrow) Assume $(x - a)$ is a factor of $p(x)$ over the integers. This means we can write $p(x) = (x - a)q(x)$ for some polynomial q with integer coefficients. In this case, we have $p(a) = (a - a)(q(a)) = 0 \cdot q(a) = 0$. So $p(a) = 0$.

(\Leftarrow) Assume $p(a) = 0$. Then

$$\begin{aligned}
 p(x) &= p(x) - 0 \\
 &= p(x) - p(a) \text{ (by our assumption } p(a) = 0\text{)} \\
 &= \sum_{j=0}^n c_j x^j - \sum_{j=0}^n c_j a^j \text{ (expanding } p(x) \text{ and } p(a)\text{)} \\
 &= \sum_{j=0}^n c_j (x^j - a^j) \text{ (algebra of sums)} \\
 &= \sum_{j=0}^n c_j \left((x - a) \sum_{k=0}^{j-1} (x^{j-1-k} a^k) \right) \text{ (by problem 1.3.6(3), proven above)} \\
 &= (x - a) \sum_{j=0}^n c_j \left(\sum_{k=0}^{j-1} (x^{j-1-k} a^k) \right) \text{ (factor out the } (x - a) \text{ from each term in the sum)} \\
 &= (x - a)q(x) \text{ (for the polynomial } q(x) = \sum_{j=0}^n c_j \left(\sum_{k=0}^{j-1} (x^{j-1-k} a^k) \right)\text{)}
 \end{aligned}$$

So $x - a$ is a factor of $p(x)$ over the integers. □

1.3.7(b) Let $p(x) = \sum_{j=0}^n c_j x^j$ be a (non-zero) polynomial of degree n , and suppose p has k distinct roots, say a_1, \dots, a_k . By part (a) above, each of the linear polynomials $x - a_1, \dots, x - a_k$ must be factors of $p(x)$ over the integers. Since the a_j 's are distinct, the product of all these linear polynomials, $(x - a_1) \cdots (x - a_k) = \prod_{j=1}^k (x - a_j)$ must also be a factor of $p(x)$ over the integers, i.e. there is some (non-zero) polynomial $q(x)$ with $p(x) = \left(\prod_{j=1}^k (x - a_j) \right) \cdot q(x)$. But the product $\prod_{j=1}^k (x - a_j)$ is a polynomial of degree exactly k , (k polynomials of degree 1 multiplied together). More generally, for any polynomials f and g , multiplying the polynomials results in adding the degrees of the polynomials, i.e. $\deg(f(x) \cdot g(x)) = \deg f(x) + \deg g(x)$. We have $k \leq k + \deg q(x) = \deg(\prod_{j=1}^k a_j) + \deg q(x) = \deg \left(\left(\prod_{j=1}^k a_j \right) \cdot q(x) \right) = \deg(p(x)) = n$. So $k \leq n$. This proves a polynomial of degree n can have at most n roots that are integers.

1.4.2 The Gap Lemma says essentially $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(n \leq m \vee m + 1 \leq n)$. We'll prove this using double induction, first on m , then on n .

Proof. Let $P(m)$ say $(\forall n \in \mathbb{N})(n \leq m \vee m + 1 \leq n)$.

- (1) $P(m)$ is a predicate in the variable m .
- (2) $P(0)$ says $(\forall n \in \mathbb{N})(n \leq 0 \vee 0 + 1 \leq n)$. We'll prove this by induction on n .

Proof. Let $Q(n)$ say $n \leq 0 \vee 0 + 1 \leq n$.

- (a) $Q(n)$ is a predicate in the variable n .
- (b) $Q(0)$ says $0 \leq 0 \vee 0 + 1 \leq 0$. $Q(0)$ is true because $0 \leq 0$ is true.
- (c) Let $n \in \mathbb{N}$, and assume $Q(n)$ is true. Then $n \leq 0 \vee 0 + 1 \leq n$. We need to show $Q(n + 1)$ is true. $Q(n + 1)$ says $n + 1 \leq 0 \vee 0 + 1 \leq n + 1$. Since $0 + n = n$ for every integer n , we also have $0 \leq n$ for each integer n by the definition of \leq . Since \leq respects the successor function σ , we also have $0 + 1 \leq n + 1$ for every integer n . (Notice, surprisingly, that we didn't need to use our induction hypothesis for this

result). Thus $Q(n+1)$ is true. So $(\forall n \in \mathbb{N})(Q(n) \Rightarrow Q(n+1))$ is true. So by induction, $(\forall n \in \mathbb{N})(Q(n))$ is true, i.e. $(\forall n \in \mathbb{N})(n \leq 0 \vee 0+1 \leq n)$. \square

So $P(0)$ is true.

- (3) Let $m \in \mathbb{N}$, and assume $P(m)$ is true. Then $(\forall n \in \mathbb{N})(n \leq m \vee m+1 \leq n)$. We need to show $P(m+1)$ is true. $P(m+1)$ says $(\forall n \in \mathbb{N})(n \leq m+1 \vee m+2 \leq n)$. We'll prove this by induction on n .

Proof. Let $R(n)$ say $n \leq m+1 \vee m+2 \leq n$.

- (a) $R(n)$ is a predicate in the variable n .
 (b) $R(0)$ says $0 \leq m+1 \vee m+2 \leq 0$. $R(0)$ is true because $0 \leq m+1$ is true for every $m \in \mathbb{N}$.
 (c) Let $n \in \mathbb{N}$, and assume $R(n)$ is true. Then $n \leq m+1 \vee m+2 \leq n$. We need to show $R(n+1)$ is true. $R(n+1)$ says $n+1 \leq m+1 \vee m+2 \leq n+1$. (To show this, as it turns out, we don't actually need to use the induction hypothesis $R(n)$; but we do need to use the induction hypothesis $P(m)$, which we recall says $(\forall n \in \mathbb{N})(n \leq m \vee m+1 \leq n)$). Using $P(m)$ with $n = n$, we have $n \leq m \vee m+1 \leq n$. If $n \leq m$, then $n+1 \leq m+1$, (since \leq respects the successor function), and if $m+1 \leq n$, then $m+2 \leq n+1$, (same reason). So in either case, we have $n+1 \leq m+1 \vee m+2 \leq n+1$, and thus $R(n+1)$ is true. So $(\forall n \in \mathbb{N})(R(n) \Rightarrow R(n+1))$ is true. So by induction, $(\forall n \in \mathbb{N})(R(n))$ is true, i.e. $(\forall n \in \mathbb{N})(n \leq m+1 \vee m+2 \leq n)$. \square

So $P(m+1)$ is true. So $(\forall m \in \mathbb{N})(P(m) \Rightarrow P(m+1))$ is true. So by induction, $(\forall m \in \mathbb{N})(P(m))$ is true, i.e. $(\forall m \in \mathbb{N})(\forall n \in \mathbb{N})(n \leq m \vee m+1 \leq n)$. \square

1.4.13 If I is a fixed set, and we assume $(\forall n \in \mathbb{N}^*)(\{\{k \in \mathbb{N}^* : k < n\} \subseteq I\} \Rightarrow n \in I)$, then in particular, the predicate $(\{k \in \mathbb{N}^* : k < n\} \subseteq I) \Rightarrow n \in I$ holds for $n = 1$. Making the substitution $n = 1$, we get $(\{k \in \mathbb{N}^* : k < 1\} \subseteq I) \Rightarrow 1 \in I$. Now the set $(\{k \in \mathbb{N}^* : k < 1\})$ is empty, since there is no element of \mathbb{N}^* less than 1, and $\emptyset \subseteq I$ is true for any set I ; Hence the statement $(\{k \in \mathbb{N}^* : k < 1\} \subseteq I) \Rightarrow 1 \in I$ is logically equivalent to the simpler statement $\emptyset \subseteq I \Rightarrow 1 \in I$, and (since $\emptyset \subseteq I$ is always true) to the even simpler statement $1 \in I$. Thus including $1 \in I$ as a separate condition would be redundant.

1.4.19 Consider the following "proof" by strong induction that $(\forall n \in \mathbb{N})(2^n = 1)$.

Proof. Let $P(n)$ say $2^n = 1$.

- (1) $P(n)$ is a predicate in the variable n .
 (2) $P(0)$ says $2^0 = 1$, which is true.
 (3) Let $n \in \mathbb{N}$. Assume $(\forall k \in \mathbb{N} : k \leq n)(2^k = 1)$ We need to show $2^{n+1} = 1$. We have

$$\begin{aligned}
 (1) \quad 2^{n+1} &= \frac{2^{2n}}{2^{n-1}} \text{ (basic algebra, true for every integer } n) \\
 (2) \quad &= \frac{2^n \cdot 2^n}{2^{n-1}} \text{ (basic algebra, true for every integer } n) \\
 (3) \quad &= \frac{1 \cdot 1}{1} \text{ (supposedly by our induction hypothesis)} \\
 (4) \quad &= 1 \text{ (algebra)}
 \end{aligned}$$

□

Steps 1, 2, and 4 are perfectly correct. The problem is with step 3. Our induction hypothesis tells us that for each $k \in \mathbb{N}$ with $k \leq n$, we have $2^k = 1$. This does tell us $2^n = 1$, because we were assuming $n \in \mathbb{N}$, and we have $n \leq n$; but it only tells us $2^{n-1} = 1$ if $n - 1 \in \mathbb{N}$. For the case $n = 0$, $n - 1 \notin \mathbb{N}$. So for $n = 0$, the induction hypothesis does not apply to $n - 1$, and the proof does not go through in step 3. This example illustrates the importance of making sure the basic hypotheses of each step in a proof are satisfied. Otherwise, it is possible to prove very false statements just like the one above.