MATH 74, FALL 2004, HOMEWORK 5 SOLUTIONS

BENJAMIN JOHNSON

Due October 6

Assignment: 1.4.3(2), 1.4.7(3), 1.5.6, 1.5.8, 2.1.5(1)(3), 2.1.6

1.4.3(2) Let $A \subseteq \mathbb{N}$ and let $k \in \mathbb{N}$.

(a) If $k \in A$, then to say k is not a least element of A means $(\exists n \in A)(n < k)$.

(b) If k is not necessarily in A, then to say k is not a least element of A means $(k \notin A) \vee (\exists n \in A)(n < k)$.

1.4.7(3) We'll adapt the proof in the book to show that $\sqrt{s}$ is irrational whenever s is not a perfect square.

Proof. Let s be a positive integer that is not a perfect square. To say that $\sqrt{s}$ is irrational means $(\forall n \in \mathbb{N}^*)(\forall m \in \mathbb{Z})(\sqrt{s} \neq \frac{m}{n})$, or equivalently, $(\forall n \in \mathbb{N}^*)(n\sqrt{s} \notin \mathbb{Z})$. Let $A = \{n \in \mathbb{N}^* : n\sqrt{s} \in \mathbb{Z}\}$. We'll use well-ordering to show $A = \emptyset$.

Suppose $A \neq \emptyset$. By well-ordering, A has a least element. Let n_1 be the least element of A. Choose m to be the greatest positive integer with $m^2 < s$. (If we wanted to be more formal, we could have chosen m to be the least member of the set $\{k \in \mathbb{N}^* : (k+1)^2 > s\}$, and then shown m was also the greatest integer with $m^2 < s$). Let $k = n_1(\sqrt{s} - m)$. We will show that $\mathbf{k} \in \mathbf{A}$, and that $\mathbf{k} < \mathbf{n_1}$.

(1) First k must be positive, since $n_1 > 0$, $\sqrt{s} - m > 0$, and $k = n_1(\sqrt{s} - m)$. Second, k must be an integer, since each of $n_1\sqrt{s}$, n_1, and m are integers, and $k = n_1\sqrt{s} - n_1 \cdot m$. So $k \in \mathbb{N}^*$. Third, $k\sqrt{s}$ must be an integer since each of n_1, s, k, and m are integers, and $k\sqrt{s} = [n_1(\sqrt{s} - m)]\sqrt{s} = n_1 s - n_1\sqrt{s}m = n_1 s - km$. So $k \in \mathbb{N}^*$ and $k\sqrt{s} \in \mathbb{Z}$. So $k \in A$.

(2) Since m is the greatest integer with $m^2 < s$, we must have $(m+1)^2 > s$. (We could prove this formally using the gap lemma). Hence $\sqrt{s} - m < 1$. So $k = n_1(\sqrt{s} - m) < n_1 \cdot 1 = n_1$. So $k < n_1$.

Together, the two statements above provide a contradiction to our assumption about n_1 being the least member of A. So we conclude A must be empty, and hence $\sqrt{s}$ must be irrational. □

1.5.6 Prove: $(\forall n, j \in \mathbb{N} : 0 \leq j \leq n)\left(\binom{n+1}{j} = \binom{n}{j-1} + \binom{n}{j}\right)$.

Date: October 6, 2004.

Proof. Let $n, j \in \mathbb{N}$, with $0 \leq j \leq n$. It's easier to figure out the algebra steps if we start with the right side of the equality, so we'll just write the proof that way.

$$\begin{aligned}
\binom{n}{j-1} + \binom{n}{j} &= \frac{n!}{(j-1)!(n-(j-1))!)} + \frac{n!}{j!(n-j)!)} \text{ (def of } \binom{n}{j-1} \text{and } \binom{n}{j}) \\
&= \frac{n! \cdot j}{j!(n+1-j)!} + \frac{n! \cdot (n+1-j)}{j!(n+1-j)!} \text{ (finding common denominator)} \\
&= \frac{n! \cdot j + n! \cdot (n+1-j)}{j!(n+1-j)!} \text{ (algebra)} \\
&= \frac{n!(j+n+1-j)}{j!(n+1-j)!)} \text{ (algebra)} \\
&= \frac{(n+1)!}{j!(n+1-j)!)} \text{ (algebra)} \\
&= \binom{n+1}{j} \text{ (def of } \binom{n+1}{j})
\end{aligned}$$

□

1.5.8(a) Prove: $(\forall m, n, j \in \mathbb{N}) \left(\binom{m+n+1}{n} = \sum_{j=0}^{n} \binom{m+j}{j} \right)$.

Proof. We'll use induction on n. Let $P(n)$ say $(\forall m, j \in \mathbb{N}) \left(\binom{m+n+1}{n} = \sum_{j=0}^{n} \binom{m+j}{j} \right)$.

(1) $P(n)$ is a predicate in the variable n.

(2) $P(0)$ says $(\forall m, j \in \mathbb{N}) \left(\binom{m+1}{0} = \sum_{j=0}^{0} \binom{m+j}{j} \right)$. $P(0)$ is true because both sides of the equation evaluate to 1.

(3) Let $n \in \mathbb{N}$, and assume $P(n)$ is true. Then $(\forall m, j \in \mathbb{N}) \left(\binom{m+n+1}{n} = \sum_{j=0}^{n} \binom{m+j}{j} \right)$. We need to show $P(n+1)$ is true. $P(n+1)$ says $(\forall m, j \in \mathbb{N}) \left(\binom{m+n+2}{n+1} = \sum_{j=0}^{n+1} \binom{m+j}{j} \right)$. Again working from right to left, we have

$$\begin{aligned}
\sum_{j=0}^{n+1} \binom{m+j}{j} &= \sum_{j=0}^{n} \binom{m+j}{j} + \binom{m+n+1}{n+1} \text{ (by definition of summation)} \\
&= \binom{m+n+1}{n} + \binom{m+n+1}{n+1} \text{ (by our induction hypothesis)} \\
&= \binom{m+n+2}{n+1} \text{ (by the addition formula for binomial coefficients)}
\end{aligned}$$

So $P(n+1)$ is true. So 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. $(\forall n \in \mathbb{N})(\forall m, j \in \mathbb{N}) \left(\binom{m+n+1}{n} = \sum_{j=0}^{n} \binom{m+j}{j} \right)$, or equivalently, $(\forall m, n, j \in \mathbb{N}) \left(\binom{m+n+1}{n} = \sum_{j=0}^{n} \binom{m+j}{j} \right)$.

□

1.5.8(b) We need to use part (a) to show that $\binom{5}{2} = \binom{4}{2} + \binom{3}{1} + \binom{2}{0}$. (Of course we could just evaluate each of the 4 expressions directly and verify the equality, but that would not be the point. The point is that we can verify the equality by citing the above result and without really evaluating anything.) We have

$$\begin{aligned}
\binom{5}{2} &= \binom{2+2+1}{2} \text{ (since 5=2+2+1)} \\
&= \sum_{j=0}^{2} \binom{2+j}{j} \text{ (by part a)} \\
&= \binom{2}{0} + \binom{3}{1} + \binom{4}{2} \text{ (writing out the terms in the sum)} \\
&= \binom{4}{2} + \binom{3}{1} + \binom{2}{0}
\end{aligned}$$

2.1.5(1) Prove: If $p(x)$ is any polynomial, and if $d(x)$ is a (non-zero) polynomial with finite degree n, then there exist unique polynomials $q(x)$ and $r(x)$ with $p(x) = q(x)d(x) + r(x)$ and $\deg r(x) < n$.

Proof. First, if $p(x)$ is the zero polynomial, we choose both $q(x)$ and $r(x)$ to be the zero polynomial. This choice of $q(x)$ and $r(x)$ satisfies $p(x) = q(x)d(x) + r(x)$ (since both sides evaluate to zero) and $\deg r(x) < \deg d(x)$ (since $-\infty < n = \deg d(x)$). This choice of $q(x)$ and $r(x)$ is unique, since if $p(x) = q'(x)d(x) + r'(x)$ and $\deg r'(x) < \deg d(x)$, then $q'(x)$ must be the zero polynomial. For if $q'(x) \neq 0$, then $r'(x) = -q'(x)d(x) \Rightarrow \deg r'(x) = \deg q'(x)d(x) = \deg q'(x) + \deg d(x) \geq \deg d(x)$, which contradicts our assumption that $\deg r'(x) < \deg d(x)$. So $q'(x) = 0$, and hence $r'(x) = q'(x)d(x) = 0$. So $r'(x) = r(x)$ and $q'(x) = q(x)$.

From now on, we may assume that $p(x)$ is not the zero polynomial, so that $p(x)$ has finite degree m. Let $d(x) = \sum_{j=0}^{n} b_j x^j$ be a (non-zero) polynomial of degree n. We'll prove $(\forall m \in \mathbb{N})[\deg p(x) = m \Rightarrow (\exists!\text{polynomials } q(x), r(x))[(p(x) = q(x)d(x) + r(x) \wedge \deg r(x) < n)]]$ using strong induction on m.

Let $m \in \mathbb{N}$ and assume $(\forall k < m)[\deg p(x) = k \Rightarrow (\exists!\text{polynomials } q(x), r(x))[(p(x) = q(x)d(x) + r(x) \wedge \deg r(x) < n)]]$. There are two cases to consider. We must prove both existence and uniqueness in each case.

(1) $m < n$: For existence, choose $q(x) = 0$, and $r(x) = p(x)$. Then we have $p(x) = 0 \cdot d(x) + p(x) = q(x)d(x) + r(x)$, and $\deg r(x) = \deg p(x) = m < n$. So $p(x) = q(x)d(x) + r(x) \wedge \deg r(x) < n$.
For uniqueness, suppose $p(x) = q'(x)d(x) + r'(x)$ and $\deg r'(x) < n$. If $q'(x)$ is not the zero polynomial, and has finite degree k, then $m = \deg p(x) = \deg(q(x)d(x) + r(x)) = \max\{\deg q(x) + \deg d(x), r(x)\} = \max\{k + n, \deg r(x)\} \geq n$. This gives a contradiction to our case assumption that $m < n$. We conclude $q'(x)$ must be the zero polynomial, and hence, $r'(x) = p(x) - q'(x)d(x) = p(x) - 0 \cdot d(x) = p(x)$. So $q'(x) = q(x)$ and $r'(x) = r(x)$.

(2) $n \leq m$: In this case, the polynomial $p(x) - \frac{a_m}{b_n}x^{m-n}d(x)$ has degree less than m. (This is true because

$$\begin{aligned} p(x) - \frac{a_m}{b_n}x^{m-n}d(x) &= \sum_{j=0}^{m} a_j x^j - \frac{a_m}{b_n}x^{m-n}\sum_{j=0}^{n} b_j x^j \\ &= \sum_{j=0}^{m-1} a_j x^j + a_m x^m - \left(\sum_{j=0}^{n-1} \frac{a_m b_j}{b_n} x^{j+m-n} + a_m x^m\right) \\ &= \sum_{j=0}^{m-1} a_j x^j - \sum_{j=0}^{n-1} b_j x^{j+m-n} \end{aligned}$$

and this last expression is the difference of two polynomials, each of which has degree at most $m-1$). By our induction hypothesis, applied to $p(x) - \frac{a_m}{b_n}x^{m-n}d(x)$, $(\exists!\text{polynomials } q_1(x), r_1(x))[(p(x) - \frac{a_m}{b_n}x^{m-n}d(x) = q_1(x)d(x) + r_1(x) \wedge \deg r_1(x) < n)]$.
For existence, choose $q(x) = q_1(x) + \frac{a_m}{b_n}x^{m-n}$, and choose $r(x) = r_1(x)$. We then have

$$\begin{aligned} p(x) &= p(x) - \frac{a_m}{b_n}x^{m-n}d(x) + \frac{a_m}{b_n}x^{m-n}d(x) \\ &= q_1(x)d(x) + r_1(x) + \frac{a_m}{b_n}x^{m-n}d(x) \\ &= \left(q_1(x) + \frac{a_m}{b_n}x^{m-n}\right)d(x) + r_1(x) \\ &= q(x)d(x) + r(x) \end{aligned}$$

and $\deg r(x) = \deg r_1(x) < n$.
For uniqueness, suppose $p(x) = q'(x)d(x) + r'(x)$ and $\deg r'(x) < n$. Then

$$\begin{aligned} p(x) - \frac{a_m}{b_n}x^{m-n}d(x) &= q'(x)d(x) + r'(x) - \frac{a_m}{b_n}x^{m-n}d(x) \\ &= \left(q'(x) - \frac{a_m}{b_n}x^{m-n}\right)d(x) + r'(x) \end{aligned}$$

By the uniqueness part of our induction hypothesis, applied to $p(x) - \frac{a_m}{b_n}x^{m-n}d(x)$, we have $q'(x) - \frac{a_m}{b_n}x^{m-n} = q_1(x)$ and $r'(x) = r_1(x)$. Hence $q'(x) = q_1(x) + \frac{a_m}{b_n}x^{m-n} = q(x)$ and $r'(x) = r_1(x) = r(x)$.

By strong induction, $(\forall m \in \mathbb{N})[\deg p(x) = m \Rightarrow (\exists!\text{polynomials } q(x), r(x))[(p(x) = q(x)d(x) + r(x) \wedge \deg r(x) < n)]]$.

We considered the case where p(x) is the zero polynomial separately, and $d(x)$ was an arbitrary non-zero polynomial of degree n. So if $p(x)$ is any polynomial, and if $d(x)$ is a (non-zero) polynomial with finite degree n, then there exist unique polynomials $q(x)$ and $r(x)$ with $p(x) = q(x)d(x) + r(x)$ and $\deg r(x) < n$.

□

2.1.5(3) Let $p(x)$ be a polynomial and let a be a number. Then a is a root of $p(x)$ if and only if a is a factor of $p(x)$.

Proof. (⇒) Assume a is a root of $p(x)$. By part (a) above (with $x - a$ in place of $d(x)$), there are unique polynomials $q(x)$ and $r(x)$ such that $p(x) = q(x)(x-a) + r(x)$ and $\deg r(x) < \deg(x-a)$. Since $x - a$ is a polynomial of degree 1, $r(x)$ must have degree 0 or $-\infty$. In either case, $r(x)$ must be a constant polynomial. Since $0 = p(a) = q(a)(a-a) + r(a) = 0 + r(a) = r(a)$, we have $r(a) = 0$, and so $r(x)$ must be the constant zero polynomial. Hence $p(x) = q(x)(x-a)$, and so $x - a$ is a factor of $p(x)$.

($\Leftarrow$) Assume $x - a$ is a factor of $p(x)$. Then $p(x) = q(x)(x - a)$ for some polynomial $q(x)$. Hence $p(a) = q(a)(a - a) = 0$. So a is a root of $p(x)$.

□

2.1.6 (a) $[29]_{10} = 16 + 8 + 4 + 1 = 2^4 + 2^3 + 2^2 + 2^0 = [11101]_2$
(b) $[259]_{10} = 1 \cdot 243 + 1 \cdot 9 + 2 \cdot 3 + 1 \cdot 1 = 1 \cdot 3^5 + 1 \cdot 3^2 + 2 \cdot 3^1 + 1 \cdot 3^0 = [100121]_3$
(c) $[502]_{10} = 2 \cdot 243 + 1 \cdot 9 + 1 \cdot 3 + 2 \cdot 1 = 2 \cdot 3^5 + 1 \cdot 3^2 + 1 \cdot 3^1 + 2 \cdot 3^0 = [200112]_3$