Solutions to Homework #7

2. Prove the binomial theorem by induction on n using Lemma 13.4. **Hint:** Do the induction step in the form $S_{n-1} \Rightarrow S_n$ (or replace n by $n+1$ in Lemma 13.4). Also, it is probably technically easier to work with the expanded expression in the binomial theorem rather than working with the Σ-notation.

Solution: *Induction base:* $n = 1$. $(a+b)^1 = \binom{1}{0} a^1 b^0 + \binom{1}{1} a^0 b^1$ - true.

Induction step: Assume that $(a+b)^{n-1} = \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^k$ for some n. Then

$$(a+b)^n = (a+b)^{n-1} \cdot (a+b) = \left(\sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^k \right) (a+b) =$$

$$\left(\sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^k \right) \cdot a + \left(\sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^k \right) \cdot b =$$

$$\sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-1-k} b^{k+1}.$$

Now make a shift of index in the second sum: let $k' = k+1$ (the limits for k' will be from $k' = 1$ to $k' = n$). The second sum becomes $\sum_{k'=1}^{n} \binom{n-1}{k'-1} a^{n-k'} b^{k'}$. Since the name of summation variable does not matter, we can write k again instead of k'. Thus we get

$$(a+b)^n = \sum_{k=0}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=1}^{n} \binom{n-1}{k-1} a^{n-k} b^k.$$

In order to combine the two sums, we separate the term with $k = 0$ in the first sum and the term with $k = n$ in the second sum. We get

$$(a+b)^n = a^n + \sum_{k=1}^{n-1} \binom{n-1}{k} a^{n-k} b^k + \sum_{k=1}^{n-1} \binom{n-1}{k-1} a^{n-k} b^k + b^n =$$

$$a^n + b^n + \sum_{k=1}^{n-1} \left(\binom{n-1}{k} + \binom{n-1}{k-1} \right) a^{n-k} b^k =$$

using part (a) $$a^n + b^n + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} b^k = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

The induction step is complete.

3. Prove the equality $\binom{n}{k} = \binom{n}{n-k}$ using either the definition of binomial coefficients or the binomial theorem. You are not allowed to use the explicit formula for binomial coefficients involving factorials.

First solution: It will be convenient to phrase this solution in terms of bijective functions. Recall the notation $[n] = \{1, \ldots, n\}$. Let A denote the collection of all subsets of $[n]$ with k elements, and let B denote the collection of all subsets of $[n]$ with $n-k$ elements. By definition $\binom{n}{k} = |A|$ and $\binom{n}{n-k} = |B|$, so we need to show that $|A| = |B|$.

One way to prove that two finite sets A and B have the same cardinality is to construct a bijective function $f : A \to B$ (the particular bijective function f is not essential; what is important is that such f exists).

In our case we define $f : A \to B$ by $f(S) = S^c$, that is, the function f sends each subset S to its complement (in $[n]$). If S has k elements, its complement has $n-k$ elements, so f is indeed a function from A to B. To prove that f is bijective, we use Theorem 19.2(2) from class (=Theorem 6.2.4 from the book), that is, we construct a function $g : B \to A$ such that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.

Define $g : B \to A$ by $g(T) = T^c$, that is, g also sends each subset to its complement (note that even though f and g are given by the same formula, they are not equal as functions since they have different domains and different codomains). Since if we take the complement of a subset twice, we get the original subset back, we get $(g \circ f)(S) = g(f(S)) = (S^c)^c = S$ for all $S \in A$, so $g \circ f = \mathrm{id}_A$ and similarly $f \circ g = \mathrm{id}_B$.

Second solution: The binomial theorem can be thought of as equality of two polynomials in formal variables x and y:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \qquad (*)$$

Swapping x and y, we get

$$(y+x)^n = \sum_{k=0}^{n} \binom{n}{k} y^k x^{n-k} = \sum_{k=0}^{n} \binom{n}{n-k} x^k y^{n-k}. \qquad (**)$$

Since $(x+y)^n = (y+x)^n$, the polynomials on the right-hand sides of (*) and (**) must be equal, which means that for each i and j the coefficient of $x^i y^j$ in both polynomials must be the same. Since the coefficient of $x^k y^{n-k}$ is equal to $\binom{n}{k}$ in RHS(*) and to $\binom{n}{n-k}$ in RHS(**), we conclude that $\binom{n}{k} = \binom{n}{n-k}$.

4. Let A be a non-empty finite set. Prove that the total number of subsets of A which have even cardinality is equal to the total number of subsets of

A which have odd cardinality. **Hint:** It is enough to do the case $A = [n]$. Express both numbers in question in terms of binomial coefficients and use the binomial theorem.

Solution: By definition the binomial coefficient $\binom{n}{k}$ is equal to the number of k-element subsets of $[n]$. Thus, the total number of subsets of $[n]$ with even cardinality is $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots$ and the total number of subsets of $[n]$ with odd cardinality is $\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots$. We need to show that these two sums are equal; this is equivalent to showing that their difference is 0. Note that

$$\left(\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots\right) - \left(\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots\right)$$
$$= \binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \ldots = \sum_{k=0}^{n} (-1)^k \binom{n}{k}.$$

is the alternating sum of binomial coefficients $\binom{n}{k}$, as k ranges from 0 to n.

On the other hand by the binomial theorem $0 = 0^n = (1 + (-1))^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} (-1)^k = \sum_{k=0}^{n} \binom{n}{k} (-1)^k$, which finishes the proof.

Note that the equality $0^n = 0$ is true because n is positive, and n is positive since we assumed that A is non-empty.

5. Let $n \in \mathbb{N}$, and write $n = p_1^{a_1} \ldots p_k^{a_k}$ where $p_1, \ldots, p_k$ are distinct primes and $a_1, \ldots, a_k \in \mathbb{N}$. Use the general Fundamental Principle of Counting (FPC) to show that the number of positive divisors of n is equal to $\prod_{i=1}^{k} (a_i + 1)$. Give a detailed argument.

Solution: By Problem 3 in HW#6, positive divisors of n are precisely integers of the form $p_1^{b_1} \ldots p_k^{b_k}$ where $b_i \in \mathbb{Z}$ and $0 \le b_i \le a_i$ for each i. If $(b_1, \ldots, b_k)$ and $(c_1, \ldots, c_k)$ are distinct k-tuples of non-negative integers, then $p_1^{b_1} \ldots p_k^{b_k} \ne p_1^{c_1} \ldots p_k^{c_k}$ by the uniqueness part of FTA, so the total number of positive divisors of n is equal to the number of k-tuples $(b_1, \ldots, b_k)$ with $b_i \in \mathbb{Z}$ and $0 \le b_i \le a_i$. Since there are $a_i + 1$ integers between 0 and a_i (including 0 and a_i), we have $a_i + 1$ choices for b_i (for each i). We can choose each b_i independently of other b_j's, so by the fundamental principle of counting, the number of k-tuples $(b_1, \ldots, b_k)$ as above is equal to $\prod_{i=1}^{k} (a_i + 1)$.

6. Let $n \in \mathbb{N}$. Use Problem 5 and a suitable result from HW#6 to prove that the number of positive divisors of n is odd $\iff$ n is a perfect square.

Solution: We will use the following simple lemma whose proof is left as an exercise:

Lemma: *Let $n_1, \ldots, n_t$ be integers. Then the product $\prod_{i=1}^{t} n_i$ is odd if and only if each n_i is odd.*

If $n = 1$, then n is a perfect square and n has odd number of positive divisors (namely just 1 divisor – 1 itself). Thus, from now on we can assume that $n \geq 2$. By FTA we can write $n = p_1^{a_1} \ldots p_k^{a_k}$ where $p_1, \ldots, p_k$ are distinct primes and $a_1, \ldots, a_k \in \mathbb{N}$. By Problem 5, the total number of divisors of n is equal to $\prod\limits_{i=1}^{k}(a_i + 1)$. Note that

(i) By the above Lemma, $\prod\limits_{i=1}^{k}(a_i + 1)$ is odd $\iff$ each $a_i + 1$ is odd
(ii) Clearly, each $a_i + 1$ is odd $\iff$ each a_i is even
(iii) Finally, by Problem 2 in HW#6 each a_i is even $\iff$ n is a perfect square.

Combining (i), (ii) and (iii), we conclude that $\prod\limits_{i=1}^{k}(a_i + 1)$ is odd $\iff$ n is a perfect square, which finishes the proof.

7. Problem 24 in Section 3.1. **Hint:** There is a reason why this problem appears in this homework.

Solution: We claim that at the end the lockers that will be open are precisely the ones numbered by a perfect square. Indeed, take any n between 1 and 500. For each $1 \leq k \leq 500$, the k^{th} student will change the state of locker n (from 'closed' to 'open' or from 'open' to 'closed') if and only if n is a multiple of k or equivalently, $k \mid n$. Thus, the number of times the state of locker n will change is equal to the number of positive divisors of n.

At the beginning all lockers are closed. Thus, n^{th} locker will be open at the end if and only if its state has changed odd number of times. By the previous paragraph this will happen $\iff$ n has odd number of positive divisors which, by Problem 6, is equivalent to n being a perfect square.

8. Problem 7 in Section 4.2. **Answers:** (a) 26^6; (b) $26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21$; (c) $6 \cdot 25^5$; (d) $26^6 - 25^6$; (e) $25^6 + 6 \cdot 25^5 = 31 \cdot 25^5$.

Justification: (a),(c) and (d) done in class; (b) Since no letter should be repeated, we have 26 choices for the first letter, 25 choices for the second letter etc.; (e) There are 25^6 passwords in which a does not appear (same argument as in (a)) and $6 \cdot 25^5$ passwords in which a appears exactly once (by (c)). Since these two sets of passwords are disjoint and 'appears at most once' is the same as 'does not appear' or 'appears exactly once', the total number of passwords where a appears at most once is the sum of those two numbers.