Solutions to Homework #5

1. Problem 12 in 2.2 from the BOOK.

Solution: In this problem we will need to use strong induction. The reason is that the recursive formula for a_n involves not only a_{n-1}, but also a_{n-2}.

Computing a_n for the first few values of n, we conjecture that $a_n = n^2$ for all $n \in \mathbb{Z}_{\geq 0}$. We now prove the conjecture by strong induction.

Base case: $n = 0, 1$. For these two values of n the formula $a_n = n^2$ holds by definition.

Strong induction step: Now fix $n \geq 2$, and assume that $a_k = k^2$ for all $0 \leq k \leq n-1$. Since $n \geq 2$, in particular the induction hypothesis is true for $k = n-1$ and $k = n-2$, so we have $a_{n-1} = (n-1)^2$ and $a_{n-2} = (n-2)^2$. Hence, by the recursive formula for a_n we have

$$a_n = 2a_{n-1} - a_{n-2} + 2 = 2(n-1)^2 - (n-2)^2 + 2 = (2n^2 - 4n + 2) - (n^2 - 4n + 4) + 2 = n^2.$$

2. Let $n \in \mathbb{N}$, and let $\{A_1, \ldots, A_n\}$ be a collection of n finite sets such that any three distinct sets in the collection have empty intersection, that is, $A_i \cap A_j \cap A_k = \emptyset$ whenever i, j, k are distinct (we do NOT assume that the sets $\{A_i\}$ are disjoint). Use induction on n to prove that

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j|.$$

Solution: In order to solve this problem we will use the following two results proved in class.

Lemma 1: (proved in Lecture 2). *For any finite sets A and B we have* $|A \cup B| = |A| + |B| - |A \cap B|$.

Lemma 2: (proved in Lecture 8). *If $B_1, \ldots, B_n$ are finite pairwise disjoint sets, then* $|\bigcup\limits_{i=1}^{n} B_i| = \sum\limits_{i=1}^{n} |B_i|$.

We now start proving the formula in the problem by induction on n.

Base case: $n = 1, 2$. If $n = 1$, the assertion of the problem is vacuous, and there is nothing to prove. If $n = 2$, the problem asserts that $|A_1 \cup A_2|$ is equal to $|A_1| + |A_2| - \sum\limits_{1 \leq i < j \leq 2} |A_i \cap A_j| = |A_1| + |A_2| - |A_1 \cap A_2|$ (the only possible choice for i and j in the above sum is $i = 1$ and $j = 2$). And we know that $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$ by Lemma 1.

Induction step: Now fix $n \geq 2$, and assume that the given formula holds for all collections of n sets with required properties. We want to prove the formula for all collections of $n+1$ sets.

So let $A_1, \ldots, A_{n+1}$ be a collection of finite sets in which any 3 distinct sets have empty intersection. Our goal is to prove that

$$|\bigcup_{i=1}^{n+1} A_i| = \sum_{i=1}^{n+1} |A_i| - \sum_{1\leq i<j\leq n+1} |A_i \cap A_j|. \qquad (*)$$

First the union $\bigcup\limits_{i=1}^{n+1} A_i$ can be written as $A \cup B$ where $A = \bigcup\limits_{i=1}^{n} A_i$ and $B = A_{n+1}$, so by Lemma 1 we have

$$|\bigcup_{i=1}^{n+1} A_i| = |\bigcup_{i=1}^{n} A_i| + |A_{n+1}| - |(\bigcup_{i=1}^{n} A_i) \cap A_{n+1}|. \qquad (**)$$

By the induction hypothesis $|\bigcup\limits_{i=1}^{n} A_i| = \sum\limits_{i=1}^{n} |A_i| - \sum\limits_{1\leq i<j\leq n} |A_i \cap A_j|$, so

$$|\bigcup_{i=1}^{n} A_i| + |A_{n+1}| = \sum_{i=1}^{n+1} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| \qquad (***).$$

Let us now compute $|(\bigcup\limits_{i=1}^{n} A_i) \cap A_{n+1}|$. First by the distributive laws we have $(\bigcup\limits_{i=1}^{n} A_i) \cap A_{n+1} = \bigcup\limits_{i=1}^{n} (A_i \cap A_{n+1})$. If we set $B_i = A_i \cap A_{n+1}$, then the sets are pairwise disjoint since for any distinct i, j with $1 \leq i, j \leq n$ we have $B_i \cap B_j = A_i \cap A_j \cap A_{n+1}$, and the latter triple intersection is empty by assumption. Since the sets $B_i = A_i \cap A_{n+1}$ are pairwise disjoint, by Lemma 2 we have

$$|(\bigcup_{i=1}^{n} A_i) \cap A_{n+1}| = |\bigcup_{i=1}^{n} (A_i \cap A_{n+1})| = \sum_{i=1}^{n} |A_i \cap A_{n+1}|. \qquad (****)$$

Plugging the expressions from (***) and (****) into (**), we get

$$|\bigcup_{i=1}^{n+1} A_i| = \sum_{i=1}^{n+1} |A_i| - \sum_{1\leq i<j\leq n} |A_i \cap A_j| - \sum_{i=1}^{n} |A_i \cap A_{n+1}|.$$

To finish the proof of (*), we just need to show that $\sum\limits_{1\leq i<j\leq n+1} |A_i \cap A_j| = \sum\limits_{1\leq i<j\leq n} |A_i \cap A_j| + \sum_{i=1}^{n} |A_i \cap A_{n+1}|$. This becomes clear if we rewrite the second sum on the right-hand side as $\sum\limits_{1\leq i<j=n+1} |A_i \cap A_j|$.

3. Locate the mistake in the following "proof" by strong induction.

Let S_n be the statement "$2^{n-1} = 1$." We claim that S_n is true for all $n \in \mathbb{N}$.

Base case: S_1 is true since $2^{1-1} = 2^0 = 1$.

Strong induction step: Now fix $n \in \mathbb{N}$, and suppose that S_k is true for all $1 \le k \le n$. We need to show that S_{n+1} is true.

By definition of S_{n+1}, we need to show that $2^n = 1$. Using exponent laws, we can write

$$2^n = 2^{(2n-2)-(n-2)} = \frac{2^{2n-2}}{2^{n-2}} = \frac{(2^{n-1})^2}{2^{n-2}}. \qquad (***)$$

By induction hypothesis S_n and S_{n-1} are both true, so $2^{n-1} = 1$ and $2^{n-2} = 1$. Thus, from the equation (***) we get $2^n = \frac{1^2}{1} = 1$, so S_{n+1} is also true.

Solution: Similarly to the "proofs" of the statements 'All people have the same height' and 'all horses have the same color', the mistake occurs in the induction step for $n = 1$. Indeed, our induction hypothesis in this case is that S_k is true for all $1 \le k \le 1$, so we are only allowed to assume S_k for $k = 1$. However, in the computation we use the fact that S_n and S_{n-1} are true, so in the case $n = 1$ we are using S_1 (which is fine) and S_0 (which we cannot assume).

4. Solve Problem 2 in 3.1 directly using definition of divisibility.

Solution: (a) Assume that $a \mid b$ and $a \mid c$. By definition this means that $b = ak$ for some $k \in \mathbb{Z}$ and $c = al$ for some $l \in \mathbb{Z}$. Then $bc = (ak)(al) = a^2(kl)$. Since $kl \in \mathbb{Z}$, it follows that $a^2 \mid bc$.

(b) Assume that $a \mid b$ and $d \mid c$. By definition this means that $b = ak$ for some $k \in \mathbb{Z}$ and $c = dl$ for some $l \in \mathbb{Z}$. Then $bc = (ak)(dl) = ad(kl)$. Since $kl \in \mathbb{Z}$, it follows that $ad \mid bc$.

Note that we could of course first prove (b) and then deduce (a) from (b) by setting $d = a$; however, we proceeded as above since we were explicitly asked to solve both parts directly from definition.

5. Problem 1(a)(d) in 3.2.

Solution: (a) $330 = 231 \cdot 1 + 99$; $231 = 99 \cdot 2 + 33$; $99 = 33 \cdot 3 + 0$. Thus, $gcd(330, 231) = 99$.

Now we express 33 as a linear combination of 330 and 231. We have $33 = 231 - 99 \cdot 2 = 231 - (330 - 231) \cdot 2 = 231 \cdot 3 + 330 \cdot (-2)$.

(d) $509 = 132 \cdot 3 + 113$; $132 = 113 \cdot 1 + 19$; $113 = 19 \cdot 5 + 18$; $19 = 18 \cdot 1 + 1$; $18 = 18 \cdot 1 + 0$, so $gcd(509, 132) = 1$.

We have $1 = 19 - 18 = 19 - (113 - 19 \cdot 5) = 19 \cdot 6 - 113 = (132 - 113) \cdot 6 - 113 = 132 \cdot 6 - 113 \cdot 7 = 132 \cdot 6 - (509 - 132 \cdot 3) \cdot 7 = 132 \cdot 27 + 509 \cdot (-7)$.

6. Let $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$, and let $d = gcd(a, b)$. Let

$$d\mathbb{Z} = \{dk \mid k \in \mathbb{Z}\}$$

be the set of all multiples of d, and let

$$L_{a,b} = \{am + bn \mid m, n \in \mathbb{Z}\}$$

be the set of all integer linear combinations of a and b. Prove that $L_{a,b} = d\mathbb{Z}$ by showing that each of these two sets is contained in the other.

Solution: "$\subseteq$" Let $x \in L_{a,b}$. By definition $x = am+bn$ for some $m, n \in \mathbb{Z}$. Since $d = gcd(a, b)$, we have $d \mid a$ and $d \mid b$ and hence $d \mid x$ by Corollary 9.2 from class. By definition of divisibility this means that $x = dk$ for some $k \in \mathbb{Z}$, so $x \in \mathbb{Z}$. Thus, we showed the inclusion $L_{a,b} \subseteq d\mathbb{Z}$.

"$\supseteq$" Now let $x \in d\mathbb{Z}$, so $x = dk$ for some $k \in \mathbb{Z}$. Since $d = gcd(a, b)$, by Theorem 9.3 there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$. Thus $x = (au+bv)k = a(uk)+b(vk)$. Since $uk, vk \in \mathbb{Z}$, it follows that $x \in L_{a,b}$. Thus, we showed the inclusion $d\mathbb{Z} \subseteq L_{a,b}$.

7. Problem 7 in 3.1.

Solution: (a) $P_1 = \emptyset$, $P_8 = \{2\}$, $P_{12} = \{2, 3\}$, $P_{126} = \{2, 3, 7\}$.

(b) $10, 20, 40, 50, 80$.

(c) All integers of the form $\pm 2^k$ with $k \in \mathbb{N}$

(d) All integers of the form $\pm 3^a 5^b$ with $a, b \in \mathbb{N}$

(e) Corollary 3.1.5(d) from the book can be rephrased as follows: if $a, b \in \mathbb{Z}$ and $a \mid b$, then any divisor of a is also a divisor of b (in the notation of the corollary in the book b plays the role of a above, c plays the role of b and a plays the role of an arbitrary divisor). Thus, if $a \mid b$, then $D_a \subseteq D_b$ where as usual D_x is the set of all divisors of x.

On the other hand, by definition $P_x = D_x \cap P$ where P is the set of all primes. Thus, if $a \mid b$, then $D_a \subseteq D_b$, which implies that $D_a \cap P \subseteq D_b \cap P$ and hence $P_a \subseteq P_b$.

(f) False. Take $a = 8$ and $b = 4$. Then $P_a = P_b = \{2\}$, so in particular $P_a \subseteq P_b$, but a does not divide b.

(g) Since $-a = (-1)a$, we have $-a \mid a$, so $P_{-a} \subseteq P_a$ by part (e). Since this inclusion is true for any nonzero a, we can replace a by $-a$ in the formula to get $P_a = P_{-(-a)} \subseteq P_{-a}$. Thus, the sets P_{-a} and P_a are contained in each other and thus must be equal.

8. Problems 21 and 22 in 3.1.

Solution:

Problem 21. We proceed by induction *Base case* $n = 1$*:* $7^1 - 1 = 6$ is divisible by 6, so the statement is true for $n = 1$.

Induction step: Fix $n \geq 1$, and assume that $6 \mid (7^n - 1)$. We want to show that $6 \mid (7^{n+1} - 1)$.

The induction hypothesis $6 \mid (7^n - 1)$ means that $7^n - 1 = 6k$ for some $k \in \mathbb{Z}$. Thus, $7^n = 6k + 1$ and hence $7^{n+1} - 1 = 7 \cdot 7^n - 1 = 7(6k+1) - 1 = 6 \cdot 7k + 6 = 6(7k+1)$. Since $7k + 1 \in \mathbb{Z}$, it follows that $6 \mid (7^{n+1} - 1)$.

Problem 22. Here it may not be clear how to set up the induction step, so we start by computing $6^{n+1} + 5 \cdot 3^n - 1$ for some small values of n trying to figure our a pattern. We start with $n = 1$ which gives $36 + 15 - 1$ (we do not simplify on purpose; this is important, as you will see shortly); $n = 2$ gives $216 + 45 - 1$ and $n = 3$ gives $1296 + 135 - 1$. The pattern is now clear – it appears that the last digit of 6^{n+1} is always 6 and the last digit of $5 \cdot 3^n$ is always 5; this is equivalent to saying that

(i) $6^{n+1} - 6$ is divisible by 10 for all $n \in \mathbb{N}$
(ii) $5 \cdot 3^n - 5$ is divisible by 10 for all $n \in \mathbb{N}$

Note that we have not proved (i) and (ii), but it seems very likely that both are true.

We can now solve the problem as follows. First prove (i) and (ii) by induction – this is completely analogous by induction. Once this is done, we observe that $6^{n+1} + 5 \cdot 3^n - 1 = (6^{n+1} - 6) + (5 \cdot 3^n - 5) + 10$. By (i) and (ii), $6^{n+1} + 5 \cdot 3^n - 1$ is the sum of three numbers divisible by 10, so $6^{n+1} + 5 \cdot 3^n - 1$ is itself divisible by 10 (by Theorem 9.1 from class).