Math 230 D — Fall 2012
Homework 5 — Drew Armstrong

Problem 1. Recall that $a \equiv b \bmod n$ means that $n|(a-b)$. Use induction to prove that for all $n \geq 2$, the following holds:

"**if** $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that each $a_i \equiv 1 \bmod 4$, **then** $a_1 a_2 \cdots a_n \equiv 1 \bmod 4$."

[Hint: Call the statement $P(n)$. Note that $P(n)$ is a statement about **all** collections of n inegers. Therefore, when proving $P(k) \Rightarrow P(k+1)$ you must say "Assume that $P(k) = T$ and consider any $a_1, a_2, \ldots, a_{k+1} \in \mathbb{Z}$." What is the base case?]

Proof. Let $P(n)$ be the statement: "For any collection of n integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ such that $a_i \equiv 1 \bmod 4$ for all $1 \leq i \leq n$, we have $a_1 a_2 \cdots a_n \equiv 1 \bmod 4$." Note that the statement $P(2)$ is true, since given any $a_1, a_2 \in \mathbb{Z}$ with $a_1 = 4k_1 + 1$ and $a_2 = 4k_2 + 1$, we have

$$a_1 a_2 = (4k_1 + 1)(4k_2 + 1) = 16k_1k_2 + 4(k_1 + k_2) + 1 = 4(4k_1k_2 + k_1 + k_2) + 1.$$

Now **assume** that the statement $P(k)$ is true for some (fixed, but arbitrary) $k \geq 2$. In this case, we wish to show that $P(k+1)$ is also true. So consider any clollection of $k+1$ integers $a_1, a_2, \ldots, a_{k+1} \in \mathbb{Z}$ such that $a_i \equiv 1 \bmod 4$ for all $1 \leq i \leq k+1$, and then consider the product $a_1 a_2 \cdots a_{k+1}$. If we let $b = a_1 a_2 \cdots a_k$, then since $P(k)$ is true, we know that $b \equiv 1 \bmod 4$. But then since $P(2)$ is true we have

$$a_1 a_2 \cdots a_{k+1} = b a_{k+1} \equiv 1 \bmod 4,$$

as desired. By induction, we conclude that $P(n)$ is true for all $n \geq 2$. □

[I left some of the logical parentheses to the imagination. Do you know where they should be?]

Problem 2. Use induction to prove that for all integers $n \geq 2$ the following statement holds: "**If** p is prime and $p|a_1 a_2 \cdots a_n$ for some integers $a_1, a_2, \ldots, a_n \geq 2$, **then** there exists i such that $p|a_i$." [Hint: Call the statement $P(n)$. Use Euclid's Lemma for the induction step. You don't need to prove it again. In fact, there's no new math in this problem; just setting up notation and not getting confused.]

Proof. Let $P(n)$ be the statement: "For any collection of n integers $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ and any prime number $p \in \mathbb{Z}$, if p divides the product $a_1 \cdots a_n$, then there exists some $1 \leq i \leq n$ such that p divides a_i." Note that $P(2)$ is exactly Euclid's Lemma, which is true. Now **assume** that the statement $P(k)$ is true for some (fixed, but arbitrary) $k \geq 2$. In this case, we wish to show that $P(k+1)$ is also true. So consider any collection of $k+1$ integers $a_1, \ldots, a_{k+1} \in \mathbb{Z}$, let $p \in \mathbb{Z}$ be any prime number, and suppose that p divides $a_1 \cdots a_{k+1}$. If we let $b = a_1 \cdots a_k$ then since $p|ba_{k+1}$, Euclid's Lemma says that $p|a_{k+1}$, in which case we're done, or $p|b$. But if $p|b$ then since $P(k)$ is true there exists some $1 \leq i \leq k$ such that $p|a_i$. In any case, there exists some $1 \leq j \leq k+1$ such that $p|a_j$, hence $P(k+1)$ is true. By induction, we conclude that $P(n)$ is true for all $n \geq 2$. □

[Again, I went for style over absolute precision. I think you're ready for it.]

Problem 3. Use induction to prove that for all integers $n \geq 1$ we have

$$\text{“}1^3 + 2^3 + 3^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2.\text{”}$$

This result appears in the *Aryabhatiya* of Aryabhata (499 CE, when he was 23 years old). [Hint: You may assume the result $1 + 2 + \cdots + n = n(n+1)/2$.]

Proof. Let $P(n)$ be the statement:

$$\text{“}1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2 = \frac{n^2(n+1)^2}{4}.\text{”}$$

Note that the statment $P(1)$ is true since $1^3 = (1^2 \cdot 2^2)/4$. Now **assume** that $P(k)$ is true for some (fixed, but arbitrary) $k \geq 1$. That is, assume $1^3 + 2^3 + \cdots + k^3 = k^2(k+1)^2/4$. In this case, we wish to show that $P(k+1)$ is also true. Indeed, we have

$$\begin{aligned} 1^3 + 2^3 + \cdots + (k+1)^3 &= (1^3 + 2^3 + \cdots + k^3) + (k+1)^3 \\ &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= (k+1)^2 \left[\frac{k^2}{4} + (k+1)\right] \\ &= \frac{(k+1)^2}{4}\left[k^2 + 4k + 4\right] \\ &= \frac{(k+1)^2}{4}(k+2)^2 \\ &= \frac{(k+1)^2((k+1)+1)^2}{4}, \end{aligned}$$

hence $P(k+1)$ is true. By induction we conclude that $P(n)$ is true for all $n \geq 1$. □

Problem 4. Consider the following two statements/principles.

PSI: **If** $P : \mathbb{N} \to \{T, F\}$ is a family of statements satisfying

- $P(1) = T$, and
- for any $k \geq 1$ we have $[P(1) = P(2) = \cdots = P(k) = T] \Rightarrow [P(k+1) = T]$.

then $P(n) = T$ for all $n \in \mathbb{N}$.

WO: Every nonempty subset $K \subseteq \mathbb{N} = \{1, 2, 3, \ldots\}$ has a least element.

Now **Prove** that PSI $\Rightarrow$ WO. [Hint: Assume PSI and show that the (equivalent) contrapositive of WO holds; i.e., that if $K \subseteq \mathbb{N}$ has **no** least element then $K = \emptyset$. To do this you can use PSI to show that the complement K^c is all of $\mathbb{N}$. Let $P(n)$ be the statement "$n \in K^c$" and show using PSI that $P(n) = T$ for all $n \in \mathbb{N}$.]

Proof. We wish to show that PSI $\Rightarrow$ WO. So (OPEN MENTAL PARENTHESIS. assume that PSI holds. In this case we wish to show that WO holds. We will do this by showing the contrapositive statement: that if $K \subseteq \mathbb{N}$ has **no** least element then $K = \emptyset$. So (OPEN MENTAL PARENTHESIS. suppose that $K \subseteq \mathbb{N}$ has no least element. In this case we wish to show that $K = \emptyset$. We will use PSI (which is true in this universe) to prove the equivalent statement $K^c = \mathbb{N}$. So let $P(n) =$ "$n \in K^c$". We wish to show that $P(n) = T$ for all $n \in \mathbb{N}$. First note that $1 \in K^c$ since otherwise $1 \in K$ would be the least element of K, which contradicts our assumption that K has no least element. Next, fix an arbitrary $k \in \mathbb{N}$ and (OPEN MENTAL PARENTHESIS. suppose that $P(1) = P(2) = \cdots = P(k) = T$; i.e. suppose that $1, 2, \ldots, k \in K^c$. In this case we wish to show that $P(k+1) = T$; i.e. that $k+1 \in K^c$. But this is true because otherwise $k+1 \in K$ is the least element of K (since by assumption $1, 2, \ldots, k \notin K$) which contradicts our assumption that K has no least element. Hence $P(k+1) = T$. CLOSE MENTAL PARENTHESIS.) We have shown that $P(1) = T$ and that $P(1) = \cdots = P(k) = T$ implies $P(k+1) = T$ for all $k \in \mathbb{N}$. By the PSI we conclude that $P(n) = T$ for all $n \in \mathbb{N}$. In other words, $K^c = \mathbb{N}$, or $K = \emptyset$. CLOSE MENTAL PARENTHESIS.) We conclude that WO holds. CLOSE MENTAL PARENTHESIS.) Hence $\mathsf{PSI} \Rightarrow \mathsf{WO}$. $\square$

Problem 5. Let $d(n)$ be the number of binary strings of length n that contain no consecutive 1's. For example, there are 5 such strings of length 3:

$$000, \quad 100, \quad 010, \quad 001, \quad 101.$$

Hence $d(3) = 5$. Prove that $d(n)$ are (essentially) the Fibonacci numbers, and hence give a closed formula for $d(n)$. [Hint: First show that $d(n) = d(n-1) + d(n-2)$ for all $n \geq 3$. [Hint: The first digit (actually, bit) of a string can be either 1 or 0.] Then use PSI.]

First we will prove a **Lemma:** We have $d(n) = d(n-1) + d(n-2)$ for all $n \geq 3$.

Proof. We wish to count the binary strings of length n with no consecutive 1's. There are two cases: The first bit is either 0 or 1. If the first bit is 0, then the remaining $n-1$ bits can be any string that avoids consecutive 1's, and by definition there are $d(n-1)$ of these. If the first bit is 1, then the second bit **must** be 0 (otherwise the first two bits are 11). After this there are by definition $d(n-2)$ ways to complete the string. We conclude that $d(n) = d(n-1) + d(n-2)$. $\square$

Now we prove the theorem.

Proof. Recall that the Fibonacci numbers are defined by $f(0) = 0$, $f(1) = 1$, and $f(n) = f(n-1) + f(n-2)$ for all $n \geq 2$. We wish to show that $d(n) = f(n+2)$. So let $P(n) =$ "$d(n) = f(n+2)$". One can check that $P(1) = P(2) = T$ (and we even know $P(3) = T$, though we don't need it). Now fix an arbitrary $k \geq 3$ and (OPEN MENTAL PARENTHESIS. assume that $P(n) = T$ for all $1 \leq n \leq k$. In this case we wish to show that $P(k+1) = T$; i.e. that $d(k+1) = f(k+3)$. By assumption we have $d(k) = f(k+2)$ and $d(k-1) = f(k+1)$. Then applying the Lemma gives

$$\begin{aligned} d(k+1) &= d(k) + d(k-1) \\ &= f(k+2) + f(k+1) \\ &= f(k+3). \end{aligned}$$

Hence $P(k+1) = T$. CLOSE MENTAL PARENTHESIS.) We have shown that $P(1) = P(2) = T$ and if $P(n) = T$ for all $1 \leq n \leq k$ then $P(k+1) = T$. By (strong, I guess) induction we conclude that $P(n) = T$ for all $n \geq 1$. $\square$

Based on a result from class, we have the following.

Corollary: For all $n \geq 1$, we have

$$d(n) = f(n+2) = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+2} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+2} \right].$$