Math 230 E **Fall 2013**
Homework 5 **Drew Armstrong**

Problem 1. 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 because $1^3 = (1^2 \cdot 2^2)/4$. 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 2. Recall that $a \equiv b \pmod{n}$ 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 $a_i \equiv 1 \pmod{4}$, **then** $a_1 a_2 \cdots a_n \equiv 1 \pmod{4}$.”

[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 collection 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

$a_1a_2\cdots a_{k+1}$. If we let $b = a_1a_2\cdots a_k$, then since $P(k)$ is true, we know that $b \equiv 1 \bmod 4$. But then since $P(2)$ is true we have

$$a_1a_2\cdots a_{k+1} = ba_{k+1} \equiv 1 \bmod 4,$$

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

Problem 3 (Generalization of Euclid's Proof of Infinite Primes)

(a) Consider an integer $n > 1$. **Prove** that if $n \equiv 3 \pmod 4$ then n has a prime factor of the form $p \equiv 3 \pmod 4$. [Hint: You may assume that n has a prime factor p, which we proved in class. Note that there are three kinds of primes: the number 2, primes $p \equiv 1 \bmod 4$ and primes $p \equiv 3 \bmod 4$. Use Problem 2.]

(b) Prove that there are infinitely many prime numbers of the form $p \equiv 3 \pmod 4$. [Hint: Assume there are only **finitely** many and call them $3 < p_1 < p_2 < \cdots < p_k$. Then consider the number $N := 4p_1p_2\cdots p_k + 3$. By part (a) this N has a prime factor of the form $p \equiv 3 \pmod 4$. Show that this p is not in the list. Contradiction.]

Proof. To prove (a) let $n > 1$ be an integer such that $n \equiv 3 \bmod 4$. Consider its prime factorization

$$n = q_1q_2\cdots q_m.$$

Since n is odd (why?), the prime 2 does not appear in this factorization, so each prime factor is either $q_i \equiv 1 \bmod 4$ or $q_i \equiv 3 \bmod 4$. We claim that **at least one prime factor** is $\equiv 3 \bmod 4$. Suppose not, i.e., suppose that **every** prime factor is $\equiv 1 \bmod 4$. Then n is a product of numbers $\equiv 1 \bmod 4$, hence by Problem 2, n itself is $\equiv 1 \bmod 4$. Contradiction.

To prove (b) suppose for contradiction that there are only **finitely many** primes of the form $3 \bmod 4$, and call them $3 < p_1 < p_2 < \cdots < p_k$. (The fact that I didn't call $3 = p_1$ is a small trick. We will need it later on.) Now consider the number

$$N := 4p_1p_2\cdots p_k + 3.$$

We have $N \equiv 3 \bmod 4$, hence by part (a) there exists a prime $p \equiv 3 \bmod 4$ such that $p|N$. If we can show that this prime p is not in the set $\{3, p_1, \ldots, p_k\}$, we will obtain a contradiction. (We really needed part (a) because if $p \equiv 1 \bmod 4$, then $p \notin \{3, p_1, \ldots, p_k\}$ is **not** a contradiction.) But notice that none of $p_1, p_2, \ldots, p_k$ divides N, because if $p_i|N$ then we would have $p_i|(N - 4p_1\cdots p_k)$, hence $p_i|3$. But this contradicts the fact that $3 < p_i$. Finally, we note that $p \neq 3$ because 3 doesn't divide N. (If $3|N$ then we would also have $3|4p_1\cdots p_k$, and then Euclid's Lemma implies that $3|4$ or $3|p_i$ for some i. Contradiction.) We conclude that

$$p \notin \{3, p_1, p_2, \ldots, p_k\},$$

so p is a **new** prime of the form $3 \bmod 4$, contradicting the assumption that we had all of them. $\square$

Problem 4. Consider the following two statements/principles.

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

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

- $P(1) = T$ and
- for any $k \geq 1$ we have $P(k) \Rightarrow P(k+1)$,

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

Now **prove** that $\mathsf{WO} \Rightarrow \mathsf{PI}$. [Hint: Assume WO and assume that $P : \mathbb{N} \to \{T, F\}$ is a family of statements satisfying the hypotheses of PI. You want to show that $P(n) = T$ for all $n \geq 1$. Assume for contradiction that there exists $n \geq 1$ such that $P(n) = F$ and let S be the set of numbers $n \geq 1$ such that $P(n) = F$. By WO the set S has a least element $m \in S$. Since $P(1) = T$ we must have $m \geq 2$. Now use the existence m to derive a contradiction. Hence $P(n) = T$ for all $n \geq 1$ and it follows that PI is true.]

Proof. We wish to show that $\mathsf{WO} \Rightarrow \mathsf{PI}$. So, (OPEN MENTAL PARENTHESIS **assume** that WO holds. In this case we want to show that PI holds. So, (OPEN MENTAL PARENTHESIS **assume** that we have $P : \mathbb{N} \to \{T, F\}$ such that $P(1) = T$ and for any $k \geq 1$ we have $P(k) \Rightarrow P(k + 1)$. In this case we want to show that $P(n) = T$ for all $n \geq 1$. So, (OPEN MENTAL PARENTHESIS **assume for contradiction** that there exists some $n \geq 1$ such that $P(n) = F$ and define the set

$$S := \{n \geq 1 : P(n) = F\}.$$

By assumption this is a **nonempty** set of positive integers. Since we assumed that WO is true, the set S has a smallest element. Call it m. What do we know about this m? First of all, we know that $P(m) = F$ because $m \in S$. Second, we know that $m \geq 2$ because we assumed $P(1) = T$. Third, we know that $P(m - 1) = T$, otherwise we find that $m - 1 \geq 1$ is a **smaller** element of S. Finally, the fact that $P(m - 1) = T$ and $P(m) = F$ **contradicts** our assumption that $P(m - 1) \Rightarrow P(m)$. CLOSE MENTAL PARENTHESIS) Hence $P(n) = T$ for all $n \geq 1$. CLOSE MENTAL PARENTHESIS) And it follows that PI holds. CLOSE MENTAL PARENTHESIS) Finally, we conclude that $\mathsf{WO} \Rightarrow \mathsf{PI}$. $\square$