Week ??

Juan Patricio Carrizales Torres

Section 3: Proof by Minimum Counterexample

January 18, 2022

With the aid of **Theorem 7**, we were able to describe a more general principle of mathematical induction that can prove the quantified statement $\forall n \in S, P(n)$, where $S = \{n \in \mathbb{Z} : n \geq m\}$ for some integer m. However, there would be times where applying induction directly would not be so readily feasable. Therefore, one can use a Proof by Minimum Counterexample, which involves both techniques of proof by Mathematical Induction and proof by contradiction.

In a proof by Minimum Counterexample, one assumes for the statement $\forall n \in S, P(n)$ that there is some nonempty set $A \subseteq S$ such that $\forall x \in A, \sim P(x)$. Since S is well ordered, it follows that A has some lowest term m. Then, with the aid of mathematical induction we show that $P(n)$ is true for all integers $n \geq m$, which leads to a contradiction.

Problem 33. Use proof by minimum counterexample to prove that $6 \mid 7n\left(n^2-1\right)$ for every positive integer n.

Proof. Assume, to the contrary, that there are positive integers n for which $6 \nmid 7n\left(n^2-1\right)$. By the Well-ordering principle, there must be a lowest counterexample m. Therefore, $6 \mid 7n\left(n^2-1\right)$ for all positive integers $n < m$. Since $6 \mid 7\left(1^2-1\right)$ and $6 \mid 7 \cdot 2\left(2^2-1\right)$, it follows that the result is true for $n = 1, 2$ and so $m \geq 3$. Thus, $m = k + 2$ for some integer $1 \leq k < m$.

Note that

$$\begin{aligned}
7m\left(m^2-1\right) &= 7(k+2)\left((k+2)^2-1\right) \\
&= 7(k+2)\left(k^2+4k+4-1\right) \\
&= 7k(k^2-1) + 7k(4k+4) + 7 \cdot 2\left(k^2+4k+3\right) \\
&= 7k(k^2-1) + 7\left(6k^2+12k+6\right) \\
&= 7k(k^2-1) + 7 \cdot 6\left(k^2+2k+1\right)
\end{aligned}$$

Since $k < m$, it follows that $6 \mid 7k(k^2-1)$ and so $7k(k^2-1) = 6c$ for some integer c. Thus,

$$\begin{aligned}
7m\left(m^2-1\right) &= 6c + 7 \cdot 6\left(k^2+2k+1\right) \\
&= 6\left(c + 7\left(k^2+2k+1\right)\right)
\end{aligned}$$

Because $(c+7(k^2+2k+1)) \in \mathbb{Z}$, it follows that $6 \mid 7m(m^2-1)$ which leads to a contradiction. $\square$

Problem 34. Use the method of minimum counterexample to prove that $3 \mid (2^{2n}-1)$ for every positive integer n.

Proof. Assume, to the contrary, that there are $n \in \mathbb{N}$ such that $3 \nmid (2^{2n}-1)$. By the Well-ordering principle, the nonempty set of counterexamples must have a minimum which can be denoted as m. Since $3 \mid (3)$ and $3 \mid (15)$, it follows that the result is true for $n=1$ and $n=2$. Thus, $m \geq 3$ and so it can be expressed as $m = k+2$ for $1 \leq k < m$. Because the positive integer $k < m$, it follows that $3 \mid \left(2^{2k}-1\right)$ and so $2^{2k}-1 = 3x$ for some integer x.

Observe that

$$\begin{aligned} 2^{2m}-1 &= 2^{2(k+2)}-1 \\ &= 2^{2k}\left(2^4\right)-1 \\ &= 2^{2k}(15+1)-1 \\ &= 2^{2k}-1+15\cdot 2^{2k} \\ &= 3x+15\cdot 2^{2k} \\ &= 3\left(x+5\cdot 2^{2k}\right) \end{aligned}$$

Since $(x+5\cdot 2^{2k}) \in \mathbb{Z}$, it follows that $3 \mid (2^{2m}-1)$, which leads to a contradiction. $\square$

Problem 35. Give a proof by minimum counterexample that $1+3+5+\cdots+(2n-1) = n^2$ for every positive integer n.

Proof. Assume, to the contrary, that there are positive integers n such that $1+3+5+\cdots+(2n-1) \neq n^2$. Let m be the smallest such integer. Since $2(1)-1 = 1^2$, it follows that $m \geq 2$. Thus, the integer m can be expressed as $m = k+1$ for $1 \leq k < m$. Therefore, $1+3+5+\cdots+(2k-1) = k^2$.

Observe that

$$\begin{aligned} 1+3+5+\cdots+(2m-1) &= 1+3+5+\cdots+(2(k+1)-1) \\ &= [1+3+5+\cdots+(2k-1)]+(2(k+1)-1) \\ &= k^2+2k+1 = (k+1)^2 = m^2 \end{aligned}$$

This clearly leads to a contradiction. $\square$

Problem 36. Prove that $5 \mid (n^5-n)$ for every integer n.

Proof. Since $5 \mid (0^5-0)$, we consider the positive and negative integers. Suppose, to the contrary, that there are positive integers n such that $5 \nmid (n^5-n)$. Let m be the smallest such positive integer. Because $5 \mid (1^5-1)$, it follows that $m \geq 2$ and so it can be expressed as $m = k+1$, where $1 \le k < m$. Thus, $5 \mid (k^5 - k)$ and so $k^5 - k = 5c$ for some $c \in \mathbb{Z}$. Therefore,

$$\begin{aligned} m^5 - m &= (k+1)^5 - (k+1) \\ &= k^5 + 5k^4 + 10k^3 + 10k^2 + 5k + 1 - (k+1) \\ &= (k^5 - k) + 5\left(k^4 + 2k^3 + 2k^2 + k\right) \\ &= 5\left(c + k^4 + 2k^3 + 2k^2 + k\right) \end{aligned}$$

Since $(c + k^4 + 2k^3 + 2k^2 + k) \in \mathbb{Z}$, it follows that $5 \mid (m^5 - m)$, which leads to a contradiction.

We know that the set of negative integers can be expressed as $\mathbb{Z}_- = \{-x : x \in \mathbb{N}\}$. Now, note that if $5 \mid (k^5 - k)$ for some $k \in \mathbb{N}$, then $k^5 - k = 5x$, where $x \in \mathbb{Z}$, and so

$$\begin{aligned} (-k)^5 - (-k) &= -k^5 - (-k) \\ &= -\left(k^5 - k\right) \\ &= -5x = 5(-x). \end{aligned}$$

Since $-x \in \mathbb{Z}$, it follows that $5 \mid [(-k)^5 - (-k)]$.

Because we have proven that $5 \mid (n^5 - n)$ for every $n \in \mathbb{N}$, it follows that the result is also true for all negative integers. $\square$

Problem 37. Use proof by minimum counterexample to prove that $3 \mid (2^n + 2^{n+1})$ for every nonnegative integer n.

Proof. Assume, to the contrary, that there is some nonnegative integer n such that $3 \nmid (2^n + 2^{n+1})$. By **Theorem 7**, there must be a smallest nonnegative integer m such that $3 \nmid (2^m + 2^{m+1})$. Since $3 \mid (2^0 + 2^{0+1})$, it follows that $m \ge 1$ and so $m = k+1$, where $0 \le k < m$. Therefore, $3 \mid \left(2^k + 2^{k+1}\right)$ and so $2^k + 2^{k+1} = 3c$ for some $c \in \mathbb{Z}$. Note that

$$\begin{aligned} 2^m + 2^{m+1} &= 2^{k+1} + 2^{(k+1)+1} \\ &= 2 \cdot 2^k + 2 \cdot 2^{k+1} \\ &= 2\left(2^k + 2^{k+1}\right) = 2(3c) = 3(2c) \end{aligned}$$

Because $2c \in \mathbb{Z}$, it follows that $3 \mid (2^m + 2^{m+1})$. This leads to a contradiciton. $\square$

Problem 38. Give a proof by minimum counterexample that $2^n > n^2$ for every integer $n \ge 5$.

Proof. Assume, to the contrary, that there are integers $n \ge 5$ such that $2^n \le n^2$. By the Well-ordering principle, there is a smallest integer $m \ge 5$ such that $2^m \le m^2$. Since

$2^5 = 32 > 25 = (5)^2$, it follows that the statement is true for $n = 5$. Therefore, $m \geq 6$ and so it can be expressed as $m = k + 1$, where $5 \leq k < m$. Thus, $2^k > k^2$. Note that

$$\begin{aligned}
2^m &= 2^{k+1} \\
&= 2 \cdot 2^k \\
&> 2 \cdot k^2 = k^2 + k^2 \\
&\geq k^2 + 5k = k^2 + 2k + 3k \\
&\geq k^2 + 2k + 15 \\
&> k^2 + 2k + 1 = (k+1)^2.
\end{aligned}$$

Therefore, $2^{k+1} = 2^m > m^2 = (k+1)^2$, which leads to a contradiction. $\square$

Problem 39. Prove that $12 \mid (n^4 - n^2)$ for every positive integer n.

Proof. Suppose, to the contrary, that there are $n \in \mathbb{N}$ such that $12 \nmid (n^4 - n^2)$. Let m be the smallest such integer. Because $1^4 - 1^2 = 0$, $2^4 - 2^2 = 12$, and $3^4 - 3^2 = 72 = 12(6)$ it follows that $m \geq 4$. Hence, m can be expressed as $m = k + 3$ for $1 \leq k < m$. Therefore, $12 \mid (k^4 - k^2)$ and so $k^4 - k^2 = 12c$, where $c \in \mathbb{Z}$. Observe that

$$\begin{aligned}
m^4 - m^2 &= (k+3)^4 - (k+3)^2 \\
&= k^4 + 3 \cdot 4k^3 + 3^2 6k^2 + 3^3 4k + 3^4 - k^2 - 6k - 9 \\
&= \left(k^4 - k^2\right) + 6 \cdot 2k^3 + 6 \cdot 3^2 k^2 + 6(18-1)k + 72 \\
&= 12c + 6\left(2k^3 + 3^2 k^2 + 17k + 12\right) \\
&= 12c + 6\left[2\left(k^3 + 6\right) + k\left(9(k+1) + 8\right)\right].
\end{aligned}$$

We now show that $k\left(9(k+1)+8\right)$ is even. If k is even, then we are set (**Theorem 3.17**). On the other hand, if k is odd, then $k+1$ is even and so $9(k+1)+8$ is even since it is the sum of two even integers (**Theorem 3.16**). Thus, $k\left(9(k+1)+8\right)$ is even (**Theorem 3.17**). Therefore, $k\left(9(k+1)+8\right) = 2y$ for some $y \in \mathbb{Z}$ and so

$$\begin{aligned}
m^4 - m^2 &= 12c + 6\left[2\left(k^3 + 6\right) + k\left(9(k+1) + 8\right)\right] \\
&= 12c + 6\left[2\left(k^3 + 6\right) + 2y\right] \\
&= 12c + 12\left(k^3 + y + 6\right) = 12\left(k^3 + c + y + 6\right).
\end{aligned}$$

Since $k^3 + c + y + 6 \in \mathbb{Z}$, it follows that $12 \mid (m^4 - m^2)$, which leads to a contradiction. $\square$

Problem 40. First we prove a lemma.

Lemma 1. Let $t \in \mathbb{N}$. Then

$$2^t = 2^0 + 2^1 + \ldots + 2^{t-1} + 1$$

Proof. We procedd by induction. Since $2^1 = 2 = 2^0 + 1$, it follows that the lemma is true for $t = 1$. Assume that

$$2^k = 2^0 + 2^1 + \ldots + 2^{k-1} + 1.$$

We prove that

$$2^{k+1} = 2^0 + 2^1 + \ldots + 2^k + 1.$$

Note that

$$\begin{aligned}
2^{k+1} &= 2 \cdot 2^k \\
&= 2\left(2^0 + 2^1 + \ldots + 2^{k-1} + 1\right) \\
&= 2^1 + 2^2 + \ldots + 2^k + 2 = 2^1 + 2^2 + \ldots + 2^k + \left(1 + 2^0\right) \\
&= 2^0 + 2^1 + 2^2 + \ldots + 2^k + 1.
\end{aligned}$$

By the Principle of Mathematical Induction, this result is true. $\square$

We now proceed to prove the result

Result 40. Let $S = \{2^r : r \in \mathbb{Z}, r \geq 0\}$. Use proof by minimum counterexample to prove that for every $n \in \mathbb{N}$, there exists a subset S_n of S such that $\sum_{i \in S_n} i = n$.

Proof. Assume, to the contrary, that there is some $n \in \mathbb{N}$ such that $\sum_{i \in S_n} i \neq n$ for all possible subsets S_n of S. Let m be the smallest such positive integer.
Since $2^0 = 1$ and $\{2^0\} \subseteq S$, it follows that $m \geq 2$. Hence, $m = k + 1$ for $1 \leq k < m$. Therefore, there is some subset S_k of S such that $\sum_{i \in S_k} i = k$. Note that

$$m = k + 1 = \sum_{i \in S_k} i + 1.$$

If $2^0 \notin S_k$, then $S_m = S_k \cup \{2^0\}$. Therefore, $S_m \subseteq S$ and $\sum_{i \in S_m} i = m$, which leads to a contradiction.

On the other hand, if $2^0 \in S_k$, then define $A = \{t : t \geq 1, t \in \mathbb{Z}, 2^t \notin S_k\}$. By the Well-ordering principle, there is a smallest element $t \in A$. Observe that, by **Lemma 1**,

$$2^t = 2^0 + 2^1 + \ldots + 2^{t-1} + 1.$$

Therefore, let $B = \{2^0, 2^1, \ldots, 2^{t-1}\}$. Then, $S_m = (S_k - B) \cup \{2^t\}$ and so

$$\begin{aligned}
\sum_{i \in S_m} i &= \sum_{i \in (S_k - B)} i + 2^0 + 2^1 + \ldots + 2^{t-1} + 1 \\
&= \sum_{i \in (S_k - B)} i + \sum_{i \in B} i + 1 \\
&= \sum_{i \in S_k} i + 1 = k + 1 = m,
\end{aligned}$$

which leads to a contradiction. $\square$

Theorems used:

Theorem 3.16. Let $x, y \in \mathbb{Z}$. Then x and y are of the same parity if and only if $x + y$ is even.

Theorem 3.17. Let a and b be integers. Then ab is even if and only if a is even or b is even.