In-Class Problem Solutions for Session 3

Samuel Lair

August 2022

Contents

1 Problem 1

This problem is awkwardly formulated as filling in the blanks of a proof. I'm going to simply reproduce the entire proof with the blanks filled in.

Prove that every amount of postage that can assembled using only 10 cent and 15 stamps is divisible by 5.

Proof. Let the notation "$j|k$" indicate that integer j is a divisor of integer k, and let $S(n)$ mean that exactly n cents postage can be assembled using only 6 and 15 cent stamps. Then we need to prove:

$$S(n) \text{ IMPLIES } 3 \mid n, \text{ for all nonnegative integers } n \tag{1}$$

Let C be the set of *counterexamples* to (1), namely

$$C ::= \{\, n \mid S(n) \text{ and } \text{NOT}(3 \mid n) \,\}$$

Assume for the purpose of obtaining a contradiction that C is nonempty. Then by the WOP, there is a smallest $m \in C$. This m must be positive because (1) holds for $n = 0$.

But if $S(m)$ holds and m is positive, then $S(m-6)$ or $S(m-15)$ must hold because there exist nonnegative integers i and j such that $m = 6i + 15j$ and at least one of i, j is greater than zero. If $i > 0$, then $S(m-6)$ must hold. If $j > 0$, then $S(m-15)$ must hold.

So suppose $S(m-6)$ holds. Then $3 \mid (m-6)$ because $m-6 = 6i + 15j$ for nonnegative integers i and j and both $3 \mid 6$ and $3 \mid 15$ are true.

But if $3 \mid (m-6)$, then $3 \mid m$ because $m = 6(i+1) + 15j$, contradicting the fact that m is a counterexample.

Next, if $S(m-15)$ holds, we arrive at a contradiction in the same way.

Since we get a contradiction in both cases, we conclude that C is empty, which proves that (1) holds. $\square$

2   Problem 2

Prove that

$$\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \tag{2}$$

for all nonnegative integers n.

Proof. We use proof by contradiction. Suppose that the claim is false. Then, some nonnegative integers serve as *counterexamples* to it. Let's collect them in a set:

$$C ::= \left\{ n \in \mathbb{N} \;\middle|\; \sum_{k=0}^{n} k^2 \neq \frac{n(n+1)(2n+1)}{6} \right\}$$

By the WOP, C has a minimum element c. I.e. (2) is false for $n = c$ but true for all nonnegative integers $n < c$. Since (2) is true for $n = 0$, $c > 0$. Therefore, $c - 1$ is a nonnegative integer for which (2) holds:

$$\sum_{k=0}^{c-1} k^2 = \frac{(c-1)(c-1+1)(2(c-1)+1)}{6} = \frac{c(c-1)(2c-1)}{6}$$

But if we add c^2 to both sides of this equation, we find:

$$\sum_{k=0}^{c} k^2 = \frac{c(c-1)(2c-1)}{6} + c^2 = \frac{(c^2 - c)(2c-1) + 6c^2}{6}$$

$$= \frac{2c^3 - c^2 - 2c^2 + c + 6c^2}{6} = \frac{c(2c^2 + 3c + 1)}{6} = \frac{c(c+1)(2c+1)}{6}$$

Therefore, we've reached a contradiction where (2) holds for c. Hence, C is empty and the claim must be true. □

3 Problem 3

Prove that

$$\nexists\, a, b, c, d \in \mathbb{Z}^+ \text{ such that } 8a^4 + 4b^4 + 2c^4 = d^4. \tag{3}$$

Proof. The proof is by the WOP. Let C be the set of counterexamples to (3). We will prove by contradiction that C is empty. Suppose that C is not empty. Then by the WOP, there is a tuple (a_0, b_0, c_0, d_0) among the elements of C such that a_0 is the least value of a of all such tuples in C. Since $8a_0^4 + 4a_0^4 + 2c_0^4 = d_0^4$, d_0^4 is a multiple of 2. By the *Fundamental Theorem of Arithmetic*, d_0 is also a multiple of 2. I.e. $\exists\, k \in \mathbb{Z}^+$ such that $d_0 = 2k$. Then:

$$c_0^4 = 8k^4 - 2b_0^4 - 4a_0^4$$

Therefore, c_0^4 is a multiple of 2. By the *Fundamental Theorem of Arithmetic*, c_0 is also a multiple of 2. I.e. $\exists\, j \in \mathbb{Z}^+$ such that $c_0 = 2j$. Then:

$$b_0^4 = 4k^4 - 8j^4 - 2a_0^4$$

Therefore, b_0^4 is a multiple of 2. By the *Fundamental Theorem of Arithmetic*, b_0 is also a multiple of 2. I.e. $\exists\, i \in \mathbb{Z}^+$ such that $b_0 = 2i$. Then:

$$a_0^4 = 2k^4 - 4j^4 - 8i^4.$$

Therefore, a_0^4 is a multiple of 2. By the *Fundamental Theorem of Arithmetic*, a_0 is also a multiple of 2. I.e. $\exists\, h \in \mathbb{Z}^+$ such that $a_0 = 2h$. But then:

$$128h^4 + 64i^4 + 32j^4 = 16k^4 \implies 8h^4 + 4i^4 + 2^4 = k^4$$

Therefore, $(h, i, j, k) \in C$. However, this is contradiction since $a_0 = 2h \implies h < a_0$. Hence, C is empty and (3) must be true.

$\square$

4   Problem 4

This problem is actually about the unsigned binary representation of unsigned integers. Namely, we asked to prove that $m + 1$ unsigned bits can represent any nonnegative integer less than or equal to $2^{m+1} - 1$. Let's restate the claim in a more straightforward manner.

Given $S ::= \{0, 1\}$ and $n \in \mathbb{N}$ such that $n < 2^{m+1}$ for some $m \in \mathbb{N}$, prove that:

$$\exists\, a_0, a_1, ..., a_m \in S \text{ such that } n = a_0 2^0 + a_1 2^1 + ... + a_m 2^m \tag{4}$$

Proof. The proof is by case analysis. Consider the following cases:

1. $m = 0$

2. $m > 0$

Case 1: We need to consider nonnegative integers less than $2^{0+1} = 2$. Fortunately, there are only two such nonnegative integers: 0 and 1. Consider that:

$$0 = 0 \cdot 2^0$$
$$1 = 1 \cdot 2^0$$

(4) holds for Case 1.

Case 2: The proof for this case is by the WOP. Let C be the set of counterexamples to (4). We will prove by contradiction that C is empty. Suppose that C is not empty. By the WOP, there is a least integer $q \in C$. Since q is the least counterexample, (4) must hold for $q - 1$:

$$q - 1 = a_0 2^0 + a_1 2^1 + ... + a_m 2^m$$
$$q = a_0 2^0 + a_1 2^1 + ... + a_m 2^m + 1$$

Let us now consider two subcases:

1. $q - 1 < 2^{m+1} - 1$

2. $q - 1 = 2^{m+1} - 1$

Case 2.1: Since $q - 1 < 2^{m+1} - 1$, at least one of the coefficients $a_0, ..., a_m$ equals 0. By the WOP, there exists a least index i such that $a_i = 0$. Then:

$$q = q - 1 + 1 = 0 \cdot 2^0 + 0 \cdot 2^1 + ... + 1 \cdot 2^i + a_{i+1} \cdot 2^{i+1} + ... + a_m \cdot 2^m$$

This leads us to the contradiction that (4) holds for q. Therefore, C is empty and (4) holds in this subcase.

Case 2.2: In this case, $q = q - 1 + 1 = 2^{m+1} - 1 + 1 = 2^{m+1}$. Therefore, we have a contradiction where q isn't a counterexample since (4) only makes a claim for $n < 2^{m+1}$. Therefore, C is empty and (4) holds in this subcase.

C is empty and (4) holds in Subcases 2.1 and 2.2. Therefore, C is empty and (4) holds in Case 2.

(4) holds for Cases 1 and 2. Therefore, (4) must be true.

$\square$

5   Problem 5

Prove that any integer greater than or equal to 30 can be represented as the sum of integer multiples of 6, 10, and 15.

Proof. Our claim can be restated as follows:

$$\forall\, n \in \mathbb{N}, \exists\, i, j, k \in \mathbb{N} \text{ such that } n + 30 = 6i + 10j + 15k \tag{5}$$

The proof is by the WOP. Let C be the set of counterexamples to (5). We will prove by contradiction that C is empty. Suppose that C is not empty. By the WOP, there is a least nonnegative integer $m \in C$. Consider the following:

$$0 + 30 = 30 = 2 \cdot 15 + 3$$

$$1 + 30 = 31 = 1 \cdot 6 + 1 \cdot 10 + 1 \cdot 15$$

$$2 + 30 = 32 = 2 \cdot 6 + 2 \cdot 10$$

$$3 + 30 = 33 = 3 \cdot 6 + 1 \cdot 15$$

$$4 + 30 = 34 = 4 \cdot 6 + 1 \cdot 10$$

$$5 + 30 = 35 = 2 \cdot 10 + 1 \cdot 15$$

Therefore, $m \geq 6$, which ensures that $(m - 6) \in \mathbb{N}$. Since m is the minimum counterexample, (**??**) must hold for $m - 6$. I.e.

$$\exists\, i, j, k \in \mathbb{N} \text{ such that } m - 6 + 30 = 6i + 10j + 15k$$

But then $m + 30 = 6(i+1) + 10j + 15k \implies m \notin C$, a contradiction. Therefore, C is empty and (5), which is equivalent to our claim, must be true. $\qquad\square$