

# 1 Answers to Problems

## 1.1 The Integers

91/100

1. Determine whether each of the following sets is well-ordered. If so, give a proof which relies on the fact that  $\mathbb{Z}^+$  is well-ordered. If not, give an example of a subset with no least element. 10/10

(a)  $\{a \mid a \in \mathbb{Z}, a > 3\}$

Is a subset of  $\mathbb{Z}^+$  and therefore is well-ordered.

(b)  $\{a \mid a \in \mathbb{Q}, a > 3\}$

There is no least element so the set is not well-ordered.

(c)  $\{\frac{a}{2} \mid a \in \mathbb{Z}, a \geq 10\}$

Consider the set  $\{a \mid a \in \mathbb{Z}, a \geq 10\}$ , it is apparent that this is a subset of  $\mathbb{Z}^+$  and therefore is well-ordered. So the set  $\{\frac{a}{2} \mid a \in \mathbb{Z}, a \geq 10\}$  is also well-ordered because it holds a least element ( $\frac{10}{2}$ ).

(d)  $\{\frac{2}{a} \mid a \in \mathbb{Z}, a > 10\}$

There is no least element so the set is not well-ordered.

2. Suppose  $a, b \in \mathbb{Z}^+$  are unknown. Let  $S = \{a - bk \mid k \in \mathbb{Z}, a - bk > 0\}$ . Explain why  $S$  has a smallest element but no largest element. 3/10

Since  $S$  is a subset of  $\mathbb{Z}^+$  by well-ordering we know that  $S$  has a least element, and because  $k \in \mathbb{Z}$ ,  $k$  can be 0 and therefore there is no most element.

3. Use the well-ordering property to show that  $\sqrt{5}$  is irrational. 10/10

*Proof.* Suppose  $\sqrt{5}$  is rational and is of the form  $\frac{a}{b}$  where  $a, b \in \mathbb{Z}^+$  and  $b \neq 0$ . Consider the set  $S$ ,

$$S = \{k \mid k, k\sqrt{5} \in \mathbb{Z}^+\}$$

We know that  $S$  is a subset of  $\mathbb{Z}^+$  and that  $b \in S$ , by well-ordering this implies that  $S$  has a least element. Let  $l$  be the least element in  $S$ .

Consider the properties of  $l'$  where  $l' = l\sqrt{5} - 2l$ ,

- $l' = l\sqrt{5} - 2l = l(\sqrt{5} - 2) \implies 0 < l' < l$ .
- Since  $l \in S$  and  $S \subset \mathbb{Z}^+$ , both  $l$  and  $l\sqrt{5} \in \mathbb{Z}^+$  which implies  $l' \in \mathbb{Z}^+$ .
- Since  $l \in \mathbb{Z}^+$  we have  $5l \in \mathbb{Z}^+$  and since  $l\sqrt{5} \in \mathbb{Z}^+$  we have  $l'\sqrt{5} = (l\sqrt{5} - 2l)\sqrt{5} = 5l - 2l\sqrt{5} \in \mathbb{Z}^+$ .

It follows that  $l' \in S$  but  $l' < l$  which contradicts  $l$  being the least element in  $S$ .  $\square$

4. Use the identity

$$\frac{1}{k^2 - 1} = \frac{1}{2} \left( \frac{1}{k-1} - \frac{1}{k+1} \right)$$

to evaluate the following:

10/10

(a)  $\sum_{k=2}^{10} \frac{1}{k^2 - 1}$

$$\begin{aligned} \sum_{k=2}^{10} \frac{1}{k^2 - 1} &= \sum_{k=2}^{10} \frac{1}{2} \left( \frac{1}{k-1} - \frac{1}{k+1} \right) = \frac{1}{2} \sum_{k=2}^{10} \left( \frac{1}{k-1} - \frac{1}{k+1} \right) \\ &= \frac{1}{2} \left[ \left( \frac{1}{1} - \frac{1}{3} \right) + \cdots + \left( \frac{1}{8} - \frac{1}{10} \right) + \left( \frac{1}{9} - \frac{1}{11} \right) \right] \\ &= \frac{1}{2} \left[ \frac{1}{1} + \frac{1}{2} - \frac{1}{10} - \frac{1}{11} \right] \\ &= \frac{1}{2} \left( \frac{72}{55} \right) = \frac{36}{55} \end{aligned}$$

(b)  $\sum_{k=2}^n \frac{1}{k^2 - 1}$

$$\sum_{k=2}^n \frac{1}{k^2 - 1} = \frac{1}{2} \left[ \frac{1}{1} + \frac{1}{2} - \frac{1}{n} - \frac{1}{n+1} \right]$$

(c)  $\sum_{k=1}^n \frac{1}{k^2 + 2k}$  Hint:  $k^2 + 2k = (k+1)^2 - 1$

$$\begin{aligned} \sum_{k=1}^n \frac{1}{k^2 + 2k} &= \sum_{k=1}^n \frac{1}{(k+1)^2 - 1} = \sum_{k=2}^{n+1} \frac{1}{k^2 - 1} \\ \sum_{k=2}^{n+1} \frac{1}{k^2 - 1} &= \frac{1}{2} \left[ \frac{1}{1} + \frac{1}{2} - \frac{1}{n+1} - \frac{1}{n+2} \right] \end{aligned}$$

5. Find the value of each of the following:

10/10

(a)  $\prod_{j=2}^7 \left( 1 - \frac{1}{j} \right)$

$$\begin{aligned} \prod_{j=2}^7 \left( 1 - \frac{1}{j} \right) &= \left[ \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \frac{4}{5} \cdot \frac{5}{6} \cdot \frac{6}{7} \right] \\ &= \frac{1}{7} \end{aligned}$$

$$(b) \prod_{j=2}^n \left(1 - \frac{1}{j}\right)$$

$$\prod_{j=2}^n \left(1 - \frac{1}{j}\right) = \frac{1}{n}$$

$$(c) \prod_{j=2}^n \left(1 - \frac{1}{j^2}\right) \quad \text{Hint: Be sneaky!}$$

$$\prod_{j=2}^n \left(1 - \frac{1}{j^2}\right) = \frac{n+1}{2n}$$

6. Use weak mathematical induction to prove that

$$\sum_{j=1}^n j(j+1) = \frac{n(n+1)(n+2)}{3}$$

for every positive integer  $n$ .

9/10

*Proof.*

**Base Case:**

Let  $n = 1$ ,  $\sum_{j=1}^1 j(j+1) = 2$  and  $\frac{1(1+1)(1+2)}{3} = 2$ , so the base case is valid.

**Inductive Hypothesis:**

Assume from the inductive hypothesis that the conclusion is true for some  $n$ .

This implies that  $\sum_{j=1}^n j(j+1) = \frac{n(n+1)(n+2)}{3}$ .

**Inductive Step:**

Then consider the sum to  $n+1$ :

$$\begin{aligned} \sum_{j=1}^{n+1} j(j+1) &= \sum_{j=1}^n j(j+1) + (n+1)((n+1)+1) \\ &= \left[ \frac{n(n+1)(n+2)}{3} \right] + (n+1)((n+1)+1) \text{ by IH} \\ &= \frac{1}{3} (n(n+1)(n+2) + 3(n+1)(n+2)) \\ &= \frac{1}{3} (n^3 + 3n^2 + 2n + 3n^2 + 9n + 6) \\ &= \frac{1}{3} (n^3 + 6n^2 + 11n + 6) \\ &= \frac{1}{3} ((n+1)(n+2)(n+3)) \end{aligned}$$

Thus for all  $n \geq 1$ ,

$$\sum_{j=1}^n j(j+1) = \frac{n(n+1)(n+2)}{3}$$

□

7. Use Weak Mathematical Induction to show that  $f_n f_{n+2} = f_{n+1}^2 + (-1)^{n+1}$  for all  $n \geq 1$ . 9/10

*Proof.*

**Base Case:**

Rewrite the statement  $f_n f_{n+2} = f_{n+1}^2 + (-1)^{n+1}$  to be  $f_n f_{n+2} - f_{n+1}^2 = (-1)^{n+1}$ .

Let  $n = 1$ ,  $f_1 f_{1+2} - f_{1+1}^2 = 1 \cdot 2 - 1 = 1$  and  $(-1)^{1+1} = 1$ , so the base case is valid.

**Inductive Hypothesis:**

Assume from the inductive hypothesis that the conclusion is true for some  $n$ .

This implies that  $f_n f_{n+2} - f_{n+1}^2 = (-1)^{n+1}$

**Inductive Step:**


Then consider the equation to  $n + 1$ :

$$\begin{aligned} f_{(n+1)} f_{(n+1)+2} - f_{(n+1)+1}^2 &= f_{n+1} f_{n+3} - f_{n+2}^2 \\ &= f_{n+1} (f_{n+1} + f_{n+2}) - f_{n+2}^2 \\ &= f_{n+1}^2 + f_{n+1} f_{n+2} - f_{n+2}^2 \\ &= f_{n+1}^2 + f_{n+2} (f_{n+1} - f_{n+2}) \\ &= f_{n+1}^2 + f_{n+2} (-f_n) \\ &= - (f_n f_{n+2} - f_{n+1}^2) \\ &= -(-1)^{n+1} \quad \text{by IH} \\ &= (-1)^{n+2} \end{aligned}$$

Thus for all  $n \geq 1$ ,

$$f_n f_{n+2} - f_{n+1}^2 = (-1)^{n+1}$$

□

8. Use weak mathematical induction to show that a  $2^n \times 2^n$  chessboard with a corner missing can be tiled with pieces shaped like  for every integer  $n \geq 0$ . 10/10

*Proof.*

**Base Case:**

Let  $n = 1$ ,  $2^1 \times 2^1$  is a  $2 \times 2$  chessboard with a corner missing and can be tiled by one tromino, so the base case is valid.

**Inductive Hypothesis:**

Assume from the inductive hypothesis that the conclusion is true for some  $n$ . This implies that any  $2^n \times 2^n$  chessboard with a corner missing can be tiled with trominoes.

**Inductive Step:**

Then consider a  $2^{n+1} \times 2^{n+1}$  chessboard.

- Divide the  $2^{n+1} \times 2^{n+1}$  chessboard into four quadrants of size  $2^n \times 2^n$ .
- By the Inductive Hypothesis we know that each  $2^n \times 2^n$  has one corner missing.
- There are then four empty squares in the  $2^{n+1} \times 2^{n+1}$  board.
- Rotate each quadrant such that the four empty squares are in the center of the board.
- Add another tromino into the board leaving only one empty square.
- Rotate the quadrant with the empty square such that the empty square is in the corner of the board.
- Therefore the  $2^{n+1} \times 2^{n+1}$  chessboard can be tiled by trominoes with a corner missing.

Thus, every  $2^n \times 2^n$  chessboard with a corner missing can be tiled with trominoes.

□

9. Define:

$$H_{2^n} = \sum_{j=1}^{2^n} \frac{1}{j}$$

Use weak mathematical induction to prove that for all  $n \geq 1$  we have  $H_{2^n} \leq 1 + n$ .

10/10

*Proof.*

**Base Case:**

Let  $n = 1$ ,  $H_{2^1} = \sum_{j=1}^{2^1} \frac{1}{j} = \frac{3}{2}$  and  $\frac{3}{2} \leq 2$ , so the base case is valid.

**Inductive Hypothesis:**

Assume from the inductive hypothesis that the conclusion is true for some  $n$ .

This implies that  $\sum_{j=1}^{2^n} \frac{1}{j} \leq 1 + n$ .

**Inductive Step:**

Then consider the equation to  $n + 1$ :

$$\begin{aligned}
 H_{2^{n+1}} &= \sum_{j=1}^{2^{n+1}} \frac{1}{j} \\
 &= \sum_{j=1}^{2^n} \frac{1}{j} + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} \\
 &\leq [1 + n] + \sum_{j=2^n+1}^{2^{n+1}} \frac{1}{j} \quad \text{by IH} \\
 &\leq [1 + n] + \frac{1}{2^n + 1} + \cdots + \frac{1}{2^{n+1}} \\
 &\leq [1 + n] + 2^n \cdot \frac{1}{2^{n+1}} \\
 &\leq \frac{3}{2} + n \leq 2 + n
 \end{aligned}$$

Thus for all  $n \geq 1$ ,

$$H_{2^n} \leq 1 + n$$

□

10. Use strong mathematical induction to prove that every amount of postage over 53 cents can be formed using 7-cent and 10-cent stamps. 10/10

*Proof.*

**Inductive Step:**

Assume we can do  $54, \dots, k$ . Because  $k - 6$  is in the  $54, \dots, k$  we can do  $k - 6$  then add a 7-cent stamp.  $k - 6$  is in  $54, \dots, k$  only if  $k - 6 \geq 54 \equiv k \geq 60$ . Thus, the inductive step is only valid for  $k = 60, 61, \dots$  to get to the next  $k + 1$ .

**Base Case:**

Must do 54, 55, 56, 57, 58, 59, 60 as base cases.

$$54 = 2(7\text{-cent}) + 4(10\text{-cent})$$

$$55 = 5(7\text{-cent}) + 2(10\text{-cent})$$

$$56 = 8(7\text{-cent})$$

$$57 = 1(7\text{-cent}) + 5(10\text{-cent})$$

$$58 = 4(7\text{-cent}) + 3(10\text{-cent})$$

$$59 = 7(7\text{-cent}) + 1(10\text{-cent})$$

$$60 = 6(10\text{-cent})$$

□

## 1.2 Primes and GCDs

69/80

1. Use the Euclidean Algorithm to calculate  $d = \gcd(510, 140)$  and then use the result to find  $\alpha$  and  $\beta$  so that  $d = 510\alpha + 140\beta$ . 10/10

Need to find  $\gcd(510, 140)$ .

$$510 = 3(140) + 90$$

$$140 = 1(90) + 50$$

$$90 = 1(50) + 40$$

$$50 = 1(40) + 10$$

$$40 = 4(10) + 0$$

So the gcd is 10. Now to find the linear combination.

$$\begin{aligned} 10 &= 1(50) - 1(40) \\ &= 1(50) - 1(90 - 1(50)) \\ &= 2(50) - 1(90) \\ &= 2(140 - 1(90)) - 1(90) \\ &= 2(140) - 3(90) \\ &= 2(140) - 3(510 - 3(140)) \\ &= -3(510) + 11(140) \\ &= \alpha a + \beta b \end{aligned}$$

where  $\alpha = -3$  and  $\beta = 11$ .

2. Use the Euclidean Algorithm to show that if  $k \in \mathbb{Z}^+$  that  $3k+2$  and  $5k+3$  are relatively prime. 8/10

Need to show that  $\gcd(3k+2, 5k+3) = 1$  for all  $k \in \mathbb{Z}^+$ .

$$5k+3 = 1(3k+2) + (2k+1)$$

$$3k+2 = 1(2k+1) + (k+1)$$

$$2k+1 = 1(k+1) + k$$

$$k+1 = 1(k) + 1$$

So the  $\gcd(3k+2, 5k+3) = 1$ , therefore  $3k+2$  and  $5k+3$  are relatively prime.

3. How many zeros are there at the end of  $(1000!)$ ? Do not do this by brute force. Explain your method. 10/10

Zeros at the end of numbers are from multiples of 10 which are pairs of 2 and 5, so we find the number of pairs of 2's and 5's to find the number of zeros. Let  $d_n(x)$  represent the sum of the numbers divisible by all powers of  $n$  less than  $x$ .

$$d_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 = 994$$

$$d_5(1000!) = 200 + 40 + 8 + 1 = 249$$

Thus, there can only be 249 pairs of 2's and 5's, so there are only 249 10's, so there are 249 zeros at the end of  $(1000!)$ .

4. Let  $a = 1038180$  and  $b = 92950$ . First find the prime factorizations of  $a$  and  $b$ . Then use these to calculate  $\gcd(a, b)$  and  $\text{lcm}(a, b)$ . 10/10

Find the prime factorization of  $a$ .

$$\begin{aligned} 1038180 &= 2^2(259545) \\ &= 2^23^1(86515) \\ &= 2^23^15^1(17303) \\ &= 2^23^15^111^3(13) \\ &= 2^23^15^111^313^1 \end{aligned}$$

Find the prime factorization of  $b$ .

$$\begin{aligned} 92950 &= 2^1(46475) \\ &= 2^15^2(1859) \\ &= 2^15^211^1(169) \\ &= 2^15^211^113^2 \end{aligned}$$

Now, to find the  $\gcd(a, b)$  and  $\text{lcm}(a, b)$ .

$$\gcd(a, b) = \gcd(2^23^15^111^313^1, 2^15^211^113^2) = 2^15^111^113^1 = 1430$$

$$\text{lcm}(a, b) = \text{lcm}(2^23^15^111^313^1, 2^15^211^113^2) = 2^23^15^211^313^2 = 67481700$$



5. Which pairs of integers have gcd of 18 and lcm of 540? Explain. 10/10

Find the prime factorization of 18.

$$\begin{aligned} 18 &= 2^1(9) \\ &= 2^13^2 \end{aligned}$$

Find the prime factorization of 540.

$$\begin{aligned} 540 &= 2^2(135) \\ &= 2^23^3(5) \\ &= 2^23^35^1 \end{aligned}$$

From the prime factors of 18 and 540 we know that  $x = 2^a3^b5^c$  and  $y = 2^e3^f5^g$ . The gcd is the minimum power of common prime factors, similarly the lcm is the maximum power of common prime factors. Therefore, the list of all possible pairs of integers is:

$$\begin{aligned} x &= 2^13^25^0, y = 2^23^35^1 \\ x &= 2^13^35^0, y = 2^23^25^1 \\ x &= 2^23^25^0, y = 2^13^35^1 \\ x &= 2^23^35^0, y = 2^13^25^1 \end{aligned}$$

6. Suppose that  $a \in \mathbb{Z}$  is a perfect square divisible by at least two distinct primes. Show that  $a$  has at least seven distinct factors. 5/10

Since  $a$  is a perfect square it can be represented by the form  $a = b^2$ , and since  $a$  has at *least* 2 prime factors we can say that  $b = p_1^\alpha p_2^\beta$ . It follows that  $a = p_1^{2\alpha} p_2^{2\beta}$ . Therefore  $a$  has factors  $1, p_1, p_2, p_1^2, p_2^2, p_1 p_2, a$ .

7. Show that if  $a, b \in \mathbb{Z}^+$  with  $a^3 | b^2$  then  $a | b$ . 10/10

Let  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$  and  $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$ . Since  $a^3 | b^2$  we know that,

$$p_1^{3\alpha_1} p_2^{3\alpha_2} \cdots p_n^{3\alpha_n} \mid p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_n^{2\beta_n}$$

Therefore,  $3\alpha_n \leq 2\beta_n$ . Now to show  $a | b$  we need to show that  $\alpha \leq \beta$ .

$$3\alpha \leq 2\beta \implies \alpha \leq \frac{2\beta}{3} \leq \beta$$

Thus, if  $a^3 | b^2$  then  $a | b$ .

8. For which positive integers  $m$  is each of the following statements true:

6/10

(a)  $34 \equiv 10 \pmod{m}$

$$m = 12, 24$$

(b)  $1000 \equiv 1 \pmod{m}$

$$m = 3, 9, 27, 37, 111, 333, 999$$

(c)  $100 \equiv 0 \pmod{m}$

$$m = 1, 2, 4, 5, 10, 20, 25, 50, 100$$

### 1.3 Congruences

/100

1. Calculate the least positive residues modulo 47 of each of the following with justification:

(a)  $2^{543}$

Using binary expansion we see that  $2^1 \equiv 2 \pmod{47}$ ,  $2^2 \equiv 4 \pmod{47}$ ,  $2^4 \equiv 16 \pmod{47}$ ,  $2^8 \equiv 21 \pmod{47}$ ,  $2^{16} \equiv 18 \pmod{47}$ ,  $2^{32} \equiv 42 \pmod{47}$ ,  $2^{64} \equiv 25 \pmod{47}$ ,  $2^{128} \equiv 14 \pmod{47}$ ,  $2^{256} \equiv 8 \pmod{47}$ , and  $2^{512} \equiv 17 \pmod{47}$ .

Then  $543 = 512 + 16 + 8 + 4 + 2 + 1$  so,

$$\begin{aligned} 2^{543} &= 2^{512} 2^{16} 2^8 2^4 2^2 2^1 \equiv \\ &\equiv 17 \cdot 18 \cdot 21 \cdot 16 \cdot 4 \cdot 2 \pmod{47} \\ &\equiv 822528 \pmod{47} \\ &\equiv 28 \pmod{47} \end{aligned}$$

So 28 is the least non-negative residue.

(b)  $32^{932}$

Using binary expansion we see that  $32^1 \equiv 32 \pmod{47}$ ,  $32^2 \equiv 37 \pmod{47}$ ,  $32^4 \equiv 6 \pmod{47}$ ,  $32^8 \equiv 47 \pmod{47}$ ,  $32^{16} \equiv 27 \pmod{47}$ ,  $32^{32} \equiv 24 \pmod{47}$ ,  $32^{64} \equiv 12 \pmod{47}$ ,  $32^{128} \equiv 3 \pmod{47}$ ,  $32^{256} \equiv 9$ , and  $32^{512} \equiv 34$ . Then  $932 = 512 + 256 + 128 + 32 + 4$  so,

$$\begin{aligned} 32^{932} &= 32^{512} 32^{256} 32^{128} 32^{32} 32^4 \equiv \\ &\equiv 34 \cdot 9 \cdot 3 \cdot 24 \cdot 6 \pmod{47} \\ &\equiv 132192 \pmod{47} \\ &\equiv 28 \pmod{47} \end{aligned}$$

So 28 is the least non-negative residue.

(c)  $46^{327349287323}$

Since  $46 \equiv -1 \pmod{47}$  we know  $46^{327349287323} \equiv (-1)^{327349287323}$ .  
 We also know  $2 \nmid 327349287323$  so  $(-1)^{327349287323} \equiv (-1)^1 \equiv -1 \equiv 46 \pmod{47}$ . So 46 is the least non-negative residue.

2. Exhibit a complete set of residues mod 17 composed entirely of multiples of 3.

Let  $S = \{0, 1, 2, \dots, 16\}$  be the set of residues mod 17. Because  $\gcd(3, 17) = 1$  the set consisting of only multiples of 3 would be,

$$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42, 45, 48\}$$

3. Show that if  $a, b, m \in \mathbb{Z}$  with  $m > 0$  and if  $a \equiv b \pmod{m}$  then  $\gcd(a, m) = \gcd(b, m)$ .

If  $a \equiv b \pmod{m}$  then  $\exists x \in \mathbb{Z}$  such that  $a = b + xm$ . So  $\gcd(a, m) = \gcd(b + xm, m) = \gcd(b, m)$ .

4. Suppose  $p$  is prime and  $x \in \mathbb{Z}$  satisfies  $x^2 \equiv x \pmod{p}$ . Prove that  $x \equiv 0 \pmod{p}$  or  $x \equiv 1 \pmod{p}$ . Show with a counterexample that this fails if  $p$  is not prime.

Because  $x^2 \equiv x \pmod{p}$  we know that  $x^2 - x \equiv 0 \pmod{p}$ , which is the same as  $x(x - 1) \equiv 0 \pmod{p}$ . This implies that either  $p \mid x$ ,  $p \mid (x - 1)$ , or both.

$$p \mid x \implies x \equiv 0 \pmod{p}$$

$$p \mid (x - 1) \implies x \equiv 1 \pmod{p}$$

If  $p$  is not prime, say  $p = 6$  we see,

$$3^2 \equiv 3 \pmod{6}$$

Where  $3 \not\equiv 0 \pmod{6}$  and  $3 \not\equiv 1 \pmod{6}$ . So  $p$  must be prime for the statement to hold true.

5. Show that if  $n$  is an odd positive integer or if  $n$  is a positive integer divisible by 4 that:

$$1^3 + 2^3 + \dots + (n - 1)^3 \equiv 0 \pmod{n}$$

There are two cases to look at, when  $n$  is an odd positive integer and when  $n$  is divisible by 4.

- If  $n$  is an odd positive integer then  $n - 1$  is even so we have an even amount of numbers. Consider the set  $S = \{1^3, 2^3, \dots, (n - 1)^3\}$ . Then consider two subsets of  $S$ , both with  $(n - 1)/2$  elements  $S_1$  and  $S_2$ , where

$$\sum S = \sum S_1 + \sum S_2 = 1^3 + 2^3 + \dots + (n - 1)^3$$

The set  $S_1 = \{1^3, 2^3, 3^3, \dots\}$  and the set  $S_2 = \{\dots, (n-3)^3, (n-2)^3, (n-1)^3\}$ . Because we know that  $a-b \equiv -b \pmod{a}$  we also know that  $(a-b)^3 \equiv (-b)^3 \pmod{a}$ . So we can say that for all elements in  $S_2 \pmod{n}$ ,  $S_2 = \{\dots, (-3)^3, (-2)^3, (-1)^n\}$ . Now if we look at  $\sum S_1 + \sum S_2 \pmod{n}$  we see that the first element of  $S_1$  is cancelled out by the last element of  $S_2$  and so forth until there are no elements left. Thus,  $1^3 + 2^3 + \dots + (n-1)^3 \equiv 0 \pmod{n}$ .

- If  $n$  is divisible by 4 then  $n-1$  is odd so we have an odd amount of numbers. Consider the set  $S = \{1^3, 2^3, \dots, (n-1)^3\}$ . Then consider two subsets of  $S$ , both with  $(n-1)/2 - 1$  elements  $S_1$  and  $S_2$ , where

$$\sum S = \sum S_1 + \left(\frac{n}{2}\right)^3 + \sum S_2 = 1^3 + 2^3 + \dots + (n-1)^3$$

The set  $S_1 = \{1^3, 2^3, 3^3, \dots\}$  and the set  $S_2 = \{\dots, (n-3)^3, (n-2)^3, (n-1)^3\}$ . Because we know that  $a-b \equiv -b \pmod{a}$  we also know that  $(a-b)^3 \equiv (-b)^3 \pmod{a}$ . So we can say that for all elements in  $S_2 \pmod{n}$ ,  $S_2 = \{\dots, (-3)^3, (-2)^3, (-1)^n\}$ . Now if we look at  $\sum S \pmod{n}$ , like in the case above we can see that sets  $S_1$  and  $S_2$  will cancel one another out. This leaves us with

$$1^3 + 2^3 + \dots + (n-1)^3 \equiv \left(\frac{n}{2}\right)^3 \pmod{n}$$

Because we know that  $4 \mid n$  we know that  $n = 4x$  for some  $x \in \mathbb{Z}$ . It follows that,

$$\left(\frac{n}{2}\right)^3 = \frac{n^3}{8} = \frac{64x^3}{8} = 8x^3 = (2x^2)n$$

So

$$\left(\frac{n^3}{2}\right)^3 \equiv (2x^2)n \equiv 0 \pmod{n}$$

Thus,  $1^3 + 2^3 + \dots + (n-1)^3 \equiv 0 \pmod{n}$ .

6. Find all solutions (mod the given value) to each of the following.

- (a)  $10x \equiv 25 \pmod{75}$

Because the  $\gcd(10, 75) = 5$  and  $5 \mid 25$  we know that solutions exist. Let  $x_0 \equiv 10 \pmod{75}$ , so all solutions are then

$$x \equiv 10 + k \cdot \frac{75}{\gcd(10, 75)} \pmod{75}, \text{ for } k = 0, 1, 2, 3, 4$$

$$x \equiv 10 + 15k \pmod{75}, \text{ for } k = 0, 1, 2, 3, 4$$

Therefore,  $x \equiv 10, 25, 40, 55, 70$ .

(b)  $9x \equiv 8 \pmod{12}$

Because the  $\gcd(9, 12) = 3$  and  $3 \nmid 8$  so there are no solutions.

7. Solve each of the following linear congruences using inverses.

(a)  $3x \equiv 5 \pmod{17}$

Since 6 is the inverse of 3 mod 17 we get,  $6 \cdot 3x \equiv 6 \cdot 5 \pmod{17}$  which implies

$$x \equiv 30 \pmod{17} \equiv 13 \pmod{17}$$

Therefore,  $x \equiv 13$ .

(b)  $10x \equiv 3 \pmod{11}$

Since 10 is the inverse of 10 mod 11 we get,  $10 \cdot 10x \equiv 10 \cdot 3 \pmod{11}$  which implies

$$x \equiv 30 \pmod{11} \equiv 8 \pmod{11}$$

Therefore,  $x \equiv 8$ .

8. What could the prime factorization of  $m$  look like so that  $6x \equiv 10 \pmod{m}$  has at least one solution? Explain.

In order for  $ax \equiv b \pmod{m}$  to have a solution(s),  $\gcd(a, m) \mid b$ . So in the context of this problem we have that  $\gcd(6, m) \mid 10$ . We are looking for an  $m$  such that  $\gcd(6, m) = 2$ . One possible  $m$  could be  $m = 2^1$ .

9. Use the Chinese Remainder Theorem to solve:

A troop of monkeys has a store of bananas. When they arrange them into 7 piles, none remain. When they arrange them into 10 piles there are 3 left over. When they arrange them into 11 piles there are 2 left over. What is the smallest positive number of bananas they can have? What is the second smallest positive number?

Let  $x$  be the number of bananas, we have

$$x \equiv 0 \pmod{7}$$

$$x \equiv 3 \pmod{10}$$

$$x \equiv 2 \pmod{11}$$

Test to see if all  $m_i$  are pairwise coprime,  $\gcd(7, 10) = \gcd(7, 11) = \gcd(10, 11) = 1$ . This means that  $M = 770$ ,  $M_1 = 110$ ,  $M_2 = 77$ , and  $M_3 = 70$ .

Solve for  $y_1$ :

$$110y_1 \equiv 1 \pmod{7}$$

$$5y_1 \equiv 1 \pmod{7}$$

$$y_1 = 3$$

Solve for  $y_2$ :

$$77y_2 \equiv 1 \pmod{10}$$

$$7y_2 \equiv 1 \pmod{10}$$

$$y_2 = 3$$

Solve for  $y_3$ :

$$70y_3 \equiv 1 \pmod{11}$$

$$4y_3 \equiv 1 \pmod{11}$$

$$y_3 = 3$$

So we then get

$$x = (0)(110)(3) + (3)(77)(3) + (2)(70)(3) \equiv 1113 \pmod{770}$$

$$x \equiv 343 \pmod{770}$$

The smallest number of bananas they can have is 343 and the second smallest is 1113.

10. Solve the system of linear congruences:

$$2x + 1 \equiv 3 \pmod{10}$$

$$x + 2 \equiv 7 \pmod{9}$$

$$4x \equiv 1 \pmod{7}$$

Rewrite the system of linear congruences to be (properties of congruences):

$$2x \equiv 2 \pmod{10}$$

$$x \equiv 5 \pmod{9}$$

$$4x \equiv 1 \pmod{7}$$

Which then becomes

$$x \equiv 1 \pmod{5}$$

$$x \equiv 5 \pmod{9}$$

$$x \equiv 2 \pmod{7}$$

Then test to see if all  $m_i$  are pairwise coprime,  $\gcd(5, 9) = \gcd(5, 7) = \gcd(7, 9) = 1$ . This means that  $M = 315$ ,  $M_1 = 63$ ,  $M_2 = 35$ , and  $M_3 = 45$ .

Solve for  $y_1$ :

$$63y_1 \equiv 1 \pmod{5}$$

$$3y_1 \equiv 1 \pmod{5}$$

$$y_1 = 2$$

Solve for  $y_2$ :

$$35y_2 \equiv 1 \pmod{9}$$

$$8y_2 \equiv 1 \pmod{9}$$

$$y_2 = 8$$

Solve for  $y_3$ :

$$45y_3 \equiv 1 \pmod{7}$$

$$3y_3 \equiv 1 \pmod{7}$$

$$y_3 = 5$$

So we then get

$$x = (1)(63)(2) + (5)(35)(8) + (2)(45)(5) \equiv 1976 \pmod{315}$$

$$x \equiv 86 \pmod{315}$$