Solutions To HW4

Zixuan Chen
X313572
zixuanchen@ucsb.edu

July 2024

Solution To Question 1

PROVE:

$$\exists n_0 \in \mathbb{N}\, \forall n \in \mathbb{Z}^{\geq n_0}(n^3 \leq (n+2)!)$$

PROOF:

First, we need to prove the **Base Case**:the inequality holds when $n = n_0$.

Here, we choose $n_0 = 1$ as the witness.(Actually we can let n_0 be any *non-negative integer.*)

Now we need to prove: $n_0^3 \leq (n_0 + 2)!$

$$n_0^3 \leq (n_0 + 2)! \Longrightarrow 1^3 \leq 3! \Longrightarrow 1 \leq 6$$

We have proved the **Base Case**.

INDUCTIVE STEPS:

Assume that for some $n = k \geq 1$, we have $k^3 \leq (k+2)!$, we need to show that:

$$(k+1)^3 \leq ((k+1)+2)!$$

We can rewrite it as:

$$(k+1)(k+1)(k+1) \leq (k+3)(k+2)(k+1)k!$$

From definition, we know that $\forall k \in \mathbb{Z}^+\, k! \geq 1$ Therefore, we only need to show that:

$$(k+1)(k+1)(k+1) \leq (k+3)(k+2)(k+1)$$

Divide both side by $(k+1)$ gives:

$$(k+1)(k+1) \leq (k+3)(k+2)$$

Expand both sides:

$$k^2 + 2k + 1 \leq k^2 + 5k + 6$$

Thus we have the inequality we need to prove:

$$3k + 5 \geq 0$$

As $k \in \mathbb{Z}^+$, the inequality holds true.

Actually, we can see that we don't need the inductive hypothesis. The justification (in inductive steps) works for every non-negative integer. So after I wrote this, I found that this was actually a **Direct Proof**: choose a witness n_0 and verify the statement.

Solution To Question 2

Consider the functions $f_a : \mathbb{N} \to \mathbb{N}$ and $f_b : \mathbb{N} \to \mathbb{N}$ defined recursively by

$$f_a(0) = 0 \quad \text{and for each } n \in \mathbb{N}, \quad f_a(n+1) = f_a(n) + 2n + 1$$

$$f_b(0) = 0 \quad \text{and for each } n \in \mathbb{N}, \quad f_b(n+1) = 2f_b(n)$$

Determine which of these functions, if any, equals 2^n and which of these functions, if any, equals n^2.

Function f_a

First, let's explore f_a by computing the first few values:

$$\begin{aligned}
f_a(1) &= f_a(0) + 2(0) + 1 = 0 + 1 = 1 \\
f_a(2) &= f_a(1) + 2(1) + 1 = 1 + 2 + 1 = 4 \\
f_a(3) &= f_a(2) + 2(2) + 1 = 4 + 4 + 1 = 9
\end{aligned}$$

Notice a pattern: $f_a(n) = n^2$.

We can use mathematical induction to prove this.

Base Case: $n = 0$

$$f_a(0) = 0^2 = 0$$

Inductive Step: Assume $f_a(k) = k^2$. We need to show $f_a(k+1) = (k+1)^2$.

Using the recursive definition:

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

By the inductive hypothesis:

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

Thus, by induction, $f_a(n) = n^2$.

Function f_b

$$\begin{aligned}
f_b(0) &= 0 \\
f_b(1) &= 2f_b(0) = 2 \cdot 0 = 0
\end{aligned}$$

If $f_b(n) = 2^n$, then $f_b(1)$ should be 2.
If $f_b(n) = n^2$, then $f_b(1)$ should be 1.
Clearly, $f_b(n) = 0$ for all $n \in \mathbb{N}$. This function does not match 2^n or n^2.

Solution To Question 3

Prove that any amount of postage worth 24 cents or more can be made from 7-cent or 5-cent stamps.

PROOF:

First, we define $S(j)$ as the strategy to make a postage worth j cents.

Base Case: First we need to prove that 24 cents can be made from 7 cents and 5 cents. We can take 2*7-cent stamps and 2*5-cent stamps since $2 \times 7 + 2 \times 5 = 24$.
25 cents: 5*5-cent stamps
26 cents: 3*7-cent stamps and 1*5-cent stamp
27 cents: 1*7-cent stamp and 4*5-cent stamps
28 cents: 4*7-cent stamps
Therefore, $S(i)$ exists for $i \in \{24, 25, 26, 27, 28\}$

Inductive Steps: Assume a postage worth $24, 25, ..., k(k \geq 28)$ cents can be made from m 7-cent stamps and n 5-cent stamps.

Therefore $S(24), S(25), ..., S(k)$ exist. And we want to prove that $S(k+1)$ exists. $S(k+1) = S(k-4+5)$.As $k \geq 28$, we know that $k - 4 \geq 24$. We have proved that $S(24)$ exists. So for any $k, S(k-4)$ exists.(Strong induction)

From definition, $S(k-4+5)$ is t he strategy to make a postage worth $k-4+5$ cents. As $S(k-4)$ exists, then we know that there exists m and n and we can make a postage worth $k-4$ cents with m*7-cent stamps and n*5-cent stamps. Then, to make a postage worth $k-4+5$ cents, we just need m*7-cent stamps and $(n+1)$*5-cent stamps. Therefore, $S(k+1)$ exists.

Solution To Question 4

Given: {22, 15, -35, 34, 72, 79, -111, -42},group them according to their congruence classes modulo 19.

$$22 \equiv 22 - 19 \equiv 3 \pmod{19}$$
$$15 \equiv 15 \pmod{19}$$
$$-35 \equiv -35 + 2 \cdot 19 \equiv -35 + 38 \equiv 3 \pmod{19}$$
$$34 \equiv 34 - 19 \equiv 15 \pmod{19}$$
$$72 \equiv 72 - 3 \cdot 19 \equiv 72 - 57 \equiv 15 \pmod{19}$$
$$79 \equiv 79 - 4 \cdot 19 \equiv 79 - 76 \equiv 3 \pmod{19}$$
$$-111 \equiv -111 + 6 \cdot 19 \equiv -111 + 114 \equiv 3 \pmod{19}$$
$$-42 \equiv -42 + 3 \cdot 19 \equiv -42 + 57 \equiv 15 \pmod{19}$$

Grouping According to Congruence Classes

- **Congruence class 3 mod 19**: {22, -35, 79, -111}
- **Congruence class 15 mod 19**: {15, 34, 72, -42}

Solution To Question 5

Prove by contradiction that $a^2 = b^2 + 1$ has no solutions a, b in the positive integers.

Proof by Contradiction

1. **Assumption**:
   Suppose there exist positive integers a and b such that
   $$a^2 = b^2 + 1$$

2. **Rearranging the equation**:
   $$a^2 - b^2 = 1$$

3. **Factoring**:
   $$(a - b)(a + b) = 1$$

4. **Analyzing the factors**:
   The product of two integers is 1. The only pairs of positive integers that multiply to 1 are (1, 1). Therefore, we have:
   $$a - b = 1 \quad \text{and} \quad a + b = 1$$

5. **Solving the system of equations**:
   Adding these two equations:
   $$(a - b) + (a + b) = 1 + 1$$
   $$2a = 2$$
   $$a = 1$$
   Substituting $a = 1$ into $a + b = 1$:
   $$1 + b = 1$$
   $$b = 0$$

6. **Contradiction**:
   We assumed a and b are positive integers. However, this leads us to $b = 0$, which contradicts the assumption that b is a positive integer.

Solution To Question 6

(a)The set S consists of all strings (including the empty string) that have an even number of 1's but may have an even or odd number of zeros.

Base Case:

- The empty string ε belongs to S.

$$\varepsilon \in S$$

Recursive Step:

- If $x \in S$, then both $0x$ and $x0$ are in S. This ensures that adding a zero does not affect the even number of 1's.

$$\text{If } x \in S, \text{ then } 0x \in S \text{ and } x0 \in S$$

- If $x \in S$, then both $1x1$ and $x11$ are in S. This ensures that adding two 1's (an even number) maintains the even number of 1's.

$$\text{If } x \in S, \text{ then } 1x1 \in S \text{ and } x11 \in S$$

(b) The set S consists of all strings (including the empty string) that have the same number of 0's and 1's.

Base Case:

- The empty string ε belongs to T.

$$\varepsilon \in T$$

Recursive Step:

- If $x \in T$, then $0x1$ and $1x0$ are in T. This ensures that for every 0 added, a corresponding 1 is added, and vice versa.

$$\text{If } x \in T, \text{ then } 0x1 \in T \text{ and } 1x0 \in T$$

- Additionally, we can ensure balance by allowing any string in T to be expanded symmetrically:

$$\text{If } x \in T, \text{ then } 0x1 \in T, 1x0 \in T, 10x \in T, \text{ and } 01x \in T$$

$$\text{If } a, b \in T, \text{ then } ab \in T, ba \in T$$

The last rule is needed because without this it's impossible to construct string like 1111 0000 0010 0111

Solution To Question 7

We want to prove that for all $s \in S$ and $t \in S$, $rnalen(st) = rnalen(s) + rnalen(t)$ using the recursive definition of $rnalen$.

Basis Step

The base cases for the recursive definition are the individual RNA bases A, C, G, U. For any single base $b \in B$, we have:

$$\text{rnalen}(b) = 1$$

We need to check that $\text{rnalen}(st) = \text{rnalen}(s) + \text{rnalen}(t)$ holds when $t \in B$. For any base $t \in B$:

$$\text{rnalen}(st) = 1 + \text{rnalen}(s)$$

and

$$\text{rnalen}(s) + \text{rnalen}(t) = \text{rnalen}(s) + 1$$

Therefore,

$$\text{rnalen}(st) = \text{rnalen}(s) + \text{rnalen}(t) = \text{rnalen}(s) + 1$$

Inductive Step

Assume the inductive hypothesis: for all $s \in S$,

$$\text{rnalen}(st) = \text{rnalen}(s) + \text{rnalen}(t)$$

We will prove that for all $s \in S$ and any base $b \in B$,

$$\text{rnalen}(stb) = \text{rnalen}(s) + \text{rnalen}(tb)$$

Let $s \in S$ be arbitrary. Then,

$$\text{rnalen}(stb) = 1 + \text{rnalen}(st)$$

(by the recursive step).

Using the inductive hypothesis, we have:

$$\text{rnalen}(stb) = 1 + \text{rnalen}(s) + \text{rnalen}(t)$$

By the recursive step,

$$\text{rnalen}(tb) = 1 + \text{rnalen}(t)$$

Thus,

$$\text{rnalen}(stb) = \text{rnalen}(s) + \text{rnalen}(tb)$$

Therefore, our inductive hypothesis is proven true.

Solution To Question 8

We want to prove that for any positive integers x and y, with $y \geq x$ and $x \neq 0$:

$$\gcd(y, x) = \gcd(y - x, x)$$

PROOF:

Let $d = \gcd(y, x)$. By definition, d is the largest positive integer that divides both y and x. Thus, we have:

$$d \mid y \quad \text{and} \quad d \mid x$$

We need to show that d also divides $y - x$. Since $d \mid y$ and $d \mid x$, there exist integers k and m such that:

$$y = kd \quad \text{and} \quad x = md$$

Now consider $y - x$:

$$y - x = kd - md = (k - m)d$$

Since d divides $(k - m)d$, it follows that $d \mid (y - x)$. Thus, d is a common divisor of both $y - x$ and x.

Next, let $d' = \gcd(y - x, x)$. By definition, d' is the largest positive integer that divides both $y - x$ and x. We need to show that d' also divides y. Since $d' \mid (y - x)$ and $d' \mid x$, there exist integers n and p such that:

$$y - x = nd' \quad \text{and} \quad x = pd'$$

Adding these two equations, we get:

$$y = (y - x) + x = nd' + pd' = (n + p)d'$$

Since d' divides $(n + p)d'$, it follows that $d' \mid y$. Thus, d' is a common divisor of both y and x.

As d is the largest positive integer that divides y and x, and d' also divides y and x. We know that

$$d' \leq d$$

As $d'$is the largest positive integer that divides $y - x$ and x, and d also divides $y - x$ and x. We know that

$$d' \geq d$$

Thus,

$$(d' \leq d) \wedge (d' \geq d) \implies (d' = d)$$

Therefore,

$$\gcd(y, x) = \gcd(y - x, x)$$

Solution To Question 9

We want to prove that for any positive integers x and y with $y \geq x$,

$$\gcd(y, x) = \gcd(x, y \, mod \, x).$$

PROOF:

We will use strong induction on y.

Base Case

Let $y = x$. Then:

$$y \mod x = x \mod x = 0$$

So,

$$\gcd(y, x) = \gcd(x, 0) = x.$$

By definition,

$$\gcd(x, 0) = x.$$

Inductive Step

Assume the statement is true for all y such that $y \leq k$ for some $k \geq x$. We need to prove it for $y = k + 1$.

Consider $y = k + 1$. We need to show:

$$\gcd(k + 1, x) = \gcd(x, (k + 1) \mod x).$$

By the division algorithm, we can write:

$$k + 1 = qx + r,$$

where $0 \leq r < x$ and $r = (k + 1) \mod x$.

Thus, we need to prove:

$$\gcd(k + 1, x) = \gcd(x, r).$$

Using the gcd lemma, we have:

$$\gcd(k + 1, x) = \gcd(k + 1 - x, x).$$

Since $k + 1 - x \leq k$, by the inductive hypothesis, we have:

$$\gcd(k + 1 - x, x) = \gcd(x, (k + 1 - x) \mod x).$$

But,

$$(k + 1 - x) \mod x = (k + 1) \mod x = r.$$

Therefore,

$$\gcd(k + 1, x) = \gcd(x, r) \iff \gcd(k + 1, x) = \gcd(x, (k + 1) \mod x)$$

Solution To Question 10

We want to prove that for positive integers a, b, and c, if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Proof

Since $\gcd(a, b) = 1$, there exist integers x and y such that

$$ax + by = 1.$$

Given that $a \mid bc$, there exists an integer k such that

$$bc = ak.$$

Now, consider the product $c \cdot (ax + by)$:

$$c(ax + by) = c \cdot 1 = c.$$

Expanding the left-hand side, we get:

$$cax + cby.$$

Since $a \mid a$, it follows that $a \mid cax$. Also, since $a \mid bc$ and $bc = ak$, it follows that $a \mid cby$.

Therefore, a divides both cax and cby. Thus, a divides their sum:

$$a \mid (cax + cby).$$

But, since

$$cax + cby = c,$$

it follows that

$$a \mid c.$$

Hence, we have shown that if $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

Solution To Question 11

Theorem: Every positive integer is a sum of one or more distinct powers of 2.

PROOF: We will use strong induction to prove this theorem.

Base Case:

For $n = 1$:

$$1 = 2^0$$

This is clearly a sum of distinct powers of 2.

Inductive Step:

Assume that for every positive integer k such that $1 \leq k \leq n$, k can be written as a sum of distinct powers of 2. We need to prove that $n + 1$ can also be written as a sum of distinct powers of 2.

Case 1: $n + 1$ is a power of 2:

If $n + 1 = 2^m$ for some integer m, then $n + 1$ is already a sum of a single power of 2.

Case 2: $n + 1$ is not a power of 2:

If $n + 1$ is not a power of 2, we can express $n + 1$ as $2^m + k$, where 2^m is the largest power of 2 less than $n + 1$ and k is the remainder (i.e., $k < 2^m$). By the inductive hypothesis, k can be written as a sum of distinct powers of 2.

Thus, $n + 1 = 2^m + k$, where k is a sum of distinct powers of 2. Therefore, $n + 1$ is also a sum of distinct powers of 2.

By strong induction, every positive integer can be written as a sum of distinct powers of 2.

Algorithm: Calculating base 2 expansion recursively

```
procedure base2recursive(n: a positive integer)

if (n = 0)
     a_0 := 0
else if (n = 1)
     a_0 := 1
else
     (a_{k-1}, ..., a_1) := base2recursive(n div 2)
     a_0 := n mod 2


return (a_{k-1}, ..., a_0){(a_{k-1} ... a_0)_b is the base 2 expansion of n}
```

Solution To Question 12

Theorem: Prove that $n \in \mathbb{N}$ is divisible by 3 if and only if the alternating sum of the bits of n in binary representation is divisible by 3. The alternating sum of any sequence $a_0, a_1, ..., a_m$ is $\sum_{i=0}^{m}(-1)^i a_i$.

PROOF: Noticing the 'iff', I'll prove this statement from 2 aspects:

- **Theorem1:** if the alternating sum(base2) of $n \in \mathbb{Z}$ is divisible by 3, then n is divisible by 3.
- **Theorem2:** if $n \in \mathbb{Z}$ is divisible by 3, then its alternating sum(base2) is divisible by 3.

Theorem1: If 3 divides $\sum_{i=0}^{m}(-1)^i a_i$, then 3 divides $\sum_{i=0}^{m} 2^i a_i$(The base-2 expansion of n).

Proof:

- **Given:** $\sum_{i=0}^{m}(-1)^i a_i \equiv 0 \pmod 3$.
- **Objective:** Show $\sum_{i=0}^{m} 2^i a_i \equiv 0 \pmod 3$.
- **Step-by-Step Approach:**
  - **Step 1:** Consider the behavior of powers of 2 modulo 3:
    * $2^0 \equiv 1 \pmod 3$
    * $2^1 \equiv 2 \pmod 3$
    * $2^2 \equiv 4 \equiv 1 \pmod 3$
    * $2^3 \equiv 8 \equiv 2 \pmod 3$
    * Generally, $2^i \mod 3$ alternates between 1 and 2 for even and odd i, respectively.
  - **Step 2:** Rewrite $\sum_{i=0}^{m} 2^i a_i$ using modular properties:

$$\sum_{i=0}^{m} 2^i a_i \equiv \sum_{\substack{i=0 \\ i \text{ even}}}^{m} a_i + \sum_{\substack{i=0 \\ i \text{ odd}}}^{m} 2a_i \pmod 3$$

  - **Step 3:** Combine the alternating sum components:

$$\sum_{i=0}^{m} 2^i a_i \equiv \sum_{\substack{i=0 \\ i \text{ even}}}^{m} a_i + 2\sum_{\substack{i=0 \\ i \text{ odd}}}^{m} a_i \pmod 3$$

  - **Step 4:** Relate this to the given alternating sum:
    * The given alternating sum is $S = \sum_{i=0}^{m}(-1)^i a_i$
    * This can be rewritten as:

$$S = \sum_{\substack{i=0 \\ i \text{ even}}}^{m} a_i - \sum_{\substack{i=0 \\ i \text{ odd}}}^{m} a_i \equiv 0 \pmod 3$$

  - **Step 5:** Transform the even and odd sums:

* Let $A = \sum_{\substack{i=0 \\ i \text{ even}}}^{m} a_i$
* Let $B = \sum_{\substack{i=0 \\ i \text{ odd}}}^{m} a_i$
* Hence,

$$A - B \equiv 0 \pmod 3 \quad \Rightarrow \quad A \equiv B \pmod 3$$

– **Step 6:** Substitute back:

$$\sum_{i=0}^{m} 2^i a_i \equiv A + 2B \equiv A + 2A \equiv 3A \equiv 0 \pmod 3$$

- **Conclusion:** Thus, $\sum_{i=0}^{m} 2^i a_i \equiv 0 \pmod 3$. This completes the proof.

Theorem2: If 3 divides $\sum_{i=0}^{m} 2^i a_i$, then 3 divides $\sum_{i=0}^{m}(-1)^i a_i$.

Proof:

Actually we don't have much to prove because we have already done most of the stuff in Theorem1.

Proving Theorem2 is similar to proving Theorem1.

Now we only need to justify:

$$\sum_{i=0}^{m}(-1)^i a_i \equiv \sum_{i=0}^{m} 2^i a_i \pmod 3$$

We can rewrite it in:

$$A - B \equiv A + 2B \pmod 3$$

As

$$A - B = A + 2B - 3B$$

Therefore

$$(A - B) \pmod 3 = ((A + 2B) \pmod 3 - 3B \pmod 3) \pmod 3$$

$$3B \pmod 3 = 0$$

Therefore,

$$(A - B) \equiv (A + 2B) \pmod 3$$