CSC165H1: Problem Set 3

Due November 15 before 10pm

Question 1

(a)

P(n):

$\forall m \in \mathbb{Z}^+, \forall a, b \in S, \forall n \in \mathbb{N}^+ \left(\forall k \geq n, a_k \equiv b_k (\text{mod } m)\right) \Longrightarrow (\prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k \text{ (mod m)})$

Proof: (By math induction)

Let $a, b: \mathbb{N} \rightarrow \mathbb{Z}$

Denote $a(n) = a_n, b(n) = b_n$

and a, b is identified with the sequence $a_0, a_1, a_2 \ldots, b_0, b_1, b_2 \ldots$

Let $S = \{f \mid f: \mathbb{N} \rightarrow \mathbb{Z}\}, a, b \in S$

Let $n \in \mathbb{N}$

Let $k \in \mathbb{N}, k < n$

Base Case: n = 1

Then $k \in \{0, 1\}$

Assume $a_0 \equiv b_0 (\text{mod } m)$

$a_1 \equiv b_1 (\text{mod } m)$

Namely $m \mid a_0 - b_0$

$m \mid a_1 - b_1$

Then $m \mid a_1(a_0 - b_0) + b_0(a_1 - b_1)$

$m \mid a_0a_1 - a_1b_0 + a_1b_0 - b_0b_1$

$m \mid a_0a_1 - b_0b_1$

Namely $a_0a_1 \equiv b_0b_1 (\text{mod } m)$

So the statement is True when n = 1

Induction step: Assume the statement is True when $n = i, i \in \mathbb{R}^{\geq 0}$

$\left(\forall k \geq i, a_k \equiv b_k (\text{mod } m)\right) \Longrightarrow (\prod_{k=0}^{k=i} a_k \equiv \prod_{k=0}^{k=i} b_k \text{ (mod m)})$

Namely

$\left(\forall k \geq i, a_k \equiv b_k (\text{mod } m)\right) \Longrightarrow (m \mid \prod_{k=0}^{k=i} a_k - \prod_{k=0}^{k=i} b_k)$

By 2.18 form text book

$\left(\forall k \geq i, a_k \equiv b_k (\text{mod } m)\right) \Longrightarrow (\prod_{k=1}^{k=i} a_k \equiv \prod_{k=1}^{k=i} b_k \text{ (mod m)})$

$\left(\forall k \geq i+1, a_k \equiv b_k (\text{mod } m)\right) \Longrightarrow (\prod_{k=1}^{k=i+1} a_k \equiv \prod_{k=1}^{k=i+1} b_k \text{ (mod m)})$

Namely

$\left(\forall k \geq i, a_k \equiv b_k (\text{mod } m)\right) \Longrightarrow (m \mid \prod_{k=1}^{k=i} a_k - \prod_{k=1}^{k=i} b_k)$

$\left(\forall k \geq i+1, a_k \equiv b_k (\text{mod } m)\right) \Longrightarrow (m \mid \prod_{k=1}^{k=i+1} a_k - \prod_{k=1}^{k=i+1} b_k)$

When n = i + 1

$m \mid a_{k+1}(\prod_{k=0}^{k=i} a_k - \prod_{k=0}^{k=i} b_k) + b_0(\prod_{k=1}^{k=i+1} a_k - \prod_{k=1}^{k=i+1} b_k)$

$m \mid [\prod_{k=0}^{k=i+1} a_k - \prod_{k=0}^{k=i+1} b_k] + [a_{k+1}b_0(\prod_{k=1}^{k=i} a_k - \prod_{k=1}^{k=i} b_k)]$

We know that $m \mid \prod_{k=1}^{k=i} a_k - \prod_{k=1}^{k=i} b_k$ (By assumption and 2.18)

Then $m \mid a_{k+1}b_0(\prod_{k=1}^{k=i} a_k - \prod_{k=1}^{k=i} b_k)$

Hence $m \mid \prod_{k=0}^{k=i+1} a_k - \prod_{k=0}^{k=i+1} b_k$

Namely $\prod_{k=0}^{k=i+1} a_k \equiv \prod_{k=0}^{k=i+1} b_k \text{ (mod m)}$ ■

(b)

P(n): $\forall \mathrm{d} \in \mathbb{N}, \mathrm{d} > 1, \forall \mathrm{m} \in \mathbb{N}, \forall \mathrm{b} \in \mathrm{S}, \mathrm{b_m} > 0, \forall n \in \mathbb{N}, (\forall \mathrm{i} \in \mathbb{N}, \mathrm{i} \leq \mathrm{n} \Rightarrow \gcd(\mathrm{d}, \mathrm{b_i}) = 1) \Rightarrow \mathrm{d} \nmid \prod_{i=0}^{i=n} \mathrm{b_i}$

Proof: (By math induction)

Let $\mathrm{n} \in \mathbb{N}$

Let $\mathrm{d} \in \mathbb{N}, \mathrm{d} > 1$

Base Case: n = 0

Assume $\forall \mathrm{i} \in \mathbb{N}, \mathrm{i} \leq \mathrm{n} \Rightarrow \gcd(\mathrm{d}, \mathrm{b_i}) = 1$

Namely $\gcd(\mathrm{d}, \mathrm{b_0}) = 1$

Then $\exists \mathrm{x_0}, \mathrm{y_0} \in \mathbb{Z}\ \mathrm{s.t.}\ \mathrm{x_0 d} + \mathrm{y_0 b_1} = 1$

$\mathrm{x_0 d} = 1 - \mathrm{y_0 b_0}$

$\mathrm{y_0 b_0} \equiv 1 (\bmod \mathrm{d})$

$\mathrm{y_0 b_0} \cdot \frac{1}{\mathrm{y_0}} \equiv 1 \cdot \frac{1}{\mathrm{y_0}} (\bmod \mathrm{d})$

$\mathrm{b_0} \equiv \frac{1}{\mathrm{y_0}} (\bmod \mathrm{d})$

Since $\frac{1}{\mathrm{y_0}} \neq 0$

$\mathrm{d} \nmid \mathrm{b_0}$

Induction step: Assume the statement is True when $\mathrm{n} = \mathrm{k}, \mathrm{k} \in \mathbb{N}$

Namely $(\forall \mathrm{i} \in \mathbb{N}, \mathrm{i} \leq \mathrm{k} \Rightarrow \gcd(\mathrm{d}, \mathrm{b_i}) = 1) \Rightarrow \mathrm{d} \nmid \prod_{i=0}^{i=k} \mathrm{b_i}$

When n = k + 1

Assume $\forall \mathrm{i} \in \mathbb{N}, \mathrm{i} \leq \mathrm{k} + 1 \Rightarrow \gcd(\mathrm{d}, \mathrm{b_i}) = 1$

WTS $\mathrm{d} \nmid \prod_{i=0}^{i=k+1} \mathrm{b_i}$

By 2(g) in Problem Set 2 know that

$\forall \mathrm{a}, \mathrm{b}, \mathrm{c} \in \mathbb{Z}, (\gcd(\mathrm{a}, \mathrm{b}) = 1 \wedge \mathrm{a} | \mathrm{bc}) \Rightarrow \mathrm{a} | \mathrm{c}$

By assumption we know that $\gcd(\mathrm{d}, \mathrm{b_{n+1}}) = 1$

If $\mathrm{d} \mid \prod_{i=0}^{i=k+1} \mathrm{b_i}$

Then $\mathrm{d} \mid \prod_{i=0}^{i=k} \mathrm{b_i}$, which is contradict to our assumption

Hence $\mathrm{d} \nmid \prod_{i=0}^{i=k+1} \mathrm{b_i}$

So far we have proved that P(n) is True ■

(c)

P(n): $\forall \mathrm{n} \in \mathbb{N}, \mathrm{n} > 1 \Rightarrow \sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$

Proof: (By math induction)

Let $\mathrm{n} \in \mathbb{N}$

Base Case: n = 2

$\sum_{j=n+1}^{j=2n} \frac{1}{j} = \frac{1}{3} + \frac{1}{4} = \frac{14}{24} > \frac{13}{24}$

So the statement is True when n = 2

Induction step: Assume the statement is True when $\mathrm{n} = \mathrm{i}, \mathrm{i} \in \mathbb{N}$

Namely $\sum_{j=i+1}^{j=2i} \frac{1}{j} > \frac{13}{24}$

When n = i + 1

$$\sum_{j=i+2}^{j=2i+2}\frac{1}{j}=\sum_{j=i+1}^{j=2i}\frac{1}{j}+\frac{1}{2i+1}+\frac{1}{2i+2}-\frac{1}{i+1}$$

$$=\sum_{j=i+1}^{j=2i}\frac{1}{j}+\frac{1}{2i+1}-\frac{1}{2i+2}$$

Since $i \in \mathbb{N}$ and $i \geq 2$

$2i+2>2i+1$

$\frac{1}{2i+1}>\frac{1}{2i+2}$

$\frac{1}{2i+1}-\frac{1}{2i+2}>0$

Since $\sum_{j=i+1}^{j=2i}\frac{1}{j}>\frac{13}{24}$

$\sum_{j=i+1}^{j=2i}\frac{1}{j}+\frac{1}{2i+1}-\frac{1}{2i+2}>\frac{13}{24}$

$\sum_{j=i+2}^{j=2i+2}\frac{1}{j}>\frac{13}{24}$

So far we have proved that P(n) is True ■

(d)

P(n): $\forall n \in \mathbb{N}, c_n \begin{cases} 0, \text{if } n=0 \\ c_{n-1}+3n^2-3n+1, \text{if } n>0 \end{cases} = n^3$

Proof: (By math induction)

Let $c: \mathbb{N} \to \mathbb{Z}$

Denote $c(n)=c_n$, and c is identified with the sequence c_0, c_1, c_2 ...

Let $S=\{f \mid f: \mathbb{N} \to \mathbb{Z}\}, c \in S$

Let $n \in \mathbb{N}$

Base Case: ① n = 0

$c_n=0=0^3=n^3$

② n = 1

$c_n=0+3-3+1=1^3=n^3$

So the statement is True when n = 0 and n = 1

Induction step: Assume the statement is True when $n=i, i \in \mathbb{N}$

Namely $c_i=c_{i-1}+3i^2-3i+1=i^3$

When n = i + 1

$$\begin{aligned} c_{i+1} &= c_i+3(i+1)^2-3(i+1)+1 \\ &= c_{i-1}+3i^2-3i+1+3(i+1)^2-3(i+1)+1 \\ &= i^3+3(i+1)^2-3(i+1)+1 \\ &= i^3+3i^2+3i+1 \\ &= (i+1)^3 \end{aligned}$$

So far we have proved that P(n) is True ■

Question 2

(a)

P(n): $\forall \mathrm{n}, \mathrm{k} \in \mathbb{N}, \mathrm{k} < n \Rightarrow \binom{\mathrm{n}}{\mathrm{k}} = \frac{\mathrm{n}!}{\mathrm{k}!(\mathrm{i}-\mathrm{k})!}$

Proof: (By math induction)

Let $\mathrm{n} \in \mathbb{N}$

Let $\mathrm{k} \in \mathbb{N}$

Let S be a set with |S| = n

We know that $\mathrm{k} \neq 0$ and $\mathrm{k} - \mathrm{n} \neq 0$ and $\mathrm{k} \leq \mathrm{n}$

If n = 0

Then k = n = 0, which is impossible

If n = 1

Then k = 0 or k = n = 1, which is impossible

Hence $\mathrm{n} \geq 2$

Base Case: n = 2 = |S|

Then k = 1

The number of subsets with length 1 of set S with length 2 is 2

And $\frac{2!}{1!(2-1)!} = 2$

So the statement is True when n = 2

Induction step: Assume the statement is True when $\mathrm{n} = \mathrm{i} = |\mathrm{S}|, \mathrm{i} \in \mathbb{N}$

Namely $\binom{\mathrm{i}}{\mathrm{k}} = \frac{\mathrm{i}!}{\mathrm{k}!(\mathrm{i}-\mathrm{k})!}$, $\binom{\mathrm{i}}{\mathrm{k}-1} = \frac{\mathrm{i}!}{(\mathrm{k}-1)!(\mathrm{i}-\mathrm{k}+1)!}$

When n = i + 1 = |S|

Let $\mathrm{c} \in \mathbb{N}$ be one element in set S

Split the subsets with length k of S with length i + 1 into two parts:

with c and without c

For the first part: its number is equivalent to $\binom{\mathrm{i}}{\mathrm{k}} = \frac{\mathrm{i}!}{\mathrm{k}!(\mathrm{i}-\mathrm{k})!}$

For the second part: its number is equivalent to $\binom{\mathrm{i}}{\mathrm{k}-1} = \frac{\mathrm{i}!}{(\mathrm{k}-1)!(\mathrm{i}-\mathrm{k}+1)!}$

Hence $\binom{\mathrm{i}+1}{\mathrm{k}} = \binom{\mathrm{i}}{\mathrm{k}} + \binom{\mathrm{i}}{\mathrm{k}-1}$

$$= \frac{\mathrm{i}!}{\mathrm{k}!(\mathrm{i}-\mathrm{k})!} + \frac{\mathrm{i}!}{(\mathrm{k}-1)!(\mathrm{i}-\mathrm{k}+1)!}$$

$$= \frac{\mathrm{i}!(\mathrm{i}-\mathrm{k}+1)}{\mathrm{k}!(\mathrm{i}-\mathrm{k})!(\mathrm{i}-\mathrm{k}+1)} + \frac{\mathrm{i}!\mathrm{k}}{(\mathrm{k}-1)!(\mathrm{i}-\mathrm{k}+1)!\mathrm{k}}$$

$$= \frac{(\mathrm{i}+1)!}{\mathrm{k}!(\mathrm{i}-\mathrm{k}+1)!}$$

So far we have proved that P(n) is True ■

(b)

$\mathrm{DTP}_2 = \{\{\{1\},\{2\}\},\{\{1,2\},\emptyset\}\}$

$\mathrm{DTP}_3 = \{\{\{1,2\},\{3\}\},\{\{1,3\},\{2\}\},\{\{2,3\},\{1\}\},\{\{1,2,3\},\emptyset\}\}$

(c)

$|\mathrm{DTP_n}| = \begin{cases} 1, n = 0 \\ 2^{n-1}, n \in \mathbb{N}^+ \end{cases}$

Proof: (By math induction)

Let $n \in \mathbb{N}$

Let $d \in \mathbb{N}, d > 1$

Base Case: When n = 0

$\mathrm{DTP_0} = \{\{\{\emptyset, \emptyset\}\}\}$

$|\mathrm{DTP_0}| = 1$, means the statement is True when n = 0

When n = 1

$\mathrm{DTP_0} = \{\{\{1\}, \emptyset\}\}$

$|\mathrm{DTP_1}| = 1$, means the statement is True when n = 1

Induction step: Assume the statement is True when $n = i, i \in \mathbb{N}^+$

Namely $|\mathrm{DTP_i}| = 2^{i-1}$

When n = i + 1

We can split $\mathrm{DTP_{i+1}}$ into two parts, $\mathrm{D_1}$and $\mathrm{D_2}$

For all elements in which have a form {A, B} in $\mathrm{D_1}$, $i \in A$

For all elements in which have a form {A, B} in $\mathrm{D_2}$, $i \in B$

Since $|\mathrm{D_1}| = |\mathrm{D_2}| = |\mathrm{DTP_i}| = 2^{i-1}$

$|\mathrm{DTP_{i+1}}| = |\mathrm{D_1}| + |\mathrm{D_2}| = 2 \cdot 2^{i-1} = 2^i$

So far we have proved that $|\mathrm{DTP_n}| = \begin{cases} 1, n = 0 \\ 2^{n-1}, n \in \mathbb{N}^+ \end{cases}$ ■

Question 3

(a)

Theorem 5.8:

$\forall f: \mathbb{N} \to \mathbb{R}^{\geq 0}, (\exists n_0 \in \mathbb{R}^+, n \geq n_0 \Rightarrow f(n) \geq 1) \Rightarrow ((\exists c_1, c_2, n_1 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_1 \Rightarrow$
$c_1 f(n) \leq \lfloor f(n) \rfloor \leq c_2 f(n)) \wedge (\exists c_3, c_4, n_2 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_2 \Rightarrow c_3 f(n) \leq \lceil f(n) \rceil \leq c_4 f(n))$

Proof: Let $f: \mathbb{N} \to \mathbb{R}^{\geq 0}$

Assume $\exists n_0 \in \mathbb{R}^+, n \geq n_0 \Rightarrow f(n) \geq 1$

①Take $c_1 = \frac{1}{2}, c_2 = 1, n_1 = n_0$

Then $f(n) \geq 1$

We know that $f(n) - 1 \leq \lfloor f(n) \rfloor$

Case1: $f(n) \geq 2$

Then $\lfloor f(n) \rfloor - c_1 f(n)$

$> f(n) - 1 - c_1 f(n)$

$= \frac{1}{2} \cdot f(n) - 1$

Since $f(n) \geq 2$

$\frac{1}{2} \cdot f(n) - 1 \geq 0$

Which means $c_1 f(n) \leq \lfloor f(n) \rfloor$

Case2: $1 \leq f(n) < 2$

Then $\lfloor f(n) \rfloor = 1$ and $c_1 f(n) = \frac{1}{2} \cdot f(n) \in \left[\frac{1}{2}, 1\right)$

Which means $c_1 f(n) \leq \lfloor f(n) \rfloor$

In all $c_1 f(n) \leq \lfloor f(n) \rfloor$

We know that $\lfloor f(n) \rfloor \leq f(n)$

Hence $\lfloor f(n) \rfloor \leq c_2 f(n) = 1 \cdot f(n) = f(n)$

②Take $c_3 = 1, c_4 = 2, n_2 = n_0$

Then $f(n) \geq 1$

We know that $f(n) \leq \lceil f(n) \rceil$

Hence $c_3 f(n) = 1 \cdot f(n) = f(n) \leq \lceil f(n) \rceil$

We know that $f(n) \geq 1, \lceil f(n) \rceil < f(n) + 1$, namely $\lceil f(n) \rceil < 2f(n)$

Hence $\lceil f(n) \rceil < c_4 f(n) = 2f(n)$ ■

(b)

WTS $\forall a, b \in \mathbb{R}^+, (b > a \wedge a > 1) \Longrightarrow (\forall c, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{N}, (n \geq n_0) \wedge (b^n > ca^n))$

Proof: Let $a, b \in \mathbb{R}^+$

Assume $b > a \wedge a > 1$

Let $c, n_0 \in \mathbb{R}^+$

Take $n = \max\{n_0, \log_{\frac{b}{a}}(c+1)\}$

Then $n \geq n_0$

And $(\frac{b}{a})^n = c + 1 > c$

$\frac{b^n}{a^n} > c$

Since $a^n > 0$

$b^n > ca^n$ ■

(c)

①First we prove that every two iterations of the loop reduces r0 by at least half:

Proof: Let $a, b \in \mathbb{N}$

To guarantee the first iteration, we need $b \neq 0$

To guarantee the second iteration, we need $b \nmid a$

Let $t_1, s_1 \in \mathbb{Z}$, by Quotient − Remainder Theorem we have $a = t_1 b + s_1, s_1 < b$

Since $b \nmid a, s_1 \neq 0$

Let $t_2, s_2 \in \mathbb{Z}$, by Quotient − Reaminder Theorem we have $b = t_2 s_1 + s_2, s_2 < s_1$

s_2 might = 0

In first iteration: quotient = t_1

r0 = b

r1 = s_1

In second iteration: quotient = t_2

r0 = s_1

r1 = s_2

Case 1: $b > \frac{a}{2}$

Then $t_1 = 1, s_1 = a - t_1 b$

Since $a - t_1 b < \frac{a}{2}$

$s_1 < \frac{a}{2}$

Case 2: $b < \frac{a}{2}$

Since $b > s_1$

$s_1 < \frac{a}{2}$

So far we have proved every two iterations of the loop reduces r0 by at least half ■

②We showed in ① that every two iterations of the loop reduces r0 by at least half.

So for any $k \in \mathbb{N}$, either the loop terminates with in 2k loops, or the value of r0 has decreased by at least a factor of 2^k

Since r0 is initialized to a, we know that $r0_k \leq \frac{a}{2^k}$

The loop terminates when $r0 \leq 1$, and this occurs when $n \leq 2^k$, i.e. $k \geq \lg a$

After adding the return step, the loop will run for at most $2\lceil \lg a \rceil + 1$ steps

Since each iteration takes constant time

The total run time is $O(\lg a)$