CSC165H1: Problem Set 3

Due November 15, 2017 before 10pm

1. (a)

WTS: $\forall m \in \mathbb{Z}, \forall a, b \in S,\ (m \neq 0) \Longrightarrow (\ \forall n \in \mathbb{N}^+, (\forall k \leq n, a_k \equiv b_k (mod\ m)) \Rightarrow \prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k\ (mod\ m))$

P(n): $(\forall k \leq n, a_k \equiv b_k (mod\ m)) \Rightarrow \prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k\ (mod\ m)$

Proof: We will prove this statement using induction on n.

Let $m \in \mathbb{Z}$, let $a, b \in S$, assume $m \neq 0$

Base case:

Let n=1.

We assume $\forall k \leq n, a_k \equiv b_k (mod\ m)$ that is $a_0 \equiv b_0 (mod\ m)$ and $a_1 \equiv b_1 (mod\ m)$, we want to prove that $\prod_{k=0}^{k=1} a_k \equiv \prod_{k=0}^{k=1} b_k\ (mod\ m)$ that is $a_0 \times a_1 \equiv b_0 \times b_1\ (mod\ m)$

Since $\forall a, b, c, d, n \in \mathbb{Z}$, with $n \neq 0$, if $a \equiv c\ (mod\ n)$ and $b \equiv d\ (mod\ n)$, then $ab \equiv cd\ (mod\ n)$ (course note 2.18(c))

And $a_0 \equiv b_0 (mod\ m)$ and $a_1 \equiv b_1 (mod\ m)$ (what we assumed before)

So $a_0 \times a_1 \equiv b_0 \times b_1\ (mod\ m)$

Hence $(\forall k \leq n, a_k \equiv b_k (mod\ m)) \Rightarrow \prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k\ (mod\ m)$

Induction step:

Let $n \in \mathbb{N}^+$ and assume that $(\forall k \leq n, a_k \equiv b_k (mod\ m)) \Rightarrow \prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k\ (mod\ m)$

We want to prove that $(\forall k \leq n+1, a_k \equiv b_k (mod\ m)) \Rightarrow \prod_{k=0}^{k=n+1} a_k \equiv \prod_{k=0}^{k=n+1} b_k\ (mod\ m)$

Assume that $(\forall k \leq n+1, a_k \equiv b_k (mod\ m))$ we want to prove that $\prod_{k=0}^{k=n+1} a_k \equiv \prod_{k=0}^{k=n+1} b_k\ (mod\ m)$

Since $\forall k \leq n+1, a_k \equiv b_k (mod\ m)$ and n<n+1 so $\forall k \leq n, a_k \equiv b_k (mod\ m)$, so $\prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k\ (mod\ m)$ (by induction hypothesis)

Since $\forall k \leq n+1, a_k \equiv b_k (mod\ m)$ so $a_{n+1} \equiv b_{n+1} (mod\ m)$

Since $\forall a, b, c, d, n \in \mathbb{Z}$, with $n \neq 0$, if $a \equiv c\ (mod\ n)$ and $b \equiv d\ (mod\ n)$, then $ab \equiv cd\ (mod\ n)$ (course note 2.18(c))

Hence $\prod_{k=0}^{k=n} a_k \times a_{n+1} \equiv \prod_{k=0}^{k=n} b_k \times b_{n+1} (mod\ m)$ that is $\prod_{k=0}^{k=n+1} a_k \equiv \prod_{k=0}^{k=n+1} b_k\ (mod\ m)$

In all, we have proven that $\forall m \in \mathbb{Z}, \forall a, b \in S,\ (m \neq 0) \Longrightarrow (\ \forall n \in \mathbb{N}^+, (\forall k \leq n, a_k \equiv b_k (mod\ m)) \Rightarrow \prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k\ (mod\ m))$ ■

(b)

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

P(n): $(\forall\ i \in \mathbb{N}, i \leq n \Longrightarrow gcd(d, b_i) = 1) \Longrightarrow d \nmid \prod_{i=0}^{i=n} b_i$

Proof: We will prove this statement using induction on n.

Let $d \in \mathbb{N}$, let $b \in S$, we assume that $d > 1$ and $(\forall m \in \mathbb{N},\ b_m > 0)$

Base case:

Let n=0

We assume that $\forall\ i \in \mathbb{N}, i \leq n \Longrightarrow \gcd(d, b_i) = 1$, that is $\gcd(d, b_0) = 1$
We want to show that $d \nmid \prod_{i=0}^{i=n} b_i$ that is $d \nmid b_0$
We will prove this by contradiction
Assume that d|b_0
Since d|d, so $\gcd(d, b_0) \geq d > 1$
Hence $\gcd(d, b_0) \neq 1, \mathit{and\ we\ get\ a\ contradiction}$
So $(\forall\ i \in \mathbb{N}, i \leq n \Longrightarrow \gcd(d, b_i) = 1) \Longrightarrow d \nmid \prod_{i=0}^{i=n} b_i$

Induction step:
Let $n \in \mathbb{N}$ and assume that $(\forall\ i \in \mathbb{N}, i \leq n \Longrightarrow \gcd(d, b_i) = 1) \Longrightarrow d \nmid \prod_{i=0}^{i=n} b_i$
We want to prove that $(\forall\ i \in \mathbb{N}, i \leq n+1 \Longrightarrow \gcd(d, b_i) = 1) \Longrightarrow d \nmid \prod_{i=0}^{i=n+1} b_i$
Assume that $\forall\ i \in \mathbb{N}, i \leq n+1 \Longrightarrow \gcd(d, b_i) = 1$
We want to show that $d \nmid \prod_{i=0}^{i=n+1} b_i$
We will prove this by contradiction
Assume that $d | \prod_{i=0}^{i=n+1} b_i$ that is $d | \prod_{i=0}^{i=n} b_i \times b_{n+1}$
Since $\forall\ i \in \mathbb{N}, i \leq n+1 \Longrightarrow \gcd(d, b_i) = 1$ and n+1>n
So $\forall\ i \in \mathbb{N}, i \leq n \Longrightarrow \gcd(d, b_i) = 1$ so $d \nmid \prod_{i=0}^{i=n} b_i$, that is gcd($d$, $\prod_{i=0}^{i=n} b_i$)=1 (by induction hypothesis)
Since $\forall a, b \in \mathbb{N},\ \forall c \in \mathbb{Z}, (\gcd(a, b) = 1 \wedge a|bc) \Longrightarrow (a|c)$ (2(g) from problem set 2)
Since gcd(d, $\prod_{i=0}^{i=n} b_i$)=1 and d, $\prod_{i=0}^{i=n} b_i \in \mathbb{N}$ and $b_{n+1} \in \mathbb{Z}$ and $d | \prod_{i=0}^{i=n} b_i \times b_{n+1}$
Thus d|b_{n+1}
So gcd(d, $b_{n+1}) \geq d > 1$
But we already know from our assumption that gcd(d, $b_{n+1}) = 1$, so we get a contradiction
Hence $d \nmid \prod_{i=0}^{i=n+1} b_i$

In all we have proven that $\forall d \in \mathbb{N},\ \forall b \in S,\ (d > 1\ \wedge\ (\forall m \in \mathbb{N},\ b_m > 0)) \Longrightarrow (\forall n \in \mathbb{N},$ $(\forall\ i \in \mathbb{N}, i \leq n \Longrightarrow \gcd(d, b_i) = 1) \Longrightarrow d \nmid \prod_{i=0}^{i=n} b_i)$ ■

(c)

WTS:$\forall n \in \mathbb{N}, n > 1 \Longrightarrow \sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$

P(n): $\sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$

Proof:
We will prove this statement using induction on n.

Base case:
Let n=2 (2>1)

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

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

Induction step:

Let $\mathrm{n} \in \mathbb{N}$, and assume that $\mathrm{n} > 1$

We assume that $\sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$

We want to prove that $\sum_{j=n+2}^{j=2n+2} \frac{1}{j} > \frac{13}{24}$

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

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

Since 2n+2>2n+1>0

So $\frac{1}{2n+1} > \frac{1}{2n+2} > 0$

So $\frac{1}{2n+1} - \frac{1}{2n+2} > 0$

So $\sum_{j=n+1}^{j=2n} \frac{1}{j} + \frac{1}{2n+1} - \frac{1}{2n+2} > \sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$ (by induction hypothesis)

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

In all we have proven that $\forall \mathrm{n} \in \mathbb{N}, \mathrm{n} > 1 \Longrightarrow \sum_{j=n+1}^{j=2n} \frac{1}{j} > \frac{13}{24}$ ■

(d)

WTS:$\forall \mathrm{c} \in \mathrm{S}, (c_n = \begin{cases} 0, & if\ n = 0 \\ c_{n-1} + 3n^2 - 3n + 1, & if\ n > 0 \end{cases}) \Longrightarrow (\forall \mathrm{n} \in \mathbb{N}, c_n = n^3)$

P(n): $c_n = n^3$

Proof: We will prove this statement using induction on n.

Let $\mathrm{c} \in \mathrm{S}$, and assume that $c_n = \begin{cases} 0, & if\ n = 0 \\ c_{n-1} + 3n^2 - 3n + 1, & if\ n > 0 \end{cases}$

Base case:

Let n=0, $c_n = 0 = n^3$,

Induction step:

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

Assume $c_n = n^3$

We want to show that $c_{n+1} = (n+1)^3$

Since n$\in\mathbb{N}$, so n≥0, hence n+1>0

Thus:

$c_{n+1} = c_n + 3(n+1)^2 - 3(n+1) + 1$

$= n^3 + 3(n+1)^2 - 3(n+1) + 1$ (by induction hypothesis)

$= n^3 + 3n^2 + 3n + 1$

$=(n+1)^3$

In all, we have proven that $\forall c \in S, (c_n = \begin{cases} 0, & if\ n = 0 \\ c_{n-1} + 3n^2 - 3n + 1, & if\ n > 0 \end{cases}) \Rightarrow (\forall n \in \mathbb{N}, c_n = n^3)$ ■

2.(a)

WTS: $\forall n, k \in \mathbb{N}, k \leq n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

P(n): $\forall\ k \in \mathbb{N}, 0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Proof:

Let $n, k \in \mathbb{N}$, assume k=n, we know that the number of subsets S of size |s| is always 1, so $\binom{n}{k} = 1$ and $\frac{n!}{k!(n-k)!} = \frac{n!}{n!0!} = 1$, hence $\forall n, k \in \mathbb{N}, k = n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ is always true.

Let $n, k \in \mathbb{N}$, assume k=0, we know that the number of empty subset of a set is always 1, so $\binom{n}{k} = 1$ and $\frac{n!}{k!(n-k)!} = \frac{n!}{n!0!} = 1$, hence $\forall n, k \in \mathbb{N}, k = 0 \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ is always true.

Therefore, we only need to prove $\forall n, k \in \mathbb{N}, 0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

We will prove this statement using induction on n.

Base case:

Let n=0

Let $k \in \mathbb{N}$, assume $0 < k < n$, that is $0 < k < 0$ and this is false, so $0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ *is true. Hence* $\forall\ k \in \mathbb{N}, 0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Let n=1

Let $k \in \mathbb{N}$, assume $0 < k < n$, that is 0<k<1 since $k \in \mathbb{N}$, so this assumption is false, so $0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ *is true. Hence* $\forall\ k \in \mathbb{N}, 0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Let n=2

Let $k \in \mathbb{N}$, assume $0 < k < n$, that is 0<k<2, so k=1, since there are two elements in a set which size is two. So the number of subsets S of size 1 is 2, so $\binom{n}{k} = 2$

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

Thus $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Hence $\forall\ k \in \mathbb{N}, 0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Induction step:

Let $n \in \mathbb{N}$, assume that $\forall\ k \in \mathbb{N}, 0 < k < n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Since $\forall n, k \in \mathbb{N}, k = n \Rightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ is always true and $\forall n, k \in \mathbb{N}, k = 0 \Rightarrow \binom{n}{k} =$

$\frac{n!}{k!(n-k)!}$ is always true. We can write the assumption as $\forall\, \mathrm{k} \in \mathbb{N}, 0 \leq \mathrm{k} \leq \mathrm{n} \Longrightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

We want to show that $\forall\, \mathrm{k} \in \mathbb{N}, 0 < \mathrm{k} < \mathrm{n}+1 \Longrightarrow \binom{n+1}{k} = \frac{(n+1)!}{k!(n+1-k)!}$

Let $\mathrm{k} \in \mathbb{N}$, assume that $0 < \mathrm{k} < \mathrm{n}+1$, we want to show that $\binom{n+1}{k} = \frac{(n+1)!}{k!(n+1-k)!}$

When it comes to a set S with |S|=n+1, we can let the elements in the set be $\{s_1, s_2, \ldots, s_n, s_{n+1}\}$ Let S'=$\{s_1, s_2, \ldots, s_n\}$ so that S=S'∪ $\{s_{n+1}\}$, *also* |S'|=n

- First, counting subset of size k that contains s_{n+1}:
  Since every subset of S of size k that contains s_{n+1} must contain exactly k-1 elements from S', there are $\binom{n}{k-1}$ choices of elements from S'.
  Since $0 < \mathrm{k} < \mathrm{n}+1$ so $0 \leq \mathrm{k}-1 \leq \mathrm{n}-1$, thus $0 \leq \mathrm{k}-1 \leq \mathrm{n}$, Hence $\binom{n}{k-1} = \frac{n!}{(k-1)!(n-k+1)!}$ (by induction hypothesis)

  Hence there is $\frac{n!}{(k-1)!(n-k+1)!}$ subsets of S of size k that contains s_{n+1}
- Second, counting subset of size k that does not contain s_{n+1}:
  Every subset of size k of S that does not contain s_{n+1} must contain k of the elements $\{s_1, s_2, \ldots, s_n\}$. That is, these subsets are exactly the subsets of size k of S', so the number of these subsets is $\binom{n}{k}$.
  Since $0 < \mathrm{k} < \mathrm{n}+1$ so $0 < \mathrm{k} \leq \mathrm{n}$ thus $0 \leq \mathrm{k} \leq \mathrm{n}$,Hence $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ (by induction hypothesis)

  Hence there is $\frac{n!}{k!(n-k)!}$ subsets of S of size k that does not contain s_{n+1}

By combining the two counts from the first and second part, the total number of subsets of size k of S is $\frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!}$

That is $\binom{n+1}{k} = \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} = \frac{n!k+n!(n-k+1)}{k!(n-k+1)!} = \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n+1-k)!}$

Hence we have shown that $\binom{n+1}{k} = \frac{(n+1)!}{k!(n+1-k)!}$

In all we have proven that $\forall \mathrm{n}, \mathrm{k} \in \mathbb{N}, 0 < \mathrm{k} < \mathrm{n} \Longrightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ And $\forall \mathrm{n}, \mathrm{k} \in \mathbb{N}, \mathrm{k} = \mathrm{n} \Longrightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ and $\forall \mathrm{n}, \mathrm{k} \in \mathbb{N}, \mathrm{k} = 0 \Longrightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$

Therefore we have proven that $\forall \mathrm{n}, \mathrm{k} \in \mathbb{N}, \mathrm{k} \leq \mathrm{n} \Longrightarrow \binom{n}{k} = \frac{n!}{k!(n-k)!}$ ■

(b)

The elements of DTP_2: $\{\emptyset, \{1,2\}\}$, $\{\{1\}, \{2\}\}$

The elements of DTP_3: $\{\emptyset, \{1,2,3\}\}$, $\{\{1\}, \{2,3\}\}$, $\{\{2\}, \{1,3\}\}$, $\{\{3\}, \{1,2\}\}$

(c)

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

Proof:

WTS: $\forall \mathrm{n} \in \mathbb{N}$, $|DTP_n| = \begin{cases} 1, \ if\ n = 0 \\ 2^{n-1}, \ \ if\ n > 0 \end{cases}$

P(n): $|DTP_n| = 2^{n-1}$

1. Let n=0

   Since we got from the question that $DTP_0 = \{\{\emptyset, \emptyset\}\}, so\ |DTP_0| = 1$

   So our statement is true when n=0.

2. We will prove the following statement using induction on n.

   Base case:

   Let n=1

   Since we got from the question that $DTP_1 = \{\{\{1\}, \emptyset\}\}, so\ |DTP_1| = 1$

   Since $2^{n-1} = 2^0 = 1$

   So $|DTP_n| = 2^{n-1}$

   Induction step:

   Let $\mathrm{n} \in \mathbb{N}$, assume $n > 0$, we assume $|DTP_n| = 2^{n-1}$

   We want to prove that $|DTP_{n+1}| = 2^n$

   Since $S_{n+1} = \{1,2,\ldots,\mathrm{n},\mathrm{n}+1\}$, S_n=$\{1,2,\ldots,\mathrm{n}\}$ so that S_{n+1}=S_n∪$\{\mathrm{n}+1\}$ (Definition 3)

   According to the definition of DTP_{n+1}: DTP_{n+1}=$\{\{\mathrm{A},\mathrm{B}\} | \mathrm{A},\mathrm{B} \subseteq S_{n+1}\ and\ A \cup B = S_{n+1}\ and\ A \cap B\ =\ \emptyset\}$

   Let $\{\mathrm{A},\mathrm{B}\} \in DTP_{n+1}$, so $\mathrm{n}+1$ must be in and only be in one of A,B

   If $\mathrm{n}+1 \in \mathrm{A}$, take C=A without n+1, D=B.

   If $\mathrm{n}+1 \in \mathrm{B}$, take C=A, D=B without n+1.

   Let's first consider the number of {C,D}, then consider the number of {A,B} which is $|DTP_{n+1}|$

   Since $\{\mathrm{A},\mathrm{B}\}$'s definition is : $\mathrm{A},\mathrm{B} \subseteq S_{n+1}\ and\ A \cup B = S_{n+1}\ and\ A \cap B\ =\ \emptyset$ and we also know that S_{n+1}=S_n∪$\{\mathrm{n}+1\}$

   So the definition of $\{\mathrm{C},\mathrm{D}\}$ is : $\mathrm{C},\mathrm{D} \subseteq S_{n+1} \backslash \{\mathrm{n}+1\} = S_n$ and $\mathrm{C} \cup \mathrm{D} = S_{n+1} \backslash \{\mathrm{n}+1\} = S_n$ and $\mathrm{C} \cap \mathrm{D}\ =\ \emptyset$

   Hence we can find that $\{\mathrm{C},\mathrm{D}\}$**'s definition is equal to the definition of** DTP_n, so the number of $\{\mathrm{C},\mathrm{D}\}$ is equal to $|DTP_n|$ which is 2^{n-1} (by induction hypothesis)

   Now let's consider the number of {A,B} which is $|DTP_{n+1}|$, since

   If $\mathrm{n}+1 \in \mathrm{A}$, take C=A without n+1, D=B.

   If $\mathrm{n}+1 \in \mathrm{B}$, take C=A, D=B without n+1.

   {A,B} is $\{\mathrm{C},\mathrm{D}\}$ add up with n+1, for every $\{\mathrm{C},\mathrm{D}\}$, we can add up n+1 on C or on D, so there are two ways to add on n+1. That is the number of {A,B} is equal to $2 \times$ **the number of** $\{\mathrm{C},\mathrm{D}\}$. Hence $|DTP_{n+1}| = 2 \times |DTP_n| = 2 \times 2^{n-1} = 2^n$

In all we have proven that

$\forall n \in \mathbb{N}$, $\quad |DTP_n| = \begin{cases} 1, & if \ n = 0 \\ 2^{n-1}, & if \ n > 0 \end{cases}$

■

3. (a)

WTS:Theorem 5.8.: For all $f: \mathbb{N} \longrightarrow \mathbb{R}^{\geq 0}$, if f(n) is eventually greater than or equal to 1, then $\lfloor f \rfloor \in \Theta(f)$ and $\lceil f \rceil \in \Theta(f)$

The definition of big-Theta: Definition 5.6. Let $f, g: \mathbb{N} \longrightarrow \mathbb{R}^{\geq 0}$. We say that g is (Big-)Theta of f if and only if g is both Big-Oh of f and Omega of f. In this case, we can write $g \in \Theta(f)$

Equivalenty, g is Theta of f if and only if there exist constants $c_1, c_2, n_0 \in \mathbb{R}^+$ such that for all $n \in \mathbb{N}$, if $n \geq n_0$ $then$ $c_1 f(n) \leq g(n) \leq c_2 f(n)$.

Proof:

Let $f: \mathbb{N} \longrightarrow \mathbb{R}^{\geq 0}$ we assume that f(n) is eventually greater than or equal to 1 that is $\exists n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow f(n) \geq 1$, let n_0 be that value.

We want to show that $\exists c_{11}, c_{21}, n_1 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_1 \Rightarrow c_{11} f(n) \leq \lfloor f \rfloor \leq c_{21} f(n)$

And $\exists c_{12}, c_{22}, n_2 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_2 \Rightarrow c_{12} f(n) \leq \lceil f \rceil \leq c_{22} f(n)$

First, from the worksheet, we know that: Given any real number x, the floor of x, denoted$\lfloor x \rfloor$, is defined to be the largest integer that is less than or equal to x. Similarly, the ceiling of x , denoted $\lceil x \rceil$, is defined to be the smallest integer that is greater than or equal to x. Hence we know that $x - 1 < \lfloor x \rfloor \leq x$ and $x \leq \lceil x \rceil < x + 1$

- show that $\exists c_{11}, c_{21}, n_1 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_1 \Rightarrow c_{11} f(n) \leq \lfloor f \rfloor \leq c_{21} f(n)$
  1. If f(n) is eventually greater than or equal to 1 but smaller than 2:
     That is $\exists n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Rightarrow 2 > f(n) \geq 1$, let n_0 be that value.

     Let $c_{11} = \frac{1}{2}$, $c_{21} = 1$, $n_1 = n_0$, so $c_{11}, c_{21}, n_1 \in \mathbb{R}^+$, since $n_0, \frac{1}{2}, 1 \in \mathbb{R}^+$

     Let $n \in \mathbb{N}$, assume $n \geq n_1$

     We want to show that $c_{11} f(n) \leq \lfloor f \rfloor \leq c_{21} f(n)$

  ✧ Since $n \geq n_1 = n_0$, so $2 > f(n) \geq 1$, so $1 > \frac{1}{2} f(n) \geq \frac{1}{2}$

     So $c_{11} f(n) = \frac{1}{2} f(n) < 1$

     Since $n \geq n_1 = n_0$, so $2 > f(n) \geq 1$, so $\lfloor f \rfloor = 1$

     Hence $c_{11} f(n) = \frac{1}{2} f(n) < 1 = \lfloor f \rfloor$

     That is $c_{11} f(n) \leq \lfloor f \rfloor$

  ✧ Since $n \geq n_1 = n_0$, so $2 > f(n) \geq 1$, so $\lfloor f \rfloor = 1$

     So $\lfloor f \rfloor \leq f(n) = c_{21} f(n)$ (since $c_{21} = 1$)

  Hence we have shown that $c_{11} f(n) \leq \lfloor f \rfloor \leq c_{21} f(n)$

  2. If f(n) is eventually greater than or equal to 2:

That is $\exists n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \Longrightarrow f(n) \geq 2$, let n_0 be that value.

Let $c_{11} = \frac{1}{3}$, $c_{21} = 1$, $n_1 = n_0$, so $c_{11}, c_{21}, n_1 \in \mathbb{R}^+$, since $n_0, \frac{1}{3}, 1 \in \mathbb{R}^+$

Let $\mathrm{n} \in \mathbb{N}$, assume $\mathrm{n} \geq n_1$
We want to show that $c_{11} f(n) \leq \lfloor \mathrm{f} \rfloor \leq c_{21} f(n)$

- ✧ Since $\mathrm{n} \geq n_1 = n_0$, so $f(n) \geq 2$, thus $\frac{2}{3} f(n) \geq \frac{4}{3} > 1$

  So $f(n) - \frac{1}{3} f(n) > 1$

  Thus $f(n) - c_{11} f(n) > 1$
  So $c_{11} f(n) < f(n) - 1$
  Since $\lfloor \mathrm{f} \rfloor > f - 1$ no matter what f is
  So $\lfloor \mathrm{f} \rfloor > f - 1 > c_{11} f(n)$
- ✧ Since $\lfloor \mathrm{f} \rfloor \leq f$ no matter what f is
  So $\lfloor \mathrm{f} \rfloor \leq f = c_{21} f(n)$ (since $c_{21} = 1$)

Hence we have shown that $c_{11} f(n) \leq \lfloor \mathrm{f} \rfloor \leq c_{21} f(n)$
In all we have shown that $\exists c_{11}, c_{21}, n_1 \in \mathbb{R}^+, \forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq n_1 \Longrightarrow c_{11} f(n) \leq \lfloor \mathrm{f} \rfloor \leq c_{21} f(n)$

- Show that $\exists c_{12}, c_{22}, n_2 \in \mathbb{R}^+, \forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq n_2 \Longrightarrow c_{12} f(n) \leq \lceil f \rceil \leq c_{22} f(n)$
  Let $c_{12} = 1, c_{22} = 3, n_2 = n_0$, so $c_{12}, c_{22}, n_2 \in \mathbb{R}^+$, since $n_0, 3, 1 \in \mathbb{R}^+$
  Let $\mathrm{n} \in \mathbb{N}$, assume $\mathrm{n} \geq n_2$
  We want to show that $c_{12} f(n) \leq \lceil f \rceil \leq c_{22} f(n)$
  - ✧ Since $\lceil f \rceil \geq f$ no matter what f is
    So $\lceil f \rceil \geq f = c_{12} f(n)$ (Since $c_{12} = 1$)
  - ✧ Since $\mathrm{n} \geq n_2 = n_0$, so $f(n) \geq 1$, so $2f(n) \geq 2 > 1$
    So $3f(n) \geq f + 1$
    Thus $c_{22} f(n) \geq f + 1$ (Since $c_{22} = 3$)
    We also know that $f + 1 > \lceil f \rceil$ no matter what f is
    Hence $c_{22} f(n) \geq f + 1 > \lceil f \rceil$

  Hence we have shown that $c_{12} f(n) \leq \lceil f \rceil \leq c_{22} f(n)$

In all we have shown that $\exists c_{12}, c_{22}, n_2 \in \mathbb{R}^+, \forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq n_2 \Longrightarrow c_{12} f(n) \leq \lceil f \rceil \leq c_{22} f(n)$

Therefore we have proven that For all $\mathrm{f}: \mathbb{N} \longrightarrow \mathbb{R}^{\geq 0}$, if f(n) is eventually greater than or equal to 1, then $\lfloor \mathrm{f} \rfloor \in \Theta(\mathrm{f})$ and $\lceil f \rceil \in \Theta(\mathrm{f})$ ■

(b)
WTS : $\forall \mathrm{a}, \mathrm{b} \in \mathbb{R}^+, (b > a \wedge a > 1) \Longrightarrow b^n \notin O(a^n)$
That is: $\forall \mathrm{a}, \mathrm{b} \in \mathbb{R}^+, (b > a \wedge a > 1) \Longrightarrow (\forall \mathrm{c}, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{N}, (n \geq n_0) \wedge (b^n > c \times a^n))$
Proof:
Let $\mathrm{a}, \mathrm{b} \in \mathbb{R}^+$,assume $b > a \; and \; a > 1$
We want to prove that $\forall \mathrm{c}, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{N}, (n \geq n_0) \wedge (b^n > c \times a^n)$

Let $\mathrm{c}, n_0 \in \mathbb{R}^+$, take $\mathrm{n} = \max(\lceil \log_{\frac{b}{a}} c \rceil + 1, \lceil n_0 \rceil + 1)$, so $n \in \mathbb{N}$

We want to prove that $(n \geq n_0) \wedge (b^n > c \times a^n)$

- We want to prove that $n \geq n_0$:

  Since $\mathrm{n} = \max(\lceil \log_{\frac{b}{a}} c \rceil + 1, \lceil n_0 \rceil + 1)$

  So $n \geq \lceil n_0 \rceil + 1 > \lceil n_0 \rceil \geq n_0$
  Hence $n \geq n_0$

- We want to prove that $b^n > c \times a^n$:

  Since $\mathrm{n} = \max(\lceil \log_{\frac{b}{a}} c \rceil + 1, \lceil n_0 \rceil + 1)$

  So $n \geq \lceil \log_{\frac{b}{a}} c \rceil + 1 > \lceil \log_{\frac{b}{a}} c \rceil \geq \log_{\frac{b}{a}} c$

  Hence $n > \log_{\frac{b}{a}} c$

  Since $b > a \; and \; a > 1$ so $\frac{b}{a} > 1$

  Hence $(\frac{b}{a})^n > (\frac{b}{a})^{\log_{\frac{b}{a}} c}$

  That is $(\frac{b}{a})^n > c$

  Since $a > 1$ so $a^n > 0$
  Hence $b^n > \; c \times a^n$

Hence we have shown that $(n \geq n_0) \wedge (b^n > c \times a^n)$
Therefore we have proven that $\forall \mathrm{a}, \mathrm{b} \in \mathbb{R}^+, (b > a \wedge a > 1) \Longrightarrow b^n \notin O(a^n)$ ■

(c)
WTS：$RT_{xgcd} \in O(\lg n)$
Proof:

Let $\mathrm{n}, \mathrm{m} \in \mathbb{N}$, we want to show that $RT_{xgcd} \in O(\lg n)$

(There is one assignment and one return sentence in the whole function and we will consider them only when there is no iteration in the loop. Cause $2 \in O(\lg n)$(take c=1 and $\mathrm{n_0}$=1000, so $\forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq \mathrm{n_0} = 1000, \mathrm{c} \times \lg\mathrm{n} = \lg\mathrm{n} \geq \lg 1000 > 2$) and from therem5.5 we know that for all $\mathrm{f}, \mathrm{g}, \mathrm{h}: \mathbb{N} \longrightarrow \mathbb{R}^{\geq 0}, \text{if } \mathrm{f} \in O(\mathrm{h}) \text{ and } \mathrm{g} \in O(\mathrm{h}), \text{then } \mathrm{f} + \mathrm{g} \in O(\mathrm{h})$, so we only need to consider whether the running time of the loop is a big-Oh of $\lg n$.)

assume $\mathrm{m} \neq 0, \text{and } \mathrm{n} \neq 0$

- CASE1: n=m:
  If n=m , then the quotient will be r0//r1=1
  Hence after one iteration, r1=n-(n//m)m=n-m=0
  And the loop is over.
  Hence when n=m, $RT_{xgcd} = 1 \in O(\lg n)$ (take c=1 and $\mathrm{n_0}$=1000, so $\forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq \mathrm{n_0} = 1000, \mathrm{c} \times \lg\mathrm{n} = \lg\mathrm{n} \geq \lg 1000 > 1$)
- CASE2: m<n:

Let r_0 be the original value of r0, r_1 be the value of r0 after one loop iteration, and r_2 the value of r0 after two loop iterations. We want to prove that $r_2 \leq \frac{1}{2}\mathrm{r}_0$

From the question, we get that $r_2 = \mathrm{r}_0 - (\mathrm{r}_0//r_1)r_1$
Since m<n from the "r0, r1 = r1, r0 - quotient * r1", we know that $r_1 < \mathrm{r}_0$, since r_1 is either be the remainder that the last r0 divides r_0 or be m when r_0 be n.
We divide up this proof into two cases:

- Case1: $0 \leq r_1 \leq \frac{1}{2}\mathrm{r}_0$

  (If $r_1 = 0$, although the loop will end at that time, we may assume that the loop is going on till the next iteration when r_2 is something related with r_0 and the loop end at that time. Since we are calculating the worst situation.)

  Since $(\mathrm{r}_0//r_1) \times r_1 + \mathrm{r}_0\%r_1 = \mathrm{r}_0$
  So $r_2 = \mathrm{r}_0 - (\mathrm{r}_0//r_1)r_1 = \mathrm{r}_0\%r_1$

  Since $\mathrm{r}_0\%r_1 < r_1$ and $r_1 \leq \frac{1}{2}\mathrm{r}_0$

  Thus $r_2 = \mathrm{r}_0\%r_1 \leq \frac{1}{2}\mathrm{r}_0$, that is $r_2 \leq \frac{1}{2}\mathrm{r}_0$

- Case2: $\frac{1}{2}\mathrm{r}_0 < r_1 < \mathrm{r}_0$

  Since $\frac{1}{2}\mathrm{r}_0 < r_1 < \mathrm{r}_0$, so $\mathrm{r}_0//r_1 = 1$ (since if $\mathrm{r}_0//r_1 \neq 1, then\ \mathrm{r}_0//r_1 = 0\ or\ \mathrm{r}_0//r_1 > 1$. for $\mathrm{r}_0//r_1 = 0, then\ \mathrm{r}_0\%r_1 = \mathrm{r}_0 < r_1$ **, we get a contradiction.** For $\mathrm{r}_0//r_1 > 1$, then $\mathrm{r}_0 \geq 2r_1 > \mathrm{r}_0$, we get a contradiction. Thus $\mathrm{r}_0//r_1 = 1$)
  So $r_2 = \mathrm{r}_0 - (\mathrm{r}_0//r_1)r_1 = \mathrm{r}_0 - r_1$

  Since $\frac{1}{2}\mathrm{r}_0 < r_1 < \mathrm{r}_0$

  So $-\frac{1}{2}\mathrm{r}_0 > -r_1 > -\mathrm{r}_0$

  So $\mathrm{r}_0 - \frac{1}{2}\mathrm{r}_0 > \mathrm{r}_0 - r_1 > \mathrm{r}_0 - \mathrm{r}_0$ (since $\mathrm{r}_0 \in \mathbb{N}$)

  Hence $\frac{1}{2}\mathrm{r}_0 > \mathrm{r}_0 - r_1$

  Thus $r_2 = \mathrm{r}_0 - r_1 < \frac{1}{2}\mathrm{r}_0$, that is $r_2 \leq \frac{1}{2}\mathrm{r}_0$

In all we have shown that $r_2 \leq \frac{1}{2}\mathrm{r}_0$

That is every two iterations of the loop reduces r0 by at least half.
And the loop will be over when r1=0 that is when r0 becomes the gcd(n.m), (since the loop is to get the extended gcd(n,m) and r0=gcd(n,m), r0=s0n+t0m)
Since we want to get the big-Oh of RT_{xgcd}, hence we can think about the worst condition that is gcd(n.m)=1. Hence when $1 \leq \mathbf{r0} < 2$, the loop will get over. (Since sometime we won't get 1 when divide n by 2 everytime and the gcd(n,m) must be

greater or equal to 1)

After 2k iterations, r0 will be $\frac{n}{2^k}$, and take this into $1 \le r0 < 2$, we get $1 \le \frac{n}{2^k} < 2$, so $k = \lfloor \log_2 n \rfloor$

Hence the number of actual iterations is at most $2\lfloor \log_2 n \rfloor$, with each iteration costing a single step

Thus $RT_{xgcd} \le 2\lfloor \log_2 n \rfloor$

Take $c_1 = \frac{\ln 10}{\ln 2}$, $c_2 = 2 \times \frac{\ln 10}{\ln 2}$, $n_0 = 100$ so $\forall n \in \mathbb{N}, n \ge n_0$: $c_2 \lg n = 2\log_2 n \ge 2\lfloor \log_2 n \rfloor$, $c_1 \lg n = \log_2 n < \log_2 n + \log_2 n - 2 < 2\lfloor \log_2 n \rfloor$

So $2\lfloor \log_2 n \rfloor \in \Theta(\lg n)$, hence $RT_{xgcd} \in O(\lg n)$

- CASE3: m>n:

  So the first iteration will do the work that exchange the value of r1 and r0, so r1 will be n and r0 will be m, and the second iteration will do the work that change n back to r0, and r1 at this time is the remainder of m divides n which is smaller than n, let's call it m'.

  Start with the third iteration. Let r_0 be the original value of r0, r_1 be the value of r0 after one loop iteration, and r_2 the value of r0 after two loop iterations. We want to prove that $r_2 \le \frac{1}{2} r_0$

  From the question, we get that $r_2 = r_0 - (r_0 // r_1) r_1$

  Since m'<n from the "r0, r1 = r1, r0 - quotient * r1", we know that $r_1 < r_0$, since r_1 is either be the remainder that the last r0 divides r_0 or be m' when r_0 be n.

  We divide up this proof into two cases:

  - Case1: $0 \le r_1 \le \frac{1}{2} r_0$

    (If $r_1 = 0$, although the loop will end at that time, we may assume that the loop is going on till the next iteration when r_2 is something related with r_0 and the loop end at that time. Since we are calculating the worst situation.)

    Since $(r_0 // r_1) \times r_1 + r_0 \% r_1 = r_0$

    So $r_2 = r_0 - (r_0 // r_1) r_1 = r_0 \% r_1$

    Since $r_0 \% r_1 < r_1$ and $r_1 \le \frac{1}{2} r_0$

    Thus $r_2 = r_0 \% r_1 \le \frac{1}{2} r_0$, that is $r_2 \le \frac{1}{2} r_0$

  - Case2: $\frac{1}{2} r_0 < r_1 < r_0$

    Since $\frac{1}{2} r_0 < r_1 < r_0$, so $r_0 // r_1 = 1$ (since if $r_0 // r_1 \ne 1, then\ r_0 // r_1 = 0\ or\ r_0 // r_1 > 1$. for $r_0 // r_1 = 0, then\ r_0 \% r_1 = r_0 < r_1$, **we get a contradiction.** For $r_0 // r_1 > 1$, then $r_0 \ge 2r_1 > r_0$, we get a contradiction. Thus $r_0 // r_1 = 1$)

    So $r_2 = r_0 - (r_0 // r_1) r_1 = r_0 - r_1$

    Since $\frac{1}{2} r_0 < r_1 < r_0$

So $-\frac{1}{2}\mathrm{r}_0 > -r_1 > -\mathrm{r}_0$

So $\mathrm{r}_0 - \frac{1}{2}\mathrm{r}_0 > \mathrm{r}_0 - r_1 > \mathrm{r}_0 - \mathrm{r}_0$ (since $\mathrm{r}_0 \in \mathbb{N}$)

Hence $\frac{1}{2}\mathrm{r}_0 > \mathrm{r}_0 - r_1$

Thus $r_2 = \mathrm{r}_0 - r_1 < \frac{1}{2}\mathrm{r}_0$, that is $r_2 \leq \frac{1}{2}\mathrm{r}_0$

In all we have shown that $r_2 \leq \frac{1}{2}\mathrm{r}_0$

That is every two iterations of the loop reduces r0 by at least half.
And the loop will be over when r1=0 that is when r0 becomes the gcd(n.m), (since the loop is to get the extended gcd(n,m) and r0=gcd(n,m), r0=s0n+t0m)
Since we want to get the big-Oh of RT_{xgcd}, hence we can think about the worst condition that is gcd(n.m)=1. Hence when $1 \leq \mathrm{r0} < 2$, the loop will get over. (Since sometime we won't get 1 when divide n by 2 everytime and the gcd(n,m) must be greater or equal to 1)

After 2k iterations, r0 will be $\frac{\mathrm{n}}{2^{\mathrm{k}}}$, and take this into $1 \leq \mathrm{r0} < 2$, we get $1 \leq \frac{\mathrm{n}}{2^{\mathrm{k}}} < 2$, so

$\mathrm{k} = \lfloor \log_2 \mathrm{n} \rfloor$
Hence the number of actual iterations is at most $2\lfloor \log_2 \mathrm{n} \rfloor + 2$ (since the first iteration will do the work that exchange the value of r1 and r0, so r1 will be n and r0 will be m, and the second iteration will do the work that change n back to r0, and r1 at this time is the remainder of m divides n which is smaller than n, so we gonna add 2 here) ,with each iteration costing a single step
Thus $RT_{xgcd} \leq 2\lfloor \log_2 \mathrm{n} \rfloor + 2$

Take $c_1 = \frac{\ln 10}{\ln 2}$, $c_2 = 3 \times \frac{\ln 10}{\ln 2}$, $n_0 = 100$ so $\forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq \mathrm{n}_0$: $c_2 \mathrm{lgn} = 3\log_2 \mathrm{n} \geq$

$2\log_2 \mathrm{n} + 2 \geq 2\lfloor \log_2 \mathrm{n} \rfloor + 2$, $c_1 \mathrm{lgn} = \log_2 \mathrm{n} < \log_2 \mathrm{n} + \log_2 \mathrm{n} < 2\lfloor \log_2 \mathrm{n} \rfloor$
So $2\lfloor \log_2 \mathrm{n} \rfloor + 2 \in \Theta(\lg n)$, hence $RT_{xgcd} \in O(\lg n)$

If m=0 :
So the condition is wrong at the first time
And $RT_{xgcd} = 2 \in O(\lg n)$ (take c=1 and n_0=1000, so $\forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq \mathrm{n}_0 = 1000, \mathrm{c} \times \mathrm{lgn} = \mathrm{lgn} \geq \mathrm{lg}1000 > 2$)
If n=0 and m$\neq 0$
There is only 1 iteration
And $RT_{xgcd} = 1 \in O(\lg n)$ (take c=1 and n_0=1000, so $\forall \mathrm{n} \in \mathbb{N}, \mathrm{n} \geq \mathrm{n}_0 = 1000, \mathrm{c} \times \mathrm{lgn} = \mathrm{lgn} \geq \mathrm{lg}1000 > 1$)

Therefore we have shown that $RT_{xgcd} \in O(\lg n)$ ■