CSC165H1F Problem Set 3

November 13, 2019

1. (a) Prove $\forall a, b, c \in \mathbb{Z}, ab \neq 0 \wedge gcd(|a|, |b|) = 1 \wedge a \mid bc \implies a \mid c$

Proof. Let $a, b, c \in \mathbb{Z}$. Assume $ab \neq 0$.

Assume $\gcd(|a|, |b|) = 1$, that is $a \neq 0 \wedge b \neq 0$ because if $a = 0 \vee b = 0$, then $ab = 0$.

Assume $a \mid bc$, that is $\exists k_0 \in \mathbb{Z}, ak_0 = bc$. This implies $\exists k_1 \in \mathbb{Z}, ak_1 = |b|c$ is also true.

We want to show $a|c$, that is $\exists k_2 \in \mathbb{Z}, ak_2 = c$.

Since $a \neq 0 \wedge b \neq 0$,

So we have $\exists p, q \in \mathbb{Z}, gcd(|a|, |b|) = 1 = |a|p + |b|q$ by Theorem 2.2

$$\begin{aligned} 1 =& |a|p + |b|q \\ c =& |a|pc + |b|qc \end{aligned} \tag{1}$$

Let $k_2 = pc + k_1 q$ if $a \geq 0$ and $k_2 = -pc + k_1 q$ if $a < 0$. We divide our proof into two cases by a.

Case 1. When $a \geq 0$, $k_2 = pc + k_1 q$.

$$\begin{aligned} ak_2 =& apc + ak_1 q \\ =& |a|pc + |b|qc \text{ by the assumption that } ak_1 = |b|c \\ =& c \text{ by } c = |a|pc + |b|qc \text{ proved above} \end{aligned} \tag{2}$$

Case 2. When $a < 0$, $k_2 = -pc + k_1 q$.

$$\begin{aligned} ak_2 =& - apc + ak_1 q \\ =& - apc + |b|qc \text{ by the assumption that } ak_1 = |b|c \\ =& - |a| \cdot -pc + |b|qc \\ =& |a|pc + |b|qc \\ =& c \text{ by } c = |a|pc + |b|qc \text{ proved above} \end{aligned} \tag{3}$$

Therefore, we have shown $ak_2 = c$ as required.

■

(b) *Proof.* We want to prove $\forall p, k \in \mathbb{N}, \text{Prime}(p) \wedge 1 < k < p \implies p \mid \binom{p}{k}$.

Let P(k) be the statement: "$p \mid \binom{p}{k}$".

We want to show $\forall p, k \in \mathbb{N}, \text{Prime}(p) \wedge 1 < k < p \implies \text{P}(k)$ by induction.

We only need to prove for $p \geq 3$ since for $p = 2$, $1 < k < p$ is always false. Therefore, for $p = 2$, the statement we want to prove is vacuously true.

Let $p, k \in \mathbb{N}$. Assume p is a prime and $p \geq 3$. Assume $1 < k < p$.

Base Case. Let $k = 2$ so that $1 < k < p$ is true.

$$\binom{p}{2} = \frac{p!}{2!(p-2)!} = \frac{p(p-1)}{2} \tag{4}$$

For all prime $p \geq 3$, p is odd and $p - 1$ is divisible by 2.

Hence, $\frac{p(p-1)}{2} = p\frac{p-1}{2}$ implies $p \mid \binom{p}{k}$.

We have proved P(2) is true.

Inductive Step. Let $a \in \mathbb{N}$ and $a \geq 2$. Assume $P(a)$ is true , that is, $p \mid \binom{p}{a}$, which is equivalent to $p \mid \frac{p!}{a!(p-a)!}$.

We want to show $P(a+1)$ is also true, that is, $p \mid \binom{p}{a+1}$, which is equivalent to $p \mid \frac{p!}{(a+1)!(p-a-1)!}$.

Because $\binom{p}{a+1}$ is an integer, $\frac{p!}{(a+1)!(p-a-1)!}$ is also an integer.

$$\frac{p!}{(a+1)!(p-a-1)!} = \frac{\frac{p!}{(a)!(p-a-1)!}}{a+1} \tag{5}$$

which indicates $a + 1 \mid \frac{p!}{a!(p-a-1)!}$. Because $gcd(a+1, p) = 1$ due to $a + 1 < p$ and $a + 1 \mid p \cdot \frac{(p-1)!}{a!(p-a-1)!}$, we have $a + 1 \mid \frac{(p-1)!}{a!(p-a-1)!}$ (using the statement we proved in 1(a)).

Then we have

$$
\begin{aligned}
& p \mid \binom{p}{a} \text{ by induction hypothesis} \\
\implies & p \mid \frac{p!}{a!(p-a)!} \\
\implies & p \mid \frac{p!}{a!(p-a)!} \cdot (p-a) \\
\implies & p \mid \frac{p!}{a!(p-a-1)!} \\
\implies & p \mid p \cdot \frac{(p-1)!}{a!(p-a-1)!} \\
\implies & p \mid p \cdot \frac{(p-1)!}{a!(p-a-1)!} \cdot \frac{1}{a+1} \text{ because } a+1 \mid \frac{(p-1)!}{a!(p-a-1)!},\ \frac{(p-1)!}{a!(p-a-1)!} \cdot \frac{1}{a+1} \text{ is an integer.} \\
\implies & p \mid p \cdot \frac{(p-1)!}{(a+1)!(p-a-1)!} \\
\implies & p \mid \frac{p!}{(a+1)!(p-a-1)!} \\
\implies & p \mid \binom{p}{a+1}
\end{aligned}
\tag{6}
$$

Therefore, P(a+1) is also true.

Finally, we have proved $\forall p, k \in \mathbb{N}, \text{Prime}(p) \wedge 1 < k < p \implies p \mid \binom{p}{k}$ by induction as required.

■

(c) Prove $\forall n, p \in \mathbb{N}, Prime(p) \implies n^p \equiv n \pmod{p}$.

Proof. We want to prove $\forall n, p \in \mathbb{N}, Prime(p) \implies n^p \equiv n \pmod{p}$.

Let $n, p \in \mathbb{N}$. Assume p is a prime.

Let P(n) be the statement: "$n^p \equiv n \pmod{p}$".

We are going to prove $\forall n, p \in \mathbb{N}, Prime(p) \implies P(n)$ by induction.

Base Case. Let $n = 0$. For any prime p, we have $n^p = 0^p = 0$ and $n = 0$.

Therefore, $n^p \equiv n \pmod{p}$ since $0 \equiv 0 \pmod{p}$ shows P(0) is true.

Inductive Step. Let $k \in \mathbb{N}$ and $k \geq 0$. Assume P(k) is true, that is $k^p \equiv k \pmod{p}$, which is equivalent to $p \mid k^p - k$.

We want to show P(k+1) is also true, that is $(k+1)^p \equiv k+1 \pmod{p}$, which is equivalent to $p \mid (k+1)^p - k - 1$.

$$
\begin{aligned}
&(k+1)^p - k - 1 \\
=&\left(\sum_{a=0}^{a=p} \binom{p}{a} k^{p-a} \cdot 1^a\right) - k - 1 \\
=&\binom{p}{0} k^{p-0} \cdot 1^0 + \binom{p}{1} k^{p-1} \cdot 1^1 + \binom{p}{p} k^{p-p} \cdot 1^p + \left(\sum_{a=2}^{a=p-1} \binom{p}{a} k^{p-a} \cdot 1^a\right) - k - 1 \\
=&k^p + p \cdot k^{p-1} + 1 + \left(\sum_{a=2}^{a=p-1} \binom{p}{a} k^{p-a} \cdot 1^a\right) - k - 1 \\
=&(k^p - k) + p \cdot k^{p-1} + \left(\sum_{a=2}^{a=p-1} \binom{p}{a} k^{p-a} \cdot 1^a\right)
\end{aligned}
\tag{7}
$$

$p \mid k^p - k$ is true by induction hypothesis.

$p \mid p \cdot k^{p-1}$ is true.

$p \mid \binom{p}{a}$ for $1 < a < p$ is true by the statement we proved in 1(b).

Since all terms in the expression of $(k^p - k) + p \cdot k^{p-1} + \left(\sum_{a=2}^{a=p-1} \binom{p}{a} k^{p-a} \cdot 1^a\right)$ is divisible by p, we conclude that $(k+1)^p - k - 1$ is also divisible by p.

Therefore, P(k+1) is true.

Finally, we have proved $\forall n, p \in \mathbb{N}, Prime(p) \implies n^p \equiv n \pmod{p}$ by induction.

■

2. (a) Prove $\forall b \in \mathbb{R}^+, bn^2 \in \mathcal{O}(2^n) \wedge bn^2 \notin \Omega(2^n)$

Proof. Let $b \in \mathbb{R}^+$.

We divide our proof into 2 parts.

PART 1. We want to prove $bn^2 \in \mathcal{O}(2^n)$, that is

$$\exists C, n_0 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_0 \implies bn^2 \leq C \cdot 2^n \tag{8}$$

Let $n_0 = 4$. Let $C = b$.

Let $n \in \mathbb{N}$. Assume $n \geq n_0$.

We want to show $bn^2 \leq C \cdot 2^n$.

Lemma 1. $\forall n \in \mathbb{N}, n \geq 4 \implies n^2 \leq 2^n$

We want to show the lemma by induction. Let $P(k)$ be the statement: $k^2 \leq 2^k$.

Base Case. Let $k = 4$. $k^2 = 4^2 = 16 \leq 16 = 2^4 = 2^k$. Therefore, $P(4)$ is true.

Inductive Step. Let $a \in \mathbb{N}$ and $a \geq 4$. Assume P(a) is true, that is $a^2 \leq 2^a$.

We want to show that $P(a+1)$ is also true, that is $(a+1)^2 \leq 2^{a+1}$.

First, we want to show

$$\begin{aligned} (a-1)^2 &> 2 \text{ because } a - 1 \geq 3 \\ a^2 - 2a + 1 &> 2 \\ a^2 &> 2a + 1 \end{aligned} \tag{9}$$

Then,

$$\begin{aligned} &(a+1)^2 \\ =&a^2 + 2a + 1 \\ <&a^2 + a^2 \text{ by that } a^2 > 2a + 1 \\ \leq&2^a + 2^a \text{ by induction hypothesis} \\ =&2^{a+1} \end{aligned} \tag{10}$$

Therefore, we have $(a+1)^2 \leq 2^{a+1}$. Finally, P(k) is true for all $k \in \mathbb{N}$ and $k \geq 4$.

Using this result, we have

$$\begin{aligned} n^2 &\leq 2^n \\ b \cdot n^2 &\leq C \cdot 2^n \text{ because } C = b \end{aligned} \tag{11}$$

Finally, we have proved $b \cdot n^2 \leq C \cdot 2^n$ as required.

PART 2. We want to prove $bn^2 \notin \Omega(2^n)$, that is

$$\forall C, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{N}, n \geq n_0 \wedge bn^2 < C \cdot 2^n \tag{12}$$

Let $C, n_0 \in \mathbb{R}^+$. Let $n = \max(\lceil n_0 + 16 \rceil, \lceil n_0 + 2\log_2 \frac{b}{C} \rceil)$.

$n \geq n_0$ is true because $n = \max(\lceil n_0 + 16 \rceil, \lceil n_0 + 2\log_2 \frac{b}{C} \rceil)$.

$$\begin{aligned} & n \geq n_0 + 16 \text{ because } n = \max(\lceil n_0 + 16 \rceil, \lceil n_0 + 2\log_2 \frac{b}{C} \rceil) \\ \implies & n > n_0 \wedge n > 16 \end{aligned} \tag{13}$$

Lemma 2. For all $n \in \mathbb{N}$ and $n > 16$, $2^n > n^4$.

Proof. We want to show the lemma by induction.

Let $P(k)$ be the statement: $2^k > k^4$.

Base Case. Let $k = 17$. $2^k = 2^{16} = 131072 > 83521 = 17^4 = k^4$. Therefore, $P(17)$ is true.

Inductive Step. Let $a \in \mathbb{N}$ and $a > 16$. Assume P(a) is true, that is $2^a > a^4$.

We want to show that $P(a+1)$ is also true, that is $2^{a+1} > (a+1)^4$.

$$\begin{aligned} & 2^{a+1} \\ =& 2^a + 2^a \\ >& a^4 + a^4 \text{ by induction hypothesis} \\ =& a^4 + \frac{1}{4}a^4 + \frac{1}{4}a^4 + \frac{1}{4}a^4 + \frac{1}{4}a^4 \\ >& a^4 + 4a^3 + 6a^2 + 4a + 1 \\ =& (a+1)^4 \end{aligned} \tag{14}$$

Therefore, $2^{a+1} > (a+1)^4$, P(a+1) is also true. Finally, we have proved this lemma. ■

Using Lemma 2, we have

$$\begin{aligned} 2^n >& n^4 \\ \implies 2^{\frac{n}{2}} >& n^2 \\ \implies \log_2 2^{\frac{n}{2}} >& \log_2 n^2 \end{aligned} \tag{15}$$

$$
\begin{aligned}
n \geq & n_0 + 2log_2\frac{b}{C} \text{ because } n = \max(\lceil n_0 + 16 \rceil, \lceil n_0 + 2\log_2\frac{b}{C} \rceil) \\
\implies & n > 2log_2\frac{b}{C} \\
\implies & \frac{n}{2} > \log_2\frac{b}{C} \\
\implies & \log_2 2^{\frac{n}{2}} > \log_2\frac{b}{C}
\end{aligned} \tag{16}
$$

Combining the result of $\log_2 2^{\frac{n}{2}} > \log_2 n^2$ and $\log_2 2^{\frac{n}{2}} > \log_2 \frac{b}{C}$, we have

$$
\begin{aligned}
2\log_2 2^{\frac{n}{2}} > & \log_2\frac{b}{C} + \log_2 n^2 \\
\implies \log_2 2^n > & \log_2\frac{b}{C} \cdot n^2 \\
\implies 2^n > & \frac{b}{C} \cdot n^2 \\
\implies \frac{2^n}{n^2} > & \frac{b}{C} \\
\implies C \cdot 2^n > & b \cdot n^2
\end{aligned} \tag{17}
$$

■

(b) Prove or disprove: $\forall f, g : \mathbb{N} \to \mathbb{R}^+, f \notin \Omega(g) \implies f \in \mathcal{O}(g)$

Proof. We want to disprove $\forall f, g : \mathbb{N} \to \mathbb{R}^+, f \notin \Omega(g) \implies f \in \mathcal{O}(g)$, that is, we want to prove its negation: $\exists f, g : \mathbb{N} \to \mathbb{R}^+, f \notin \Omega(g) \land f \notin \mathcal{O}(g)$

Let $f(n) = \left(\sin \frac{\pi n}{2}\right) \cdot n^2$. Let $g(n) = n$. $f, g : \mathbb{N} \to \mathbb{R}^+$ are satisfied.

We want to prove $f \notin \Omega(g) \land f \notin \mathcal{O}(g)$, that is

$$\begin{aligned} &(\forall c_0, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{Z}, n \geq n_0 \land f(n) < c_0 \cdot g(n)) \\ \land &(\forall c_1, n_1 \in \mathbb{R}^+, \exists n \in \mathbb{Z}, n \geq n_1 \land f(n) > c_1 \cdot g(n)) \end{aligned} \tag{18}$$

Part 1. We want to show $f \notin \Omega(g)$, that is $\forall c_0, n_0 \in \mathbb{R}^+, \exists n \in \mathbb{Z}, n \geq n_0 \land f(n) < c_0 \cdot g(n)$.

Let $c_0, n_0 \in \mathbb{R}^+$. Let $n = 2k_0$ for $k_0 \in \mathbb{Z} \land 2k_0 > n_0$.
We want to show $n \geq n_0 \land f(n) < c_0 \cdot g(n)$.

$n \geq n_0$ is true because we take n as $2k_0$ and $2k_0 > n_0$.

$$\begin{aligned} & f(n) \\ =& \sin\left(\frac{\pi n}{2}\right) \cdot n^2 \\ =& \sin\left(\frac{\pi \cdot 2k_0}{2}\right) \cdot (2k_0)^2 \\ =& \sin(\pi \cdot k_0) \cdot (2k_0)^2 \\ =& 0 \text{ because } \sin \pi \cdot k_0 = 0 \text{ due to } k_0 \text{ is an integer.} \\ <& c_0 \cdot 2k_0 \\ =& c_0 \cdot n \\ =& c_0 \cdot g(n) \end{aligned} \tag{19}$$

Therefore, we have shown $n \geq n_0 \land f(n) < c_0 \cdot g(n)$.

Part 2. We want to show $f \notin \mathcal{O}(g)$, that is $\forall c_1, n_1 \in \mathbb{R}^+, \exists n \in \mathbb{Z}, n \geq n_1 \land f(n) > c_1 \cdot g(n)$.

Let $c_1, n_1 \in \mathbb{R}^+$. Let $n = 4k_1 + 1$ for $k_1 \in \mathbb{Z} \land 4k_1 + 1 > n_1 \land 4k_1 + 1 > c_1$.
We want to show $n \geq n_1 \land f(n) > c_1 \cdot g(n)$.

$n \geq n_1$ is true because we take n as $4k_1 + 1$ and $4k_1 + 1 > n_1$.

$$
\begin{aligned}
& f(n) \\
=& \left(\sin \frac{\pi n}{2}\right) \cdot n^2 \\
=& \left(\sin \frac{\pi \cdot (4k_1 + 1)}{2}\right) \cdot (4k_1 + 1)^2 \\
=& \left(\sin \left(2\pi \cdot k_1 + \frac{\pi}{2}\right)\right) \cdot (4k_1 + 1)^2 \\
=& (4k_1 + 1)^2 \text{ because } \sin \left(2\pi \cdot k_1 + \frac{\pi}{2}\right) = 1 \\
>& c_1 \cdot 4k_1 + 1 \text{ because we take } n = 4k_1 + 1 \text{ such that } 4k_1 + 1 > c_1 \\
=& c_1 \cdot n \\
=& c_1 \cdot g(n)
\end{aligned}
\tag{20}
$$

Therefore, we have shown $n \geq n_1 \wedge f(n) > c_1 \cdot g(n)$.

Finally, we have disproved $\forall f, g : \mathbb{N} \to \mathbb{R}^+, f \notin \Omega(g) \implies f \in \mathcal{O}(g)$ by showing its negation: $\exists f, g : \mathbb{N} \to \mathbb{R}^+, f \notin \Omega(g) \wedge f \notin \mathcal{O}(g)$ is true.

■

(c) Prove or disprove: $\forall f_1, f_2, g_1, g_2 : \mathbb{N} \to \mathbb{R}^+, f_1 \in \Theta(g_1) \wedge f_2 \in \Theta(g_2) \implies max(f_1, f_2) \in \Theta(max(g_1, g_2))$.

Proof. We want to prove $\forall f_1, f_2, g_1, g_2 : \mathbb{N} \to \mathbb{R}^+, f_1 \in \Theta(g_1) \wedge f_2 \in \Theta(g_2) \implies max(f_1, f_2) \in \Theta(max(g_1, g_2))$.

Let $f_1, f_2, g_1, g_2 : \mathbb{N} \to \mathbb{R}^+$.

Assume $f_1 \in \Theta(g_1)$, that is $\exists c_1, c_2, n_1 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_1 \implies c_1 g_1(n) \leq f_1(n) \leq c_2 g_1(n)$.

Assume $f_2 \in \Theta(g_2)$, that is $\exists c_3, c_4, n_2 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_2 \implies c_3 g_2(n) \leq f_2(n) \leq c_4 g_2(n)$.

We want to show $max(f_1, f_2) \in \Theta(max(g_1, g_2))$, that is $\exists c_5, c_6, n_3 \in \mathbb{R}^+, \forall n \in \mathbb{N}, n \geq n_3 \implies c_5 max(g_1(n), g_2(n)) \leq max(f_1(n), f_2(n)) \leq c_6 max(g_1(n), g_2(n))$.

Let $c_1, c_2, n_1 \in \mathbb{R}^+$ such that $\forall n \in \mathbb{N}, n \geq n_1 \implies c_1 g_1(n) \leq f_1(n) \leq c_2 g_1(n)$.

Let $c_3, c_4, n_2 \in \mathbb{R}^+$ such that $\forall n \in \mathbb{N}, n \geq n_2 \implies c_3 g_2(n) \leq f_2(n) \leq c_4 g_2(n)$.

Let $c_5 = min\left(\frac{c_1}{max(1, \frac{c_2}{c_3})}, \frac{c_3}{max(1, \frac{c_4}{c_1})}\right)$. Let $c_6 = max(c_2, c_4)$.

Let $n_3 = max(n_1, n_2)$. Let $n \in \mathbb{N}$. Assume $n \geq n_3$.

We are going to divide our proof into two cases.

Case 1. Assume $f_1(n) \geq f_2(n)$ for some n in the domain $\mathbb{N}$.

We want to show $c_5 max(g_1(n), g_2(n)) \leq max(f_1(n), f_2(n)) \leq c_6 max(g_1(n), g_2(n))$.

Since $n \geq n_3$, then $n \geq n_1$ and $n \geq n_2$ are also satisfied. Therefore, we have $c_1 g_1(n) \leq f_1(n) \leq c_2 g_1(n)$ and $c_3 g_2(n) \leq f_2(n) \leq c_4 g_2(n)$.

Because $c_2 g_1(n) \geq f_1(n)$ and $f_2(n) \geq c_3 g_2(n)$ with the assumption $f_1(n) \geq f_2(n)$, $c_2 g_1(n) \geq c_3 g_2(n)$ is true.

$$
\begin{aligned}
& c_2 g_1(n) \geq c_3 g_2(n) \\
\implies & \frac{c_2}{c_3} g_1(n) \geq g_2(n) \\
\implies & max(1, \frac{c_2}{c_3}) g_1(n) \geq \frac{c_2}{c_3} g_1(n) \geq g_2(n) \\
\implies & max(1, \frac{c_2}{c_3}) g_1(n) \geq g_2(n) \wedge max(1, \frac{c_2}{c_3}) g_1(n) \geq g_1(n) \\
\implies & max(1, \frac{c_2}{c_3}) g_1(n) \geq max(g_1(n), g_2(n)) \qquad (21) \\
\implies & c_1 g_1(n) \geq \frac{c_1}{max(1, \frac{c_2}{c_3})} max(g_1(n), g_2(n)) \\
\implies & c_1 g_1(n) \geq c_5 max(g_1(n), g_2(n)) \text{ because } c_5 \leq \frac{c_1}{max(1, \frac{c_2}{c_3})} \\
\implies & c_5 max(g_1(n), g_2(n)) \leq c_1 g_1(n) \leq f_1(n) \\
\implies & c_5 max(g_1(n), g_2(n)) \leq f_1(n)
\end{aligned}
$$

$$
\begin{aligned}
& f_1(n) \leq c_2 g_1(n) \leq c_2 max(g_1(n), g_2(n)) \leq c_6 max(g_1(n), g_2(n)) \text{ because } c_6 \geq c_2 \\
\implies & f_1(n) \leq c_6 max(g_1(n), g_2(n)) \qquad (22)
\end{aligned}
$$

Combining above 2 equations, we have

$$c_5 max(g_1(n), g_2(n)) \leq f_1(n) \leq c_6 max(g_1(n), g_2(n)) \qquad (23)$$

By the assumption that $f_1(n) \geq f_2(n)$, we have $f_1(n) = max(f_1(n), f_2(n))$. Therefore, we have shown

$$c_5 max(g_1(n), g_2(n)) \leq max(f_1(n), f_2(n)) \leq c_6 max(g_1(n), g_2(n)) \qquad (24)$$

Case 2. Assume $f_1(n) < f_2(n)$ for some n in the domain $\mathbb{N}$.

Then $f_1(n) \leq f_2(n)$ is also true. We want to show $c_5 max(g_1(n), g_2(n)) \leq max(f_1(n), f_2(n)) \leq c_6 max(g_1(n), g_2(n))$.

Since $n \geq n_3$, then $n \geq n_1$ and $n \geq n_2$ are also satisfied. Therefore, we have $c_1 g_1(n) \leq f_1(n) \leq c_2 g_1(n)$ and $c_3 g_2(n) \leq f_2(n) \leq c_4 g_2(n)$.

Because $c_1 g_1(n) \leq f_1(n)$ and $f_2(n) \leq c_4 g_2(n)$ with the assumption $c_1 g_1(n) \leq c_4 g_2(n)$ is true.

$$
\begin{aligned}
& c_1 g_1(n) \leq c_4 g_2(n) \\
\implies & \frac{c_4}{c_1} g_2(n) \geq g_1(n) \\
\implies & max(1, \frac{c_4}{c_1}) g_2(n) \geq \frac{c_4}{c_1} g_2(n) \geq g_1(n) \\
\implies & max(1, \frac{c_4}{c_1}) g_2(n) \geq g_1(n) \wedge max(1, \frac{c_4}{c_1}) g_2(n) \geq g_2(n) \\
\implies & max(1, \frac{c_4}{c_1}) g_2(n) \geq max(g_1(n), g_2(n)) \qquad (25) \\
\implies & c_3 g_2(n) \geq \frac{c_3}{max(1, \frac{c_4}{c_1})} max(g_1(n), g_2(n)) \\
\implies & c_3 g_2(n) \geq c_5 max(g_1(n), g_2(n)) \text{ because } c_5 \leq \frac{c_3}{max(1, \frac{c_4}{c_1})} \\
\implies & c_5 max(g_1(n), g_2(n)) \leq c_3 g_2(n) \leq f_2(n) \\
\implies & c_5 max(g_1(n), g_2(n)) \leq f_2(n)
\end{aligned}
$$

$$
\begin{aligned}
& f_2(n) \leq c_4 g_2(n) \leq c_4 max(g_1(n), g_2(n)) \leq c_6 max(g_1(n), g_2(n)) \text{ because } c_6 \geq c_4 \\
\implies & f_2(n) \leq c_6 max(g_1(n), g_2(n))
\end{aligned} \qquad (26)
$$

Combining above 2 equations, we have

$$c_5 max(g_1(n), g_2(n)) \leq f_2(n) \leq c_6 max(g_1(n), g_2(n)) \qquad (27)$$

By the assumption that $f_1(n) \leq f_2(n)$, we have $f_1(n) = max(f_1(n), f_2(n))$. Therefore, we have shown

$$c_5 max(g_1(n), g_2(n)) \leq max(f_1(n), f_2(n)) \leq c_6 max(g_1(n), g_2(n)) \qquad (28)$$

Finally, we have shown for both $f_1(n) \geq f_2(n)$ and $f_1(n) < f_2(n)$,

$$c_5 max(g_1(n), g_2(n)) \leq max(f_1(n), f_2(n)) \leq c_6 max(g_1(n), g_2(n)) \qquad (29)$$

is always true. Therefore, we have proved $\forall f_1, f_2, g_1, g_2 : \mathbb{N} \to \mathbb{R}^+, f_1 \in \Theta(g_1) \wedge f_2 \in \Theta(g_2) \implies max(f_1, f_2) \in \Theta(max(g_1, g_2))$ as required.

■

3. *Proof.* The runtime analysis framework for a program with one loop inside another loop is

$$RT_{\text{repeat}}(n) = \text{iteration for outside loop } \times \text{ iteration for inside loop} \tag{30}$$

However, for this program *repeat*, the iterations for inside loop varies as iteration variable i in outside loop changes.

By Quotient-Remainder Theorem, when iteration variable i in outside loop is divided by 3, the possible remainders are $0, 1, 2$.

Therefore, we are going to divide the runtime analysis into three cases by three remainders $0, 1, 2$.

Case 1. Assume the remainder of iteration variable i in outside loop divided by 3 is 0.

In this condition, $range(n**(i\%3)) = range(1)$. Therefore, the inside loop iterates 1 time.

Since the remainder of iteration variable i in outside loop divided by 3 is 0 occurs $\lceil \frac{n}{3} \rceil$ times, the number of iteration under this condition is

$$\begin{aligned} & RT_{\text{repeat only considering } i\%3\,=\,0}(n) \\ =& \text{number of this condition is met} \times \text{iteration for inside loop} \\ =& \left\lceil \frac{n}{3} \right\rceil \times 1 \end{aligned} \tag{31}$$

Case 2. Assume the remainder of iteration variable i in outside loop divided by 3 is 1.

In this condition, $range(n**(i\%3)) = range(n)$. Therefore, the inside loop iterates n time.

Since the remainder of iteration variable i in outside loop divided by 3 is 1 occurs $\lceil \frac{n-1}{3} \rceil$ times, the number of iteration under this condition is

$$\begin{aligned} & RT_{\text{repeat only considering } i\%3\,=\,1}(n) \\ =& \text{number of this condition is met} \times \text{iteration for inside loop} \\ =& \left\lceil \frac{n-1}{3} \right\rceil \times n \end{aligned} \tag{32}$$

Case 3. Assume the remainder of iteration variable i in outside loop divided by 3 is 2.

In this condition, $range(n**(i\%3)) = range(n^2)$. Therefore, the inside loop iterates n^2 time.

Since the remainder of iteration variable i in outside loop divided by 3 is 2 occurs $\lceil \frac{n-2}{3} \rceil$ times, the number of iteration under this condition is

$$\begin{aligned} & RT_{\text{repeat only considering } i\%3\,=\,2}(n) \\ =& \text{number of this condition is met} \times \text{iteration for inside loop} \\ =& \left\lceil \frac{n-2}{3} \right\rceil \times n^2 \end{aligned} \tag{33}$$

Finally, the total runtime of this program is the sum of runtime in above three cases.

$$\begin{aligned} RT_{\text{repeat}}(n) =& RT_{\text{repeat only considering } i\%3=0}(n) + RT_{\text{repeat only considering } i\%3=1}(n) \\ & + RT_{\text{repeat only considering } i\%3=2}(n) + RT_{\text{return}}(n) \\ =& \left\lceil \frac{n}{3} \right\rceil \times 1 + \left\lceil \frac{n-1}{3} \right\rceil \times n + \left\lceil \frac{n-2}{3} \right\rceil \times n^2 + 1 \\ & \text{because } \left\lceil \frac{n}{3} \right\rceil \times 1 \in \Theta(n), \left\lceil \frac{n-1}{3} \right\rceil \times n \in \Theta(n^2), \left\lceil \frac{n-2}{3} \right\rceil \times n^2 \in \Theta(n^3), \\ & \text{Their sum is } \in \Theta(n^3) \end{aligned} \tag{34}$$

Therefore, the runtime of program *repeat* is $\in \Theta(n^3)$.

■

4. (a) Prove $\forall n \in \mathbb{N}, 6 \mid 5^{2n+1} + 1$

Proof. We want to prove $\forall n \in \mathbb{N}, 6 \mid 5^{2n+1} + 1$.

Let P(n) be the statement: 6 divides $5^{2n+1} + 1$. We want to show for all natural number n, P(n) is true by induction.

Base Case. For P(0), $5^{2n+1} + 1 = 5^{2\cdot 0+1} + 1 = 5^1 + 1 = 6 = 6 \cdot 1$, which is equivalent to $6 \mid 5^{2\cdot 0+1} + 1$. Therefore, P(0) is true.

Inductive Step. Let $k \in \mathbb{N}$ and $k \geq 0$. Assume P(k) is true, that is $6 \mid 5^{2k+1} + 1$, which is equivalent to $\exists k_0 \in \mathbb{Z}, 6k_0 = 5^{2k+1} + 1$.

We want to show P(k+1) is also true, that is $6 \mid 5^{2(k+1)+1} + 1$, which is equivalent to $\exists k_1 \in \mathbb{Z}, 6k_1 = 5^{2(k+1)+1} + 1$.

Let $k_1 = 25k_0 - 4$.

$$
\begin{aligned}
& 5^{2(k+1)+1} + 1 \\
=& 5^{2k+1+2} + 1 \\
=& 25 \cdot 5^{2k+1} + 1 \\
=& 25 \cdot (5^{2k+1} + 1 - 1) + 1 \\
=& 25 \cdot (5^{2k+1} + 1) - 25 + 1 \\
=& 25 \cdot (5^{2k+1} + 1) - 24 \\
=& 25 \cdot 6k_0 - 24 \text{ by induction hypothesis } 6k_0 = 5^{2k+1} + 1 \\
=& 6 \cdot (25k_0 - 4) \\
=& 6k_1
\end{aligned}
\tag{35}
$$

Therefore, P(k) is true implies P(k+1) is also true.

Finally, we have shown $\forall n \in \mathbb{N}, 6 \mid 5^{2n+1} + 1$ by induction as required.

■

(b) Prove $\sum_{i=0}^{i=n} \left(\frac{1}{7}\right)^i = \frac{7-\left(\frac{1}{7}\right)^n}{6}$.

Proof. We want to prove

$$\sum_{i=0}^{i=n} \left(\frac{1}{7}\right)^i = \frac{7-\left(\frac{1}{7}\right)^n}{6}$$

by induction.

Let P(n) be the statement: "$\sum_{i=0}^{i=n} \left(\frac{1}{7}\right)^i = \frac{7-\left(\frac{1}{7}\right)^n}{6}$".

Base Case. For P(0), we have

$$\sum_{i=0}^{i=0} \left(\frac{1}{7}\right)^i = \left(\frac{1}{7}\right)^0 = 1 = \frac{6}{6} = \frac{7-1}{6} = \frac{7-\left(\frac{1}{7}\right)^0}{6} \tag{36}$$

Therefore, P(0) is true.

Inductive Step. Let $k \in \mathbb{N}$ and $k \geq 0$. Assume P(k) is true, that is $\sum_{i=0}^{i=k} \left(\frac{1}{7}\right)^i = \frac{7-\left(\frac{1}{7}\right)^k}{6}$.

We want to show P(k+1) is also true, that is $\sum_{i=0}^{i=k+1}\left(\frac{1}{7}\right)^i = \frac{7-\left(\frac{1}{7}\right)^{k+1}}{6}$

$$
\begin{aligned}
&\sum_{i=0}^{i=k+1}\left(\frac{1}{7}\right)^i \\
=&\left(\sum_{i=0}^{i=k}\left(\frac{1}{7}\right)^i\right)+\left(\frac{1}{7}\right)^{k+1} \\
=&\frac{7-\left(\frac{1}{7}\right)^k}{6}+\left(\frac{1}{7}\right)^{k+1} \quad \text{by induction hypothesis } \sum_{i=0}^{i=k}\left(\frac{1}{7}\right)^i = \frac{7-\left(\frac{1}{7}\right)^k}{6} \\
=&\frac{7}{6}-\frac{\left(\frac{1}{7}\right)^k}{6}+\left(\frac{1}{7}\right)^{k+1} \\
=&\frac{7}{6}-\frac{\left(\frac{1}{7}\right)^k}{6}+\frac{1}{7}\cdot\left(\frac{1}{7}\right)^k \\
=&\frac{7}{6}-\frac{1}{6}\cdot\left(\frac{1}{7}\right)^k+\frac{1}{7}\cdot\left(\frac{1}{7}\right)^k \\
=&\frac{7}{6}-\left(\frac{1}{6}-\frac{1}{7}\right)\cdot\left(\frac{1}{7}\right)^k \\
=&\frac{7}{6}-\left(\frac{1}{42}\right)\cdot\left(\frac{1}{7}\right)^k \\
=&\frac{7}{6}-\left(\frac{1}{6}\cdot\frac{1}{7}\right)\cdot\left(\frac{1}{7}\right)^k \\
=&\frac{7}{6}-\left(\frac{1}{6}\right)\cdot\left(\frac{1}{7}\right)^{k+1} \\
=&\frac{7-\left(\frac{1}{7}\right)^{k+1}}{6}
\end{aligned}
\tag{37}
$$

Therefore, P(k) is true implies P(k+1) is also true.

We have shown

$$\sum_{i=0}^{i=n}\left(\frac{1}{7}\right)^i = \frac{7-\left(\frac{1}{7}\right)^n}{6}$$

by induction as required.

■

(c) *Proof.* We want to prove every square can be tiled by m smaller square for all natural number $m \geq 6$.

Lemma 1. *For all natural number n, any square can be tiled by $6 + 3n$ smaller square.*

Proof. Let $P_6(n)$ be the statement: "Any square can be tiled by $6 + 3n$ smaller square."

We are going to prove $\forall n \in \mathbb{N}, P_6(n)$.

Base Case. Let $n = 0$. For $P_6(0)$, a square can be tiled by $6 + 3 \cdot 0 = 6$ smaller squares as the following diagram shows.

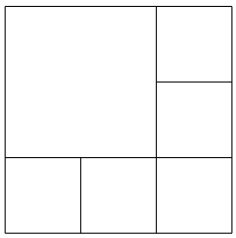

Figure 1: one big square consist of 6 smaller square

Therefore, $P_6(0)$ is true.

Inductive Step. Let $k \in \mathbb{N}$ and $k \geq 0$. Assume $P_6(k)$ is true, that is a square can be tiled by $6 + 3 \cdot k$ smaller squares.

We want to show that $P_6(k + 1)$ is true, that is a square can be tiled by $6 + 3 \cdot (k + 1)$ smaller squares.

By induction hypothesis, at least one arrangement of $6 + 3 \cdot k$ small squares that constructs a big square exist as a square can be tiled by $6 + 3 \cdot k$ smaller squares. We choose any one small square from the one possible arrangement of $P_6(k)$.

Let k_0 be the side length of this small square. We are going to replace this square with 4 smaller squares which has a side length of $\frac{k_0}{2}$ arranged as two per row.

The area of 1 smaller squares is $(\frac{k_0}{2})^2 = \frac{k_0^2}{4}$. Therefore, the area of 4 smaller squares is $4\frac{k_0^2}{4} = k_0^2$, which is the same as the area of original square. The side length of 1 smaller squares is $\frac{k_0}{2}$. Therefore, the side length of 2 smaller squares is $2\frac{k_0}{2} = k_0$, which is the same as the side length of original square.

After replacing the original square with 4 smaller squares described above, the number of small squares consisting of big square become $6 + 3 \cdot k - 1 + 4 = 6 + 3 \cdot (k + 1)$, which implies $P_6(k + 1)$ is also true.

Hence, we have proved the lemma that for all natural number n, any square can be tiled by $6 + 3n$ smaller square.

■

Lemma 2. *For all natural number n, any square can be tiled by $7 + 3n$ smaller square.*

Proof. Let $P_7(n)$ be the statement: "Any square can be tiled by $7 + 3n$ smaller square."

We are going to prove $\forall n \in \mathbb{N}, P_7(n)$.

Base Case. Let $n = 0$. For $P_7(0)$, a square can be tiled by $7 + 3 \cdot 0 = 7$ smaller squares as the following diagram shows.

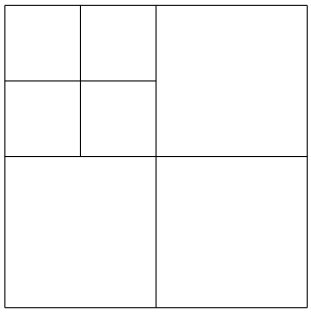

Figure 2: one big square consist of 7 smaller square

Therefore, $P_7(0)$ is true.

Inductive Step. Let $k \in \mathbb{N}$ and $k \geq 0$. Assume $P_7(k)$ is true, that is a square can be tiled by $7 + 3 \cdot k$ smaller squares.

We want to show that $P_7(k + 1)$ is true, that is a square can be tiled by $7 + 3 \cdot (k + 1)$ smaller squares.

By induction hypothesis, at least one arrangement of $7 + 3 \cdot k$ small squares that constructs a big square exist as a square can be tiled by $7 + 3 \cdot k$ smaller squares. We choose any one small square from the one possible arrangement of $P_7(k)$.

Let k_0 be the side length of this small square. We are going to replace this square with 4 smaller squares which has a side length of $\frac{k_0}{2}$ arranged as two per row.

The area of 1 smaller squares is $(\frac{k_0}{2})^2 = \frac{k_0^2}{4}$. Therefore, the area of 4 smaller squares is $4\frac{k_0^2}{4} = k_0^2$, which is the same as the area of original square. The side length of 1 smaller squares is $\frac{k_0}{2}$. Therefore, the side length of 2 smaller squares is $2\frac{k_0}{2} = k_0$, which is the same as the side length of original square.

After replacing the original square with 4 smaller squares described above, the number of small squares consisting of big square become $7 + 3 \cdot k - 1 + 4 = 7 + 3 \cdot (k + 1)$, which implies $P_7(k + 1)$ is also true.

Hence, we have proved the lemma that for all natural number n, any square can be tiled by $7 + 3n$ smaller square.

■

Lemma 3. *For all natural number n, any square can be tiled by* $8 + 3n$ *smaller square.*

Proof. Let $P_8(n)$ be the statement: "Any square can be tiled by $8 + 3n$ smaller square."

We are going to prove $\forall n \in \mathbb{N}, P_8(n)$.

Base Case. Let $n = 0$. For $P_8(0)$, a square can be tiled by $8 + 3 \cdot 0 = 8$ smaller squares as the following diagram shows.

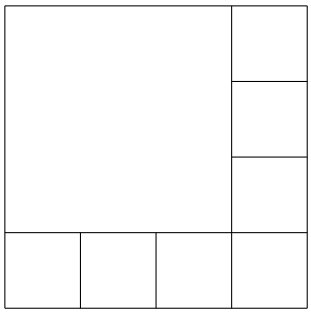

Figure 3: one big square consist of 8 smaller square

Therefore, $P_8(0)$ is true.

Inductive Step. Let $k \in \mathbb{N}$ and $k \geq 0$. Assume $P_8(k)$ is true, that is a square can be tiled by $8 + 3 \cdot k$ smaller squares.

We want to show that $P_8(k + 1)$ is true, that is a square can be tiled by $8 + 3 \cdot (k + 1)$ smaller squares.

By induction hypothesis, at least one arrangement of $8 + 3 \cdot k$ small squares that constructs a big square exist as a square can be tiled by $8 + 3 \cdot k$ smaller squares. We choose any one small square from the one possible arrangement of $P_8(k)$.

Let k_0 be the side length of this small square. We are going to replace this square with 4 smaller squares which has a side length of $\frac{k_0}{2}$ arranged as two per row.

The area of 1 smaller squares is $(\frac{k_0}{2})^2 = \frac{k_0^2}{4}$. Therefore, the area of 4 smaller squares is

$4\frac{k_0^2}{4} = k_0^2$, which is the same as the area of original square. The side length of 1 smaller squares is $\frac{k_0}{2}$. Therefore, the side length of 2 smaller squares is $2\frac{k_0}{2} = k_0$, which is the same as the side length of original square.

After replacing the original square with 4 smaller squares described above, the number of small squares consisting of big square become $8 + 3 \cdot k - 1 + 4 = 8 + 3 \cdot (k + 1)$, which implies $P_8(k + 1)$ is also true.

Hence, we have proved the lemma that for all natural number n, any square can be tiled by $8 + 3n$ smaller square.

■

Let $m \in \mathbb{N}$. Assume $n \geq 6$. By Quotient-Remainder Theorem, when m is divided by 3, the remainder can be $0, 1, 2$. We divide our proof into 3 cases by the remainder.

Case 1. We want to show any square can be tiled by m smaller square, when the remainder of m divided by 3 is 0, that is $\exists k \in \mathbb{Z}, m = 3k + 0$.

Because $m \geq 6$, we have $\exists k \in \mathbb{Z}, k \geq 0 \wedge m = 3k + 0 + 6$ is also true.

By Lemma 1, any square can be tiled by $6 + 3n$ smaller square for natural number n. By $k \in \mathbb{N}, m = 6 + 3k$, we conclude any square can be tiled by m smaller square when the remainder of m divided by 3 is 0.

Case 2. We want to show any square can be tiled by m smaller square, when the remainder of m divided by 3 is 1, that is $\exists k \in \mathbb{Z}, m = 3k + 1$.

Because $m \geq 6$, we have $\exists k \in \mathbb{Z}, k \geq 0 \wedge m = 3k + 1 + 6$ is also true.

By Lemma 2, any square can be tiled by $7 + 3n$ smaller square for natural number n. By $k \in \mathbb{N}, m = 7 + 3k$, we conclude any square can be tiled by m smaller square when the remainder of m divided by 3 is 1.

Case 3. We want to show any square can be tiled by m smaller square, when the remainder of m divided by 3 is 2, that is $\exists k \in \mathbb{Z}, m = 3k + 2$.

Because $m \geq 6$, we have $\exists k \in \mathbb{Z}, k \geq 0 \wedge m = 3k + 2 + 6$ is also true.

By Lemma 3, any square can be tiled by $8 + 3n$ smaller square for natural number n. By $k \in \mathbb{N}, m = 8 + 3k$, we conclude any square can be tiled by m smaller square when the remainder of m divided by 3 is 2.

We have proved every square can be tiled by m smaller square for all natural number $m \geq 6$ as required.

■