CSC165H1 Problem Set 3 (due 11/15/17)

Jacob Nazarenko, James Currier, Mark Abdullah

November 15, 2017

1. For all of the proofs in 1,

   Let $a : \mathbb{N} \mapsto \mathbb{Z}$. Denote $a(n) = a_n$, and a is identified with the sequence a_0, a_1, a_2,.....
   Let $S = \{f | f : \mathbb{N} \mapsto \mathbb{Z}\}$ be the set of integer sequences.

   (a) **Proof. (by mathematical induction)**

   Assume Theorem 2.18,

   $$\forall a, b, c, n \in \mathbb{Z}, n \neq 0, a \equiv c \mod n \wedge b \equiv d \mod n \implies ab \equiv cd \mod n$$

   Let m be a non zero integer
   Let $a, b \in S$ be arbitrary integer sequences

   Base case:

   Let n = 1

   Assume $\forall k \leq n, a_k \equiv b_k \mod m$

   Then, $a_0 \equiv b_0 \mod m \wedge a_1 \equiv b_1 \mod m$

   Using Theorem 2.18,

   $$a_0 * b_0 \equiv a_1 * b_1 \mod m$$
   $$\prod_{k=0}^{k=1} a_k \equiv \prod_{k=0}^{k=1} b_k \mod m$$
   $$\prod_{k=0}^{k=n} a_k \equiv \prod_{k=0}^{k=n} b_k \mod m$$

   So the statement is true for n = 1

   Inductive step:

   Let $q \in \mathbb{N}$

   Assume $(\forall k \leq q, a_k \equiv b_k \mod m) \implies \prod_{k=0}^{k=q} a_k \equiv \prod_{k=0}^{k=q} b_k \mod m$

WTS $(\forall k \leq q+1, a_k \equiv b_k \mod m) \implies \prod_{k=0}^{k=q+1} a_k \equiv \prod_{k=0}^{k=q+1} b_k \mod m$

Assume $\forall k \leq q+1, a_k \equiv b_k \mod m$

By this assumption,

$$a_{q+1} \equiv b_{q+1} \mod m$$

Also, since $q \leq q+1$,

$$\forall k \leq q, a_k \equiv b_k \mod m$$

Then, by our inductive hypothesis,

$$\prod_{k=0}^{k=q} a_k \equiv \prod_{k=0}^{k=q} b_k \mod m$$

Using Theorem 2.18,

$$\left(\prod_{k=0}^{k=q} a_k\right) * a_{q+1} \equiv \left(\prod_{k=0}^{k=q} b_k\right) * b_{q+1} \mod m$$

Then,

$$\prod_{k=0}^{k=q+1} a_k \equiv \prod_{k=0}^{k=q+1} b_k \mod m$$

Therefore, by induction, we have proven the theorem true. ■

(b) **Proof. (by mathematical induction)**

Let $d \in \mathbb{N}$
Let b be an integer sequence with $b_m > 0$, for all $m \in \mathbb{N}$

Base case:

Let $n = 0$

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

WTS $d \nmid \prod_{i=0}^{i=n} b_i$

Since 0 is the only natural number $\leq n$, we know that the if part of our assumption only true when $i = 0$.

We know that $\gcd(d, b_0) = 1$, so,

$$d \nmid b_0$$

$$d \nmid \prod_{i=0}^{i=0} b_i$$

$$d \nmid \prod_{i=0}^{i=n} b_i$$

So the theorem holds true for $n = 0$

Inductive step:

Let $k \in \mathbb{N}$

Assume PS2 #2(g),

$$(\gcd(a, b) = 1 \wedge a \mid bc) \implies a \mid c$$

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

WTS $(\forall i \in \mathbb{N}, i \leq k+1 \implies gcd(d, b_i) = 1) \implies d \nmid \prod_{i=0}^{i=k+1} b_i$

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

Since $k \leq k+1$, we know $\forall i \in \mathbb{N}, i \leq k \implies gcd(d, b_i) = 1$

Then, by our inductive hypothesis,

$$d \nmid \prod_{i=0}^{i=k} b_i$$

By PS2 #2(g), we know that

$$\left(\gcd(d, b_{k+1}) = 1 \wedge d \mid b_{k+1} * \prod_{i=0}^{i=k} b_i \right) \implies d \mid \prod_{i=0}^{i=k} b_i$$

$$d \nmid \prod_{i=0}^{i=k} b_i \implies \neg \left(\gcd(d, b_{k+1}) = 1 \wedge d \mid b_{k+1} * \prod_{i=0}^{i=k} b_i \right)$$

$$d \nmid \prod_{i=0}^{i=k} b_i \implies \left(\gcd(d, b_{k+1}) \neq 1 \vee d \nmid b_{k+1} * \prod_{i=0}^{i=k} b_i \right)$$

$$d \nmid \prod_{i=0}^{i=k} b_i \implies \left(\gcd(d, b_{k+1}) = 1 \implies d \nmid b_{k+1} * \prod_{i=0}^{i=k} b_i \right)$$

We know that $d \nmid \prod_{i=0}^{i=k} b_i$, So,

$$\gcd(d, b_{k+1}) = 1 \implies d \nmid b_{k+1} * \prod_{i=0}^{i=k} b_i$$

Since we know that $\forall i \in \mathbb{N}, i \leq k+1 \implies gcd(d, b_i) = 1$,

$$\Big(\forall i \in \mathbb{N}, i \leq k+1 \implies gcd(d, b_i) = 1 \Big) \implies d \nmid b_{k+1} * \prod_{i=0}^{i=k} b_i$$

$$\Big(\forall i \in \mathbb{N}, i \leq k+1 \implies gcd(d, b_i) = 1 \Big) \implies d \nmid \prod_{i=0}^{i=k+1} b_i$$

Therefore, by induction, we have proven the theorem true. ■

(c) **Proof. (by mathematical induction)**

Base case:

$$\sum_{j=(2)+1}^{j=2(2)} \frac{1}{j} = \sum_{j=3}^{j=4} \frac{1}{j} = \frac{1}{3} + \frac{1}{4} = \frac{7}{12} > \frac{13}{24}$$

So the theorem holds true for n = 2

Inductive step:

Let $k \in \mathbb{N}$. Assume $k \geq 2$

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

WTS $\sum_{j=(k+1)+1}^{j=2(k+1)} \frac{1}{j} > \frac{13}{24}$

Since $k \geq 2 > -1$,

$$k > -1$$

$$7k > 6k - 1$$

$$7k + 3 > 6k + 2$$

$$4k^2 + 7k + 3 > 4k^2 + 6k + 2$$

$$\frac{4k^2 + 7k + 3}{4k^2 + 6k + 2} > 1$$

$$\frac{(4k + 3)(k + 1)}{(2k + 1)(2k + 2)} > 1$$

$$\frac{4k + 3}{(2k + 1)(2k + 2)} > \frac{1}{k + 1}$$

$$\frac{2k + 2 + 2k + 1}{(2k + 1)(2k + 2)} > \frac{1}{k + 1}$$

$$\frac{2k + 2}{(2k + 1)(2k + 2)} + \frac{2k + 1}{(2k + 1)(2k + 2)} > \frac{1}{k + 1}$$

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

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

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

By our inductive hypothesis,

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

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

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

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

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

Therefore, by induction, we have proven the theorem true. ■

(d) **Proof. (by mathematical induction)**

Define integer sequence $c \in S$ by

$$\begin{cases} 0, & \text{if } n = 0 \\ c_{n-1} + 3n^2 - 3n + 1, & \text{if } n > 0 \end{cases}$$

Base cases:

$c_0 = 0 = 0^3$
$c_1 = c_0 + 3(1)^2 - 3(1) + 1 = 0 + 3 - 3 + 1 = 1 = 1^3$

So the theorem holds true for n = 0 and n = 1

Inductive step:

Let $k \in \mathbb{N}$. Assume $k \geq 1$

Assume $c_k = k^3$
WTS $c_k + 1 = (k+1)^3$

By our inductive hypothesis,

$$\begin{aligned} c_k &= k^3 \\ c_k + 3k^2 - 3k^2 + 6k - 6k + 4 - 4 &= k^3 \\ c_k + 3k^2 - 3k^2 + 6k - 3k - 3k + 3 + 1 - 3 - 1 &= k^3 \\ c_k + 3k^2 + 6k + 3 - 3k - 3 + 1 &= k^3 + 3k^2 + 3k + 1 \\ c_k + 3(k+1)^2 - 3(k+1) + 1 &= (k+1)^3 \end{aligned}$$

Since $k \geq 1$,

$$c_{k+1} = c_k + 3(k+1)^2 - 3(k+1) + 1$$

So,

$$c_{k+1} = (k+1)^3$$

Therefore, by induction, we have proven the theorem true. ■

2. (a) **Claim:**

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

$$\forall n \in \mathbb{N},\ P(n)$$

Proof. (by mathematical induction)

We will have three base cases - one where $n = 0$ and therefore k can only equal n, one where $n = 1$ and therefore k can be either 0 or n, and one where $n = 2$, and therefore k can be 0, n, or 1, a number that is neither n nor 0.

Base case #1: $n = 0,\ k = 0$

$$\binom{0}{0} = \frac{0!}{0!0!} = \frac{1}{1} = 1$$

There is only 1 set of size 0 that can be made from an empty set, and that is the empty subset, so this statement holds.

Base case #2: $n = 1,\ k = 0, n$

$$\text{If } k = 0, \quad \binom{1}{0} = \frac{1!}{0!1!} = \frac{1}{1} = 1$$

$$\text{If } k = 1, \quad \binom{1}{1} = \frac{1!}{1!0!} = \frac{1}{1} = 1$$

There is only 1 set of size 0 that can be made from a set of 1, which is again the empty set, and one can notice that this is true for any set. That is, if $k = 0$, then then the expression will always evaluate to 1, as there is always only 1 way to make an empty subset. This can also be proven with the expression:

$$\text{If } k = 0, \quad \binom{n}{0} = \frac{n!}{0!n!} = \frac{n!}{n!} = 1$$

Similarly, there is also only 1 way of making a set of size 1, because $n = 1$ in this case. In fact, we can prove that there is always 1 way to make a subset of size n out of a set of size n with the expression:

$$\text{If } k = n, \quad \binom{n}{n} = \frac{n!}{n!0!} = \frac{n!}{n!} = 1$$

Therefore, both of the situations above must make the expression hold, and therefore our second base case holds.

Base case #3: $n = 2,\ k = 0, 1, n$

For this case, we already know that $k = 0$ and $k = n$ hold true by the above statements. We only need to check that $k = 1$ holds. Logically, we know that there are exactly 2 ways to get subsets of size 1 out of a set of size 2. By the expression,

$$\binom{2}{1} = \frac{2!}{1!1!} = \frac{2}{1} = 2$$

So we know that this statement holds true. We may now proceed to the inductive step.

Inductive step: Let x be an arbitrary, fixed natural number. Assume $P(x)$, that is,

$$\forall y \in \mathbb{N},\ y \leq x \Rightarrow \binom{x}{y} = \frac{x!}{y!(x-y)!}$$

We must prove that $P(x+1)$ follows, that is,

$$\forall y \in \mathbb{N},\ y \leq x \Rightarrow \binom{x+1}{y} = \frac{(x+1)!}{y!(x+1-y)!}$$

For the remainder of this proof, let y be an arbitrary natural number no greater than x. In order to prove the above implication, we must first consider several situations related to $P(x)$. First consider $P(x)$ itself. By our inductive hypothesis, we have that

$$\binom{x}{y} = \frac{x!}{y!(x-y)!}$$

This is the number of ways to make unique subsets of size y out of a set of size x. Next, consider the same situation, but with subsets of size $y-1$. Again, by our inductive hypothesis, we have that

$$\binom{x}{y-1} = \frac{x!}{(y-1)!(x-y+1)!}$$

This is the number of ways to make unique subsets of size $y-1$ out of a set of size x. Now, consider the situation where we must make unique subsets of size y out a set of size $x+1$. This would be like taking all of the subsets from a set of size x, and combining them with all possible subsets containing the extra added element. We already know the result of the former from the first situation above. The latter, however, can be thought of as the number of all possible unique subsets of size y where 1 of the elements will always be the extra added element, which comes out to be the number of all possible subsets of size $y-1$ (as one of the spots in each subset of size y will already be taken). This is the result of the second situation above. Hence, this total may be expressed as the sum of the two situations described, as follows:

$$\binom{x+1}{y} = \binom{x}{y} + \binom{x}{y-1}$$

$$= \frac{x!}{y!(x-y)!} + \frac{x!}{(y-1)!(x-y+1)!}$$

$$= \frac{x!(x-y+1)}{y!(x-y)!(x-y+1)} + \frac{x!(y)}{(y-1)!(x-y+1)!(y)}$$

$$= \frac{x!(x-y+1)}{y!(x-y+1)!} + \frac{x!(y)}{y!(x-y+1)!}$$

$$= \frac{x!(x-y+1)+x!(y)}{y!(x-y+1)!}$$

$$= \frac{x!(x+1)}{y!(x-y+1)!}$$

$$= \frac{(x+1)!}{y!(x+1-y)!}$$

We have therefore proven the implication. ■

(b)

$$DTP_2 = \{\{\emptyset, \{1,2\}\},\ \{\{1\},\{2\}\}\}$$
$$DTP_3 = \{\{\emptyset, \{1,2,3\}\},\ \{\{1\},\{2,3\}\},\ \{\{1,3\},\{2\}\},\ \{\{1,2\},\{3\}\}\}$$

(c)

$$|DTP_n| = 2^{n-1} \quad \text{or} \quad |DTP_n| = 1 \ \text{ if } \ n = 0$$

Claim[1]**:**

$$P(n) : |DTP_n| = 2^{n-1}$$
$$\forall n \in \mathbb{N}^+,\ P(n)$$

Proof (by mathematical induction):

Base cases: Let the base cases be the one defined in the problem instructions for $n = 1$, as well as the two above for $n = 2$ and $n = 3$. We see that in all three cases, the predicate holds. For $n = 1$, $|DTP_1| = 2^{1-1} = 1$. For $n = 2$, $|DTP_2| = 2^{2-1} = 2$. And for $n = 3$, $|DTP_3| = 2^{3-1} = 4$.

Inductive step: Let k be an arbitrary natural number greater than 0. Assume $P(k)$, that is,

$$|DTP_k| = 2^{k-1}$$

We must show that $P(k+1)$ follows, that is,

$$|DTP_{k+1}| = 2^k$$

[1]The claim will only work for $n > 0$, but the case for $n = 0$ is defined in the original function

We know the expression for $|DTP_k|$ from our inductive hypothesis above, and we can consider the fact that if one more number is added to the set S, then this number can be added into one of the two disjoint set partitions in every set of disjoint partitions for k elements. Therefore, every set in the solution for k elements will yield two new sets in the solution for $k+1$, and we will therefore have that the number of sets in the solution for k elements may be mutliplied by 2 to obtain the number of sets in the solution for $k+1$ elements:

$$\begin{aligned} |DTP_{k+1}| &= 2 * |DTP_k| \\ &= 2 * 2^{k-1} \qquad \text{(by our inductive hypothesis)} \\ &= 2^k \end{aligned}$$

We have thereby proven our expression for $|DTP_n|$. ■

3. (a) We want to show that

$$\forall f \in \{g \mid g : N \to \mathbb{R}^{\geq 0}\}, (\exists n_o \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_o \implies f(n) \geq 1) \implies \lfloor f \rfloor \in \theta(f) \wedge \lceil f \rceil \in \theta(f)$$

Proof:
Let f be a function such that $f : \mathbb{N} \to \mathbb{R}^{\geq 0}$
Assume $\exists n_o \in \mathbb{N}, \forall n \in \mathbb{N}, n \geq n_o \implies f(n) \geq 1$
Want to show $\lfloor f \rfloor \in \theta(f)$ and $\lceil f \rceil \in \theta(f)$

We will first prove $\lfloor f \rfloor \in \theta(f)$. We will start by expanding the definition,

$$\lfloor f \rfloor \in \theta(f) : \exists c_1, c_2, n_1 \in \mathbb{R}^+, \forall x \in \mathbb{N}, x \geq n_1 \implies c_1 \cdot f(x) \leq \lfloor f(x) \rfloor \leq c_2 \cdot f(x)$$

Take $c_1 = 0.5$
Take $c_2 = 1$
Take $n_1 = n_o$
Let $x \in \mathbb{N}$
Assume $x \geq n_1$
Want to show $(c_1 \cdot f(x) \leq \lfloor f(x) \rfloor)$ and $(\lfloor f(x) \rfloor \leq c_2 \cdot f(x))$

To show $(c_1 \cdot f(x) \leq \lfloor f(x) \rfloor)$, we will split it up into 2 cases.
By our hypothesis, we know $f(x) \geq 1$ since $x \geq n_1$
Case 1: Assume $1 \leq f(x) < 2$

$$\begin{aligned} f(x) &< 2 \\ 0.5 \cdot f(x) &< 1 = \lfloor f(x) \rfloor \\ 0.5 \cdot f(x) &< \lfloor f(x) \rfloor \end{aligned}$$

Case 2: Assume $2 \leq f(x)$
The difference between $f(x)$ and $0.5 \cdot f(x)$ is atleast 1. The difference between $f(x)$ and $\lfloor f(x) \rfloor$ must be less than 1 by the defintion of floor.

$$\begin{aligned} f(x) - \lfloor f(x) \rfloor &< 1 \leq f(x) - (0.5 \cdot f(x)) \\ f(x) - \lfloor f(x) \rfloor &< f(x) - (0.5 \cdot f(x)) \\ -\lfloor f(x) \rfloor &< -(0.5 \cdot f(x)) \end{aligned}$$

$$\lfloor f(x) \rfloor > 0.5 \cdot f(x)$$

By the defintion of floor, the floor of $f(x)$ is the greatest integer less than or equal to $f(x)$.
Thus $(\lfloor f(x) \rfloor \leq 1 \cdot f(x))$.

We've shown $(c_1 \cdot f(x) \leq \lfloor f(x) \rfloor)$ and $(\lfloor f(x) \rfloor \leq c_2 \cdot f(x))$ and thus $\lfloor f \rfloor \in \theta(f)$.

Secondly, we will prove $\lceil f \rceil \in \theta(f)$. We will start by expanding the definition,

$$\lceil f \rceil \in \theta(f) : \exists c_1, c_2, n_2 \in \mathbb{R}^+, \forall x \in \mathbb{N}, x \geq n_2 \implies c_1 \cdot f(x) \leq \lceil f(x) \rceil \leq c_2 \cdot f(x)$$

Take $c_1 = 1$
Take $c_2 = 2$
Take $n_2 = n_0$
Let $x \in \mathbb{N}$
Assume $x \geq n_2$
Want to show $(c_1 \cdot f(x) \leq \lceil f(x) \rceil)$ and $(\lceil f(x) \rceil \leq c_2 \cdot f(x))$

By the defintion of ceiling, the ceiling of $f(x)$ is the least integer greater than or equal to $f(x)$.
Thus $(1 \cdot f(x) \leq \lceil f(x) \rceil)$

The difference between $\lceil f(x) \rceil$ and $f(x)$ must be less than 1 by the definition of floor. By our hypothesis, we know $f(x) \geq 1$ since $x \geq n_2$, therefore we know the difference between $f(x)$ and $2 \cdot f(x)$ is atleast 1.

$$\begin{aligned} \lceil f(x) \rceil - f(x) &< 1 \leq 2 \cdot f(x) - f(x) \\ \lceil f(x) \rceil - f(x) &< 2 \cdot f(x) - f(x) \\ \lceil f(x) \rceil &< 2 \cdot f(x) \\ \lceil f(x) \rceil &\leq 2 \cdot f(x) \end{aligned}$$

We've shown $(c_1 \cdot f(x) \leq \lceil f(x) \rceil)$ and $(\lceil f(x) \rceil \leq c_2 \cdot f(x))$ and thus $\lceil f \rceil \in \theta(f)$.
To conclude, we've shown $\lfloor f \rfloor \in \theta(f)$ and $\lceil f \rceil \in \theta(f)$, proving the original statement true. ■

(b) We want to show that

$$\forall a, b, \in \mathbb{R}^+, (b > a \wedge a > 1) \implies b^n \notin O(a^n)$$

Proof:
Let $a, b \in \mathbb{R}^+$
Assume $b > a \wedge a > 1$
WTS $b^n \notin O(a^n)$ such that

$$\forall c, n_o \in \mathbb{R}^+, \exists n \in \mathbb{N}, (n \geq n_o) \wedge (c \cdot a^n < b^n)$$

Let $c, n_o \in \mathbb{R}^+$
Take $n = \frac{\log c}{\log b - \log a} + n_o$
Step 1, we will prove $n \geq n_o$

$n_0 = n_0$

$n_0 \leq n_0 + \dfrac{\log c}{\log b - \log a}$ (Since $b > a$, we made right side bigger by adding a positive fraction)

$n_0 \leq n$

Step 2, we will prove $c \cdot a^n < b^n$

$$
\begin{aligned}
n &= \frac{\log c}{\log b - \log a} + n_0 \\
n &> \frac{\log c}{\log b - \log a} && \text{(made right side smaller)} \\
n \cdot (\log b - \log a) &> \log c && \text{(Since } b > a, \log b - \log a \text{ is positive)} \\
\log b^n - \log a^n &> \log c \\
\log b^n &> \log c + \log a^n \\
\log b^n &> \log(c \cdot a^n) \\
b^n &> c \cdot a^n
\end{aligned}
$$

We've proven $b^n \notin O(a^n)$ ■

(c) We want to show that $RT_{xgcd} \in O(logn)$.
Proof:
Assume $n, m \in \mathbb{N}$
We will split the proof into three cases.

Case 1: $n > m$
Let r_n^i be r_n after i iterations.

Before loop (when $i = 0$):
$r_0^0 = n$
$r_1^0 = m$

First Iteration (when $i = 1$):
quotient $= \lfloor r_0^0 / r_1^0 \rfloor$
$r_0^1 = r_1^0 = m$
$r_1^1 = r_0^0 - \lfloor r_0^0 / r_1^0 \rfloor * r_1^0 = n - \lfloor n/m \rfloor * m$

Second Iteration (when $i = 2$):
quotient $= \lfloor r_0^1 / r_1^1 \rfloor$
$r_0^2 = r_1^1 = n - \lfloor n/m \rfloor * m$
$r_1^2 = r_0^1 - \lfloor r_0^1 / r_1^1 \rfloor * r_1^1$

We want to show that r_0^2 is atleast less than half of $r_0^0 = n$:

$$r_0^2 = n - \lfloor n/m \rfloor * m \leq \frac{1}{2} * n$$

We will further split this case up into 2 cases. Let q $= \frac{n}{m}$
Case A: $q \geq 2$

$$
\begin{aligned}
q &> 2\epsilon \quad \text{where } 0 \leq \epsilon < 1 \\
-q &< -2\epsilon
\end{aligned}
$$

$$
\begin{aligned}
q &< 2q - 2\epsilon \\
q &< 2(q - \epsilon) \\
q/2 &< \lfloor q \rfloor
\end{aligned}
$$

Case B: $1 < q < 2$
We know that in this range, the floor of q must be 1, $\lfloor q \rfloor = 1$.
We also get that $q/2 < 1$.

$$
\begin{aligned}
q/2 &< 1 = \lfloor q \rfloor \\
q/2 &< \lfloor q \rfloor
\end{aligned}
$$

In both cases A and B, we derive the result $q/2 < \lfloor q \rfloor$. Replacing q with $\frac{n}{m}$,

$$
\begin{aligned}
\frac{n/m}{2} &< \lfloor n/m \rfloor \\
\frac{n/m}{2} * m &< \lfloor n/m \rfloor * m \\
\frac{n}{2} &< \lfloor n/m \rfloor * m
\end{aligned}
$$

Rearranging r_0^2,

$$
\begin{aligned}
r_0^2 &= n - \lfloor n/m \rfloor * m \\
\lfloor n/m \rfloor * m &= n - r_0^2
\end{aligned}
$$

Combining this and our derivation,

$$
\begin{aligned}
\frac{n}{2} &< \lfloor n/m \rfloor * m = n - r_0^2 \\
\frac{n}{2} &< n - r_0^2 \\
r_0^2 &< n - \frac{n}{2} \\
r_0^2 &< \frac{n}{2}
\end{aligned}
$$

We've shown that r_0^2 is atleast less than half of $r_0^0 = n$

Case 2: $n < m$
Let r_n^i be r_n after i iterations.

Before loop (when $i = 0$):
$r_0^0 = n$
$r_1^0 = m$

First Iteration (when $i = 1$):
Since $n < m$, we know $(n/m) < 1$ and hence the floor of (n/m) will be 0.

quotient $= \lfloor r_0^0 / r_1^0 \rfloor = 0$
$r_0^1 = r_1^0 = m$
$r_1^1 = r_0^0 - \lfloor r_0^0 / r_1^0 \rfloor * r_1^0 = n - 0 * m = n$

Notice after the first iteration r_0^1 and r_1^1 switched values. Now we have that $r_0^1 > r_1^1$. With this, we can now use the body of Case 1 to show that r_0^1 will he halved atleast every second iteration, however there will an additional step in switching the values.

Case 3: $n = m$
Let r_n^i be r_n after i iterations.

$r_0^0 = n$
$r_1^0 = m$

First Iteration (when $i = 1$):
quotient $= \lfloor r_0^0 / r_1^0 \rfloor = 1$
$r_0^1 = r_1^0 = m$
$r_1^1 = r_0^0 - \lfloor r_0^0 / r_1^0 \rfloor * r_1^0 = n - 1 * m = 0$

Then in this case, r_1 becomes 0 after the first iteration.

Now that we've shown in cases 1 and 2 that every two iterations r_0 is being reduced by atleast half, we see the same applies to r_1 as it is set equal to the previous r_0 every iteration. Then every second iteration we have a reducton of atleast $0.5 * r_1$,

$$r_1 = r_1 * 0.5$$

Then the maximum number of iterations until we exit the loop is $log_2(n)$ times 2 since it only halves atleast every second iteration, plus some constant number of iterations, c (ie: first iteration and last iteration). Then an upper bound on the run time of xgcd is $[c + 2 * log_2(n)] \in O(log\ n)$

Therefore we've proven $RT_{xgcd} \in O(log\ n)$ ■