This assignment covers some basic big-$O$ concepts, modular arithmetic and RSA (ch. 4.1-4.4, 4.6) and induction (ch 5.1-5.4). Optional reading: Doctor Who S09E11: Heaven Sent. Cite any conversations that have contributed to your solutions and turn in only work that you understand and have written up yourself.

1. (Optional) Run the Euclidean gcd algorithm to compute the GCD of 222 and 2016. Show all your work.

Solution:

2. (12 points) Answer the following questions related to “Big-O” computational complexity. For each, you must use the definition of “Big-O”. Show all your work.

(a) Show that $(n + 1)^5$ is $O(n^5)$
(b) Show that $O(\max\{f(n), g(n)\}) = O(f(n) + g(n))$.
(c) Show that if $d(n)$ is $O(f(n))$ and $e(n)$ is $O(g(n))$, then the product $d(n)e(n)$ is $O(f(n)g(n))$

Solution:

3. (20 points) Compute, by hand, the value of the following expressions. Give the smallest positive value for each answer. Show all your work, but try to do as little work as possible:

Solution:

(a) $344 \mod 5 =$
(b) $-344 + 3230 \mod 5 =$
(c) $58^{73} \mod 7 =$
(d) $(16)^{1271} \mod 17 =$
(e) $(65^{4321}) \mod 77 =$ (hint: use the Chinese Remainder Theorem)

4. (10 points) Prove that $5^{2017} + 2^{2017}$ isn’t prime by finding a prime factor.

Solution:
5. (15 points) Suppose that for positive integers $a$ and $b$, we have $\gcd(a, b) = d$. What is $\gcd(a/d, b/d)$? Give a formal proof of this fact.

**Solution:**

6. (EXAMPLE) For positive integer $n$, find a simple formula for $\sum_{i=1}^{n} \frac{1}{2^i} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots + \frac{1}{2^n}$, and prove it.

**Solution:** Claim: $\sum_{i=1}^{n} \frac{1}{2^i} = 1 - \frac{1}{2^n}$.

We prove this by induction.

Basis Step: for $n = 1$, $\frac{1}{2} = 1 - \frac{1}{2}$ as desired.

Inductive Step: For a fixed $n \geq 1$, assume that $\sum_{i=1}^{n} \frac{1}{2^i} = 1 - \frac{1}{2^n}$.

Then,

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

(Expand the sum)

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

(Inductive Hypothesis)

$$= 1 - \left( \frac{1}{2^n} - \frac{1}{2^n} \right)$$

(Algebra)

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

(Simplification)

Thus $\sum_{i=1}^{n+1} \frac{1}{2^i} = 1 - \frac{1}{2^{n+1}}$. This concludes the inductive step.

Therefore, we conclude by induction that $\sum_{i=1}^{n} \frac{1}{2^i} = 1 - \frac{1}{2^n}$ for all positive $n$.

7. (EXAMPLE) Show by induction that the number of distinct 2 element subsets of an $n$ element set is $\frac{n(n-1)}{2}$ for $n \geq 2$.

**Solution:** Basis Step: for $n = 2$, there is only one 2-element subset of a 2-element set. Also, $\frac{2(2-1)}{2} = 1$ as desired.

Inductive Step: Say that the claim is true for a fixed $n$. Consider a set $A$ with $n + 1$ elements. Let those elements be referred to as $a_1, a_2, \ldots, a_{n+1}$. We separate the 2-element subsets of $A$ into two groups.

- The set of 2-element subsets of $A$ that include $a_{n+1}$.

Knowing that $a_{n+1}$ is one element of the 2-element subset, the only possible subsets are $\{a_1, a_{n+1}\}, \{a_2, a_{n+1}\}, \ldots, \{a_n, a_{n+1}\}$.

There are exactly $n$ such subsets.
The set of 2-element subsets of \( A \) that do not include \( a_{n+1} \).

Since we do not include \( a_{n+1} \), these subsets are exactly the subsets of \( \{a_1, a_2, \ldots a_n\} \), which has \( n \) elements.

By the inductive hypothesis, there are \( \frac{n(n-1)}{2} \) of these sets.

Therefore, the total number of 2-element subsets of \( A \) is \( \frac{n(n-1)}{2} + n = \frac{n(n-1)+2n}{2} = \frac{(n+1)n}{2} \) as desired.

8. (OPTIONAL) Find the flaw in this inductive proof.

Claim: Let \( n \) be a finite integer. In every set of \( n \) people, all the people in the set share the same height.

Proof: We prove this by induction.

Base Case: If \( n = 1 \), then it’s true that the one person in a set of 1 element has the same height as everyone in the set.

Inductive step: Say that, for fixed \( n \), every set of \( n \) people must have the same height.

Consider a set of \( n+1 \) people. Number each person \( a_1 \ldots a_{n+1} \). The subset \( \{a_1 \ldots a_n\} \) has \( n \) people, and therefore all of them must have the same height by the inductive hypothesis. The subset \( \{a_2 \ldots a_{n+1}\} \) also has \( n \) elements, and they must all have height as well by the inductive hypothesis. Since the two sets overlap, it follows that all \( n+1 \) people in the group must have the same height.

Therefore, we conclude by induction that all finite sets of people have the same height.

Solution:

9. (OPTIONAL) Clearly state the flaw in this inductive proof. (Pretend that someone you hate is trying to make the following argument. Convince them why they are wrong.)

Claim: \( 2^n = 1 \) for all \( n \geq 0 \).

Proof: We prove this by strong induction.

Base Case: If \( n = 0 \), then it’s true that \( 2^0 = 1 \).

Inductive step: Assume that for fixed \( n \) and all \( i: 0 \leq i \leq n \) that \( 2^i = 1 \). Then \( 2^{n+1} = 2^i \cdot 2^n \). By the inductive hypothesis, \( 2^n \) and \( 2^{n-1} \) are both 1. Therefore \( 2^{n+1} = 1 \cdot 1 = 1 \).

Therefore, we conclude that \( 2^n = 1 \) for all \( n \geq 0 \)

Solution:
10. (15 points) I define a function from the set of polynomials to themselves that satisfies the following properties.

- $d(1) = 0$
- $d(x) = 1$
- Product Rule: $d(f(x) \cdot g(x)) = d(f(x)) \cdot g(x) + f(x) \cdot d(g(x))$.

Find a pattern for the general rule for $d(x^n)$ for $n \geq 0$, and prove that pattern by induction, using only the above properties about the function $d$.

**Solution:**

11. (20 points) In the inductive step of an induction, the claim you are trying to prove comes into play in two places. You *assume* your claim for smaller values up to $n$, and you use those facts to *prove* the claim for $n + 1$. This question illustrates the idea of inductive loading - the idea that sometimes it’s easier to prove by induction a *stronger* statement than the one you’re trying to prove because you get to make stronger assumptions.

(a) Say that we’re trying to show that

$$\frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot 2n - 1}{2 \cdot 4 \cdot 6 \cdot \cdots \cdot 2n} < \frac{1}{\sqrt{3n}}$$

by induction.

Show that the base case succeeds, and show an attempt to do the inductive step. Unfortunately, your inductive step will fail at a certain point - describe why it fails.

**Solution:**

(b) Now, we make use of the fact that $\frac{1}{\sqrt{3n+1}} < \frac{1}{\sqrt{3n}}$ for all $n$. This means that

$$\frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot 2n - 1}{2 \cdot 4 \cdot 6 \cdot \cdots \cdot 2n} \leq \frac{1}{\sqrt{3n + 1}}$$

is a *stronger* statement than the one above, since this one implies the one above.

Prove the stronger statement by induction.

**Solution:**

12. (8 points) Show by induction that a set with $n + 1$ different positive integers all between 1 and $2n$ (including the endpoints) must have one integer in this set that divides another.

**Solution:**