CSE 390Z: Mathematics for Computation Workshop

Week 5 Workshop Solutions

0. Conceptual Review

(a) **Definitions**
a divides b: $\quad a \mid b \quad \leftrightarrow \quad \exists k \in \mathbb{Z}\ (b = ka)$
a is congruent to b modulo m: $\quad a \equiv_m b \quad \leftrightarrow \quad m \mid (a - b)$

(b) How do you know if a multiplicative inverse does not exist?
A multiplicative inverse does not exist when $\gcd(a, b) \neq 1$.

(c) Bezout's theorem: If a and b are positive integers, then there exist integers s and t such that gcd(a, b) is equal to what?

$$\text{gcd}(a, b) = sa + tb$$

(d) What is the Euclidean algorithm? What does it help us calculate?
The Euclidean algorithm helps us find gcd(a, b). The algorithm is as follows:

- Repeatedly use gcd$(a, b) =$ gcd$(b, a\%b)$. Make sure a is the larger number.
- When you reach gcd$(g, 0)$, return g.

(e) What is the extended Euclidean algorithm? What does it help us calculate?
We use the extended Euclidean algorithm to find s, t such that $\gcd(a, b) = sa + tb$.
t is the multiplicative inverse of b modulo a.
The multiplicative inverses can be used solve modular equations.
The algorithm is as follows:

- Repeatedly use gcd$(a, b) =$ gcd$(b, a\%b)$ and keep track of the equation $a = q * b + a\%b$ in every step.
- When you reach gcd$(g, 0)$, g is the gcd. **Do not** keep track of the equation for this step. The final equation should have the gcd in the remainder $(a\%b)$ position.
- Rearrange the equations from $a = q * b + a\%b$ to $a\%b = a - q * b$.
- The b in every equation was the $a\%b$ in the equation above it. Starting from the final equation substitute the equation above it in for b.
- Gather like terms but do not simplify more than that.
- Repeat the previous two steps until you have an equation of the form gcd$(a, b) = sa + tb$. Note that the previous two steps are referred to as back substitution.

1. Extended Euclidean Algorithm and Multiplicative Inverse – Together!

Solve the equation and state the full set of solutions

$$311x \equiv_{2021} 3$$

(a) Use the Euclidean algorithm to find $\gcd(2021, 311)$. Make sure to keep track of the equation $a = q*b+a\%b$ in every step.

Solution:

$$\gcd(2021, 311) = \gcd(311, 2021 \ \% \ 311) = \gcd(311, 155) \qquad 2021 = 6 * 311 + 155$$
$$\gcd(311, 155) = \gcd(155, 311 \ \% \ 155) = \gcd(155, 1) \qquad 311 = 2 * 155 + 1$$
$$\gcd(155, 1) = \gcd(1, 155 \ \% \ 1) = \gcd(1, 0) = 1 \qquad \text{no equation for this line}$$

Note: I find this hard to keep track of. I prefer this way:
Starting with 2021 and 311:
$2021 = \_\_\_ * 311 + \_\_\_ = 6 * 311 + 155$ (Take 311 and 155 from here and move to the next line)
$311 = \_\_\_ * 155 + \_\_\_ = 2 * 155 + 1$ (Take 155 and 1 from here and move to the next line)
$155 = \_\_\_ * 1 + \_\_\_ = 155 * 1 + 0$ (Throw this line out since it has a + 0 at the end.)

(b) Rearrange the equations from $a = q * b + a\%b$ to $a\%b = a - q * b$

Solution:

$$2021 = 6 * 311 + 155 \qquad 155 = 2021 - 6 * 311 \qquad (1)$$
$$311 = 2 * 155 + 1 \qquad 1 = 311 - 2 * 155 \qquad (2)$$

(c) Use back substitution to find an equation of the form $\gcd(2021, 311) = s * 2021 + t * 311$. The t in this equation is the multiplicative inverse. If t is not in the range $0 \leq t < 2021$, add or subtract 2021 until you get a value for t that is in that range.

Solution:

The labels used below are from the previous step.

$$\begin{aligned} 1 &= 311 - 2 * 155 && \text{Start with equation (2)} \\ &= 311 - 2 * (2021 - 6 * 311) && \text{Sub in equation (1)} \\ &= 311 - 2 * 2021 + 12 * 311 \\ &= -2 * 2021 + 13 * 311 \end{aligned}$$

So 13 is the multiplicative inverse.

(d) Use the multiplicative inverse found in the previous step to solve the original equation $311x \equiv_{2021} 3$.

Solution:

Since 13 is the multiplicative inverse of 311 modulo 2021, we multiply both sides of our equation by 13:

$$13 \cdot 311x \equiv_{2021} 13 \cdot 3 \qquad [13 \cdot 311 \equiv_{2021} 1]$$
$$x \equiv_{2021} 39$$

So the full set of solutions is $39 + 2021k$ for any integer k.

2. Extended Euclidean Algorithm and Multiplicative Inverse – Your Turn

Solve the equation and state the full set of solutions

$$38y \equiv_{101} 5$$

.

Solution:

First we use the Euclidean algorithm to compute gcd(101,38) keeping track of our equations in every step

$\gcd(101, 38) = \gcd(38, 101\%38) = \gcd(38, 25)$	$101 = 2 * 38 + 25$
$\gcd(38, 25) = \gcd(25, 38\%25) = \gcd(25, 13)$	$38 = 1 * 25 + 13$
$\gcd(25, 13) = \gcd(13, 25\%13) = \gcd(13, 12)$	$25 = 1 * 13 + 12$
$\gcd(13, 12) = \gcd(12, 13\%12) = \gcd(12, 1)$	$13 = 1 * 12 + 1$
$\gcd(12, 1) = \gcd(1, 12\%1) = \gcd(1, 0)$	no equation for this line

Now, we rearrange:

$$101 = 2 * 38 + 25 \qquad 25 = 101 - 2 * 38 \qquad (1)$$
$$38 = 1 * 25 + 13 \qquad 13 = 38 - 1 * 25 \qquad (2)$$
$$25 = 1 * 13 + 12 \qquad 12 = 25 - 1 * 13 \qquad (3)$$
$$13 = 1 * 12 + 1 \qquad 1 = 13 - 1 * 12 \qquad (4)$$

Now we use back substitution to find an equation of the form $\gcd(101, 38) = s * 101 + t * 38$.
The labels used below are from the previous step.

$1 = 13 - 1 * 12$	Start with equation (4)
$= 13 - 1 * (25 - 1 * 13)$	Sub in equation (3)
$= 13 - 1 * 25 + 1 * 13$	
$= -1 * 25 + 2 * 13$	
$= -1 * 25 + 2 * (38 - 1 * 25)$	Sub in equation (2)
$= -1 * 25 + 2 * 38 - 2 * 25$	
$= 2 * 38 - 3 * 25$	
$= 2 * 38 - 3 * (101 - 2 * 38)$	Sub in equation (1)
$= 2 * 38 - 3 * 101 + 6 * 38$	
$= -3 * 101 + 8 * 38$	

So 8 is our multiplicative inverse.
We multiply both sides of our original equation $38y \equiv_{101} 5$ by 8.

$$8 \cdot 38y \equiv_{101} 8 \cdot 5 \qquad [8 \cdot 38 \equiv_{101} 1]$$
$$y \equiv_{101} 40$$

So the full set of solutions is $40 + 101k$ for any integer k.

3. Induction: Warm-Up

Prove $5 \mid (6^n - 1)$ for all $n \in \mathbb{N}$ by induction.

Solution:

Let $P(n)$ be "$5 \mid 6^n - 1$". We will show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case ($n = 0$): $6^0 - 1 = 1 - 1 = 0 = 0 \cdot 5$, so $5 \mid 6^0 - 1$.

Inductive Hypothesis. Suppose $P(k)$ holds for some arbitrary integer $k \geq 0$.

Inductive Step.

Goal: Show $P(k+1)$, i.e. $5 \mid (6^{k+1} - 1)$.

By the Inductive Hypothesis, we have that $5 \mid (6^k - 1)$. Then by definition of divides, $6^k - 1 = 5j$ for some $j \in \mathbb{Z}$. We have:

$$\begin{aligned} 6^k - 1 &= 5j && \text{IH} \\ 6^{k+1} - 6 &= 30j && \text{Multiply both sides by 6} \\ 6^{k+1} - 1 &= 30j + 5 && \text{Add 5 to both sides} \\ 6^{k+1} - 1 &= 5(6j+1) && \text{Factor} \end{aligned}$$

By definition of divides, we have that $5 \mid (6^{k+1} - 1)$, as desired. So P($k+1$) holds.

Conclusion. P(n) is true for all $n \in \mathbb{N}$ by induction.

Alternate Solution for Inductive Step:

Goal: Show $P(k+1)$, i.e. $5 \mid (6^{k+1} - 1)$.

$$\begin{aligned} 6^{k+1} - 1 &= 6^{k+1} - 1 + 0 \\ &= 6^{k+1} - 1 + (-5 + 5) \\ &= (6^{k+1} - 6) + 5 \\ &= 6(6^k - 1) + 5 \\ &= 6(5j) + 5 && \text{[by IH for some integer } j\text{]} \\ &= 5(6j + 1) \end{aligned}$$

By definition of divides, $5 \mid (6^{k+1} - 1)$ as required. So P(k+1) holds.

4. Induction: Equality

Prove by induction that for every $n \in \mathbb{N}$, the following equality is true:

$$0 \cdot 2^0 + 1 \cdot 2^1 + 2 \cdot 2^2 + \cdots + n \cdot 2^n = (n-1)2^{n+1} + 2.$$

Solution:

Let $P(n)$ be "$0 \cdot 2^0 + 1 \cdot 2^1 + 2 \cdot 2^2 + \cdots + n \cdot 2^n = (n-1)2^{n+1} + 2$". We will prove $P(n)$ for all $n \in \mathbb{N}$ by induction on n.

Base Case $(n = 0)$: $0 \cdot 2^0 = 0 = 0 = -2 + 2 = (0-1)2^{0+1} + 2$ therefore $P(0)$ is true. OR

LHS: $0 \cdot 2^0 = 0$

RHS: $(0-1)2^{0+1} + 2 = -2 + 2 = 0$

Since LHS = RHS, $P(0)$ is true.

Inductive Hypothesis. Suppose that $P(k)$ holds for some arbitrary integer $k \geq 0$.

Induction Step We show $P(k+1)$:

$$0 \cdot 2^0 + 1 \cdot 2^1 + 2 \cdot 2^2 + \cdots + (k+1) \cdot 2^{k+1}$$

$$\begin{aligned}
&= (0 \cdot 2^0 + 1 \cdot 2^1 + 2 \cdot 2^2 + \cdots + k \cdot 2^k) + (k+1) \cdot 2^{k+1} && \text{[Show another term inside "..."]} \\
&= ((k-1)2^{k+1} + 2) + (k+1)2^{k+1} && \text{[Inductive Hypothesis]} \\
&= ((k-1) + (k+1))2^{k+1} + 2 && \text{[Group multiples of } 2^{k+1}\text{]} \\
&= (2k)2^{k+1} + 2 && \text{[Algebra]} \\
&= k2^{k+2} + 2 && \text{[Algebra]}
\end{aligned}$$

Therefore $P(k+1)$ holds.

Conclusion. $P(n)$ holds for all $n \in \mathbb{N}$ by induction.

5. Induction: Inequality

Prove that $2^n + 1 \leq 3^n$ for all positive integers n by induction.

Solution:

Let $P(n)$ be "$2^n + 1 \leq 3^n$". We will prove that $P(n)$ holds for all integers $n \geq 1$ by induction on n.
Base Case: $(n = 1)$: $2^1 + 1 = 2 + 1 = 3 \leq 3 = 3^1$ therefore $P(1)$ holds. OR
LHS: $2^1 + 1 = 2 + 1 = 3$
RHS: $3^1 = 3$
$3 \leq 3$ (i.e., LHS $\leq$ RHS), so $P(1)$ holds.
Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary integer $k \geq 1$.
Inductive Step:

Goal: Show $P(k+1)$, i.e. $2^{k+1} + 1 \leq 3^{k+1}$.

$$\begin{aligned}
2^{k+1} + 1 &= 2 * 2^k + 1 && \\
&< 2 * 2^k + 2 && \text{Since } 1 < 2 \\
&= 2(2^k + 1) && \\
&\leq 2 * 3^k && \text{IH} \\
&< 3 * 3^k && \text{Since } 2 < 3 \\
&= 3^{k+1} &&
\end{aligned}$$

So, $P(k+1)$ holds.
Conclusion: Therefore, by the principle of induction, $P(n)$ holds for all positive integers n.

6. Induction: Divides

Prove that $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ for all integers $n > 1$ by induction.

Solution:

Let $P(n)$ be "$9 \mid n^3 + (n+1)^3 + (n+2)^3$". We will prove $P(n)$ for all integers $n > 1$ by induction on n.

Base Case $(n = 2)$**:** $2^3 + (2+1)^3 + (2+2)^3 = 8 + 27 + 64 = 99 = 9 \cdot 11$, so $9 \mid 2^3 + (2+1)^3 + (2+2)^3$, so $P(2)$ holds.

Inductive Hypothesis: Suppose $9 \mid k^3 + (k+1)^3 + (k+2)^3$ for an arbitrary integer $k \geq 2$. Note that this is equivalent to assuming that $k^3 + (k+1)^3 + (k+2)^3 = 9j$ for some integer j by the definition of divides.

Inductive Step: Goal: Show $9 \mid (k+1)^3 + (k+2)^3 + (k+3)^3$

$$\begin{aligned}
(k+1)^3 + (k+2)^3 + (k+3)^3 &= (k+1)^3 + (k+2)^3 + (k+3)(k^2 + 6k + 9) && \text{[expanding]} \\
&= (k+1)^3 + (k+2)^3 + (k^3 + 6k^2 + 9k + 3k^2 + 18k + 27) && \text{[expanding]} \\
&= (k+1)^3 + (k+2)^3 + k^3 + 9k^2 + 27k + 27 && \text{[adding like terms]} \\
&= [k^3 + (k+1)^3 + (k+2)^3] + 9k^2 + 27k + 27 && \text{[rearranging]} \\
&= 9j + 9k^2 + 27k + 27 && \text{[by I.H., } j \in \mathbb{Z}\text{]} \\
&= 9(j + k^2 + 3k + 3) && \text{[factoring out 9]}
\end{aligned}$$

By the definition of divides, $9 \mid (k+1)^3 + (k+2)^3 + (k+3)^3$ and $P(k+1)$ holds.

Conclusion: $P(n)$ holds for all integers $n > 1$ by the principle induction.

7. Inductively Odd

A 123 student learning recursion wrote a recursive Java method to determine if a number is odd or not, and needs your help proving that it is correct.

```
public static boolean oddr(int n) {
   if (n == 0)
      return False;
   else
      return !oddr(n-1);
}
```

Help the student by writing an inductive proof to prove that for all integers $n \geq 0$, the method `oddr` returns `True` if n is an odd number, and `False` if n is not an odd number (i.e. n is even). You may recall the definitions Odd$(n) := \exists x \in \mathbb{Z}(n = 2x + 1)$ and Even$(n) := \exists x \in \mathbb{Z}(n = 2x)$; Note that `!True = False` and `!False = True`.

Solution:

Let P(n) be "`oddr(n)` returns True if n is odd and False if n is even". We will show that P(n) is true for all integers $n \geq 0$ by induction on n.

Base Case: (n = 0)
0 is even, so P(0) holds if `oddr(0)` returns False, which is exactly the base case of `oddr`. Therefore, P(0) holds.
Inductive Hypothesis: Suppose P(k) holds for an arbitrary integer $k \geq 0$.
Inductive Step: Since $k \geq 0$, $k + 1 \geq 1$ so `oddr(k+1)` is in the recursive case, and it returns `!oddr(k)`. We consider two cases: k is even, and k is odd.

Case 1: k is even.
By definition of even, $k = 2x$ for some integer x. Then, $k + 1 = 2x + 1$ is odd by definition.
By the inductive hypothesis, since k is even, `oddr(k)` returns False. Since `oddr(k+1)` returns `!oddr(k)`, it returns `!False = True`.
Since $k + 1$ is odd, this is the correct output, and P(k+1) holds.

Case 2: k is odd.
By definition of odd, $k = 2x + 1$ for some integer x. Then, $k + 1 = 2x + 1 + 1 = 2x + 2 = 2(x + 1)$ is even by definition.
By the inductive hypothesis, since k is odd, `oddr(k)` returns True. Since `oddr(k+1)` returns `!oddr(k)`, it returns `!True = False`.
Since $k + 1$ is even, this is the correct output, and P(k+1) holds.

Since these cases are exhaustive, we have shown P$(k + 1)$ always holds.

Conclusion: P(n) is true for all integers $n \geq 0$ by the principle of induction.

8. Strong Induction: Recursively Defined Functions

Consider the function $f(n)$ defined for integers $n \geq 1$ as follows:
$f(1) = 1$ for $n = 1$
$f(2) = 4$ for $n = 2$
$f(3) = 9$ for $n = 3$
$f(n) = f(n-1) - f(n-2) + f(n-3) + 2(2n-3)$ for $n \geq 4$

Prove that $f(n) = n^2$ for all integers $n \geq 1$ by strong induction.

Solution:

Let P(n) be defined as " $f(n) = n^2$". We will prove $P(n)$ is true for all integers $n \geq 1$ by strong induction.

Base Cases ($n = 1, 2, 3$)**:**

- $n = 1$: $f(1) = 1 = 1^2$.
- $n = 2$: $f(2) = 4 = 2^2$.
- $n = 3$: $f(3) = 9 = 3^2$

So the base cases hold.

Inductive Hypothesis: Assume that for some arbitrary integer $k \geq 3$, we have $f(j) = j^2$ for every integer j from 1 to k.
In other words, assume $P(1) \wedge P(2) \wedge ... \wedge P(k)$ for an arbitrary integer $k \geq 3$.

Inductive Step:

Goal: Show $P(k+1)$, i.e. show that $f(k+1) = (k+1)^2$.

$$
\begin{aligned}
f(k+1) &= f(k+1-1) - f(k+1-2) + f(k+1-3) + 2(2(k+1)-3) && \text{Definition of f} \\
&= f(k) - f(k-1) + f(k-2) + 2(2k-1) \\
&= k^2 - (k-1)^2 + (k-2)^2 + 2(2k-1) && \text{By IH} \\
&= k^2 - (k^2 - 2k + 1) + (k^2 - 4k + 4) + 4k - 2 \\
&= k^2 - k^2 + 2k - 1 + k^2 - 4k + 4 + 4k - 2 \\
&= (k^2 - k^2 + k^2) + (2k - 4k + 4k) + (-1 + 4 - 2) \\
&= k^2 + 2k + 1 \\
&= (k+1)^2
\end{aligned}
$$

So P($k+1$) holds.

Conclusion: We have shown P(n) holds for all integers $n \geq 1$ by the principle of induction.

9. Strong Induction: Packs of Candy

A store sells candy in packs of 4 and packs of 7. Let P(n) be defined as "You are able to buy n packs of candy". For example, $P(3)$ is not true, because you cannot buy exactly 3 packs of candy from the store. However, it turns out that P(n) is true for all $n \geq 18$. Use strong induction to prove this.

Hint: It may be easier to leave your base cases blank, write your inductive step, then figure out how many base cases you need, and go back and fill them in.

Solution:

Let P(n) be defined as "You are able to buy n packs of candy". We will prove $P(n)$ is true for all integers $n \geq 18$ by strong induction.

Base Cases: ($n = 18, 19, 20, 21$)**:**

- $n = 18$: 18 packs of candy can be made up of 2 packs of 7 and 1 pack of 4 $(18 = 2 * 7 + 1 * 4)$.
- $n = 19$: 19 packs of candy can be made up of 1 pack of 7 and 3 packs of 4 $(19 = 1 * 7 + 3 * 4)$.
- $n = 20$: 20 packs of candy can be made up of 5 packs of 4 $(20 = 0 * 7 + 5 * 4)$.
- $n = 21$: 21 packs of candy can be made up of 3 packs of 7 $(21 = 3 * 7 + 0 * 4)$.

Inductive Hypothesis: Assume that for some arbitrary integer $k \geq 21$, we can buy j packs of candy for every integer j from 18 to k.
In other words, assume P(18) $\wedge$... $\wedge$P(k) hold for some arbitrary integer $k \geq 21$.

Inductive Step:

Goal: Show $P(k+1)$, i.e. show that we can buy $k+1$ packs of candy.

We want to buy $k+1$ packs of candy. Since $k \geq 21$, $(k+1) - 4 = k - 3 \geq 18$.
Our inductive hypothesis covers everything from 18 to k and $18 \leq k - 3 \leq k$
Therefore $k - 3$ is covered by our inductive hypothesis.
So, by the I.H., we can buy exactly $k - 3$ packs of candy. We can add another 4 packs in order to buy $k + 1$ packs of candy, so P($k + 1$) is true.

Conclusion: By strong induction, P(n) is true for all integers $n \geq 18$.

Note: Notice that we use the fact that $k - 3$ was covered by our inductive hypothesis as part of our proof. Since 18 is the smallest value in our domain, we need $k - 3 \geq 18$. Adding 3 to both sides this means $k \geq 21$. That's how we knew we needed the largest value in our base case to be 21.
Some people find it helpful to think of it this way: we had to use a fact from 4 steps back from $k + 1$ to $k - 3$ in the IS, so we needed 4 base cases.