CSE 390Z: Mathematics for Computation Workshop

Week 5 Workshop

0. Conceptual Review

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

(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?

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

(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.

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

(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.

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

2. Extended Euclidean Algorithm and Multiplicative Inverse – Your Turn

Solve the equation and state the full set of solutions

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

.

3. Induction: Warm-Up

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

4. Induction: Equality

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

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

5. Induction: Inequality

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

6. Induction: Divides

Prove that $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ for all integers $n > 1$ by 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 $\text{Odd}(n) := \exists x \in \mathbb{Z}(n = 2x + 1)$ and $\text{Even}(n) := \exists x \in \mathbb{Z}(n = 2x)$; Note that `!True = False` and `!False = True`.

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.

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.