CS 13: Mathematics for Computer Scientists Spring 2023

Homework 01 (due Friday, April 21)

Directions: *Write up carefully argued solutions to the following problems. Your solution should be clear enough that it should explain to someone who does not already understand the answer why it works. You may use results from lecture and previous homeworks without proof.*

0. 11 Modom (20 points)

We say an integer is *palindromic* if the digits read the same when written forward or backward. Prove that every palindromic integer with an even number of digits is divisible by 11.

1. Too Many Twos (25 points)

In this question, you will explore some properties of the Two's Complement system discussed in class.

(a) [20 Points] Prove that in a fixed-width two's complement representation with n bits, any integer $-2^{n-1} < x < 2^{n-1}$ can be negated by flipping all bits and adding 1.

(b) [5 Points] Prove that, over the given range, negation is bijective. If this is a property we'd like to retain for our fixed-width number system, what does this mean for the negation of -2^{n-1} in two's complement?

2. OMgcd (25 points)

In this problem, you will bound the runtime of the gcd algorithm discussed in class.

(a) [15 Points] Let n and m be arbitrary positive integers with $n \leq m$. Prove that m mod $n \leq \frac{m}{2}$.

(b) [10 Points] Recall the Euclidean Algorithm:

```
def gcd(m, n):
   if n == 0:
      return m
   else:
      return gcd(n, m % n)
```

Assume $n \leq m$. Use part (a) to show that the Euclidean Algorithm will make a total of at most $2\log_2 m$ recursive calls.

Note: if $n > m$, we have `(n, m % n) = (n, m)` *and so we simply swap the two on the first call. Thus, we can conclude that the total number of recursive calls is at most $2\max(\log_2 m, \log_2 n) + 1$*

3. Around and Around Again (15 points)

Find the multiplicative inverse of $n - 1$ in mod n for $n \geq 2$.

4. Freshman's Dream (15 points)

Prove that for a prime p and $a, b, n \in \mathbb{Z}$ with $n > 0$,

$$(a+b)^{p^n} \equiv_p a^{p^n} + b^{p^n}$$

Hint: Recall the binomial theorem: for all $x, y \in \mathbb{R}$ and $n \in \mathbb{N}$, $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$. Use it to prove a base case for an induction on n.