# CS 13: Mathematical Foundations of Computer Science — Fall 2023

## Written Homework 01 (due Monday, Oct 16)

**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. Your solutions* must *be written in LaTeX using our homework template.* ***No solution to a single part may be more than one page.***

## 0. 11 Modom (25 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 (30 points)

Recall that in lecture we defined the valuation function for binary strings:

$$V(b_n b_{n-1} \dots b_1 b_0) = \sum_{i=0}^{n} b_i 2^i$$

Note that $V$ always outputs a non-negative integer - but in digital systems, it is often necessary to additionally represent negative numbers. To address this issue, the *two's complement* representation of signed binary numbers is widely adopted.

The valuation function for a two's complement representation can be given as:

$$V(b_n b_{n-1} \dots b_1 b_0) = -b_n 2^n + \sum_{i=0}^{n-1} b_i 2^i$$

Here, if $b_n = 0$, the number is non-negative and its value is the same as in the ordinary binary representation. If $b_n = 1$, the number is negative, and its value is given by $V$.

(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) [10 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 (30 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) [15 Points] Recall the Euclidean Algorithm:

```
1 def gcd(m, n):
2     if n == 0:
3         return m
4     else:
5         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.

## 3. Around and Around Again (15 points)

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

## 4. Freshman's Dream (Extra Credit) (5 points)

**This question is extra credit. It is much harder than the 5 points it's worth.**

Prove that for a prime $p$ and $a, b, n \in \mathbb{Z}$ with $n > 0$, $(a+b)^{p^n} \equiv_p a^{p^n} + b^{p^n}$.