Math 240: Discrete Structures I (W18) – Assignment 4

Solutions must typed or very neatly written and uploaded to MyCourses no later than **6 pm** on **Saturday, February 17, 2018**. Up to 4 bonus marks will be awarded for solutions typeset in LaTeX; both the .tex file and .pdf file must be uploaded.

You may use theorems proven or stated in class, but you must state the theorem you are using.

[7] 1. **Division algorithm**
The division algorithm states that for any $a, b \in \mathbb{Z}$ $(b \neq 0)$ there exist $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$; furthermore, these q, r are unique for a, b. We proved this when $a, b > 0$. Prove that q, r exist for all a, b[1]. Hints: (1) You may use the fact that the statement holds when $a, b > 0$ as a tool without proving it and (2) you will need to consider cases.

[18] 2. **Divisors**

(a) Find $\gcd(2018, 240)$, and express your answer as a linear combination of 2018 and 240 (that is, find $r, s \in \mathbb{Z}$ such that $\gcd(2018, 240) = 2018r + 240s$).

(b) Let k be a positive integer. Show that if a and b are relatively prime integers, then $\gcd(a + kb, b + ka)$ divides $k^2 - 1$. Hint: Consider two linear combinations of $a + kb$ and $b + ka$.

(c) Suppose $n, m, p \in \mathbb{N}$, p a prime, where $p \mid n$, $m \mid n$, and $p \nmid m$. Either prove that p divides $\frac{n}{m}$ or provide a counterexmple to show that it doesn't. Make sure to address whether or not "p divides $\frac{n}{m}$" even makes sense.

[15] 3. **Congruence and modular arithmetic**

(a) Let $k \in \mathbb{Z} \setminus \{0\}$. Prove that $ka \equiv kb \pmod{kn}$ if and only if $a \equiv b \pmod{n}$.

(b) Prove that if $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

(c) Show that $1806^{6236} \equiv 1 \pmod{17}$.

[1] You do not need to prove uniqueness; the proof we provided in class did not rely on the signs of a and b.