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.

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.

Solution. Case 1: $a = 0$. If $a = 0$, then $q = r = 0$ suffice: $qb + r = (0)b + (0) = 0 = a$.
Case 2: $a < 0, b > 0$. Since $a < 0$, we have $-a > 0$, and so there exist q, r such that $-a = qb + r, 0 \leq r < |b| = b$. This means

$$\begin{aligned} a &= -qb - r \\ &= (-q)b - r + b - b \\ &= (-q-1)b + (b - r). \end{aligned}$$

Since $b \neq 0$, we get $0 < b - r < b$, so the integers $-q-1$ and $b-r$ suffice.
Case 3: $b < 0$. Since $-b > 0$, we know (by the part done in class and case 1 above) there exist q, r such that $a = q(-b) + r, 0 \leq r < |-b| = b$, or that $a = (-q)b + r$. Thus $-q$ and r are the desired integers.

[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 $\gcd(2018, 240) = 2018r + 240s$).

Solution. First, we apply the Euclidean Algorithm:

$$\begin{aligned} 2018 &= 8(240) + 98 \\ 240 &= 2(98) + 44 \\ 98 &= 2(44) + 10 \\ 44 &= 4(10) + 4 \\ 10 &= 2(4) + 2 \\ 4 &= 2(2) + 0. \end{aligned}$$

Thus $\gcd(2018, 240) = 2$. We then reverse the algorithm to find 2 as a linear combination of 2018 and 240:

$$\begin{aligned}
2 &= (10) - 2(4) \\
&= (10) - 2\big(44 - 4(10)\big) \\
&= 9(10) - 2(44) \\
&= 9\big(98 - 2(44)\big) - 2(44) \\
&= 9(98) - 20(44) \\
&= 9(98) - 20\big(240 - 2(98)\big) \\
&= 49(98) - 20(240) \\
&= 49\big(2018 - 8(240)\big) - 20(240) \\
&= 49(2018) - 412(240)
\end{aligned}$$

(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 $b + ka$.

Solution. Let $g = \gcd(a + kb, b + ka)$. Since $g \mid a + kb$ and $g \mid b + ka$, we have

$$g \mid [k(a + kb) - (b + ka)] \Rightarrow g \mid \left[k^2 b - b\right] \Rightarrow g \mid b(k^2 - 1)$$

and similarly

$$g \mid [k(b + ka) - (a + kb)] \Rightarrow g \mid \left[k^2 a - a\right] \Rightarrow g \mid a(k^2 - 1).$$

Since $\gcd(a, b) = 1$, there exist $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Multiplying by $(k^2 - 1)$ gives

$$m\left[a(k^2 - 1)\right] + n\left[b(k^2 - 1)\right] = (k^2 - 1).$$

Since g divides the expression on the left hand side of the equation, we have $g \mid (k^2 - 1)$.

(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.

Solution. Firstly, since m divides n, $\frac{n}{m} \in \mathbb{N}$ so "p divides $\frac{n}{m}$" is a well defined sentence. Let $k = \frac{n}{m}$, or $n = mk$. Now, since $p \mid n$ but $p \nmid m$, we must have that $p \mid k$ (we proved in class that $p \mid ab$ implies that p divides at least one of a and b). In other words, $p \mid \frac{n}{m}$.

[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 $a \equiv b \pmod{n}$.

Solution.

$$\begin{aligned} ka \equiv kb \pmod{kn} &\Leftrightarrow ka - kb \equiv 0 \pmod{kn} \\ &\Leftrightarrow kn = c(ka - kb), c \in \mathbb{Z} \\ &\Leftrightarrow n = c(a - b), c \in \mathbb{Z} \\ &\Leftrightarrow a - b \equiv 0 \pmod{n} \\ &\Leftrightarrow a \equiv b \pmod{n}. \end{aligned}$$

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

Solution. Since $a \equiv b \pmod{n}$, there is some integer k such that $a = kn + b$. Since $\gcd(a, n)$ divides both a and n, we get that $\gcd(a, n)$ divides $b = a - kn$. But, since $\gcd(a, n)$ divides both b and n, we get $\gcd(a, n) \leq \gcd(b, n)$. Similarly, since $\gcd(b, n)$ divides both b and n, we get that $\gcd(b, n)$ divides $a = kn + b$. But, since $\gcd(b, n)$ divides both a and n, we get $\gcd(b, n) \leq \gcd(a, n)$. Together, we conclude $\gcd(a, n) = \gcd(b, n)$.

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

Solution. We first note that $1806 = 17(106) + 4$, so

$$\begin{aligned} 1806^{6236} &\equiv 4^{6236} \pmod{17} \\ &\equiv 4^{2(3118)} \pmod{17} \\ &\equiv 16^{3118} \pmod{17} \\ &\equiv (-1)^{3118} \pmod{17} \\ &\equiv (-1)^{2(1559)} \pmod{17} \\ &\equiv 1^{1559} \pmod{17} \\ &\equiv 1 \pmod{17}. \end{aligned}$$

If you want to make use of Fermat's Little Theorem, since $17 \nmid 1806$, we have

$$\begin{aligned} 1806^{6236} &\equiv 4^{6236} \pmod{17} \\ &\equiv 4^{(16)(389)+12} \pmod{17} \\ &\equiv \left(4^{16}\right)^{389} 4^{12} \pmod{17} \\ &\equiv (1)\, 4^{12} \pmod{17} \\ &\equiv 16^{6} \pmod{17} \\ &\equiv (-1)^{6} \pmod{17} \\ &\equiv 1 \pmod{17}. \end{aligned}$$