Math 4000/6000 – Homework #2

posted August 28, 2015; due at the **start of class** on September 4, 2015

> Mathematics is not a deductive science — that's a cliché. When you try to prove a theorem, you don't just list the hypotheses, and then start to reason. What you do is trial and error, experimentation, guesswork. – Paul Halmos

Assignments are expected to be neat and stapled. **Illegible work may not be marked**. Starred problems (*) are required for those in MATH 6000 and extra credit for those in MATH 4000.

1. Prove the *law of cancelation* in $\mathbb{Z}$: If $ab = ac$ and $a \neq 0$, then $b = c$.

   Hint: If $ab = ac$, then $a(b - c) = 0$. Now use a result from HW #1.

2. Let $a, b \in \mathbb{Z}$, not both zero. In class, we defined $\gcd(a, b)$ to be the largest common divisor of a and b. It was then a theorem that the number $d = \gcd(a, b)$ satisfies

   $$d \text{ divides } a \text{ and } b\text{, and every common divisor of } a \text{ and } b \text{ divides } d. \qquad (\dagger)$$

   Show that $\gcd(a, b)$ is the *only* positive integer d that satisfies $(\dagger)$.

   Remark. This exercise shows that $(\dagger)$ could have been taken as the **definition** of $\gcd(a, b)$. That is the approach followed in your textbook.

3. Suppose a, b, c are positive integers, $a \mid bc$, and $\gcd(a, b) = 1$. Prove that $a \mid c$.

   Hint: Imitate the proof of Euclid's lemma from class.

4. Exercise 1.2.4, + the following part (c):
   Prove or give a counterexample: If $d = \gcd(a, b)$, then $\gcd(a/d, b) = 1$.

5. Exercise 1.2.8.

   Hint: You may want to start by proving the following lemma: $\gcd(A, B) > 1$ if and only if there is a prime p dividing both A and B.

6. Exercise 1.2.16(b).

7. Let a and b be positive integers with $\gcd(a, b) = 1$. Prove that ab is the smallest positive integer divisible by both a and b.

8. Exercise 1.3.12.

9. Exercise 1.3.15.

10. In your last HW, you proved that $\gcd(a, b)$ can always be expressed in the form $ax + by$, with $x, y \in \mathbb{Z}$. In fact, the Euclidean algorithm gives us a method of finding x and y. We illustrate with the example of $x = 942$ and $y = 408$. Here the Euclidean algorithm runs as follows:

$$\begin{aligned} 942 &= 408 \cdot 2 + 126 \\ 408 &= 126 \cdot 3 + 30 \\ 126 &= 30 \cdot 4 + 6 \\ 30 &= 6 \cdot 5 + 0. \end{aligned}$$

In particular, $\gcd(942, 408) = 6$. So there should be $x, y \in \mathbb{Z}$ with $942x + 408y = 6$. We can find x, y by backtracking through the algorithm. First,

$$6 = 126 + 30(-4), \qquad \text{so we get 6 as a combination of } 126, 30.$$

Next,

$$\begin{aligned} 6 &= 126 + (408 - 126 \cdot 3)(-4) \\ &= 408(-4) + 126(13), \qquad \text{so we get 6 as a combination of } 408, 126. \end{aligned}$$

Continuing,

$$\begin{aligned} 6 &= 408(-4) + (942 - 408 \cdot 2)(13) \\ &= 942 \cdot 13 + 408(-30), \qquad \text{so we get 6 as a combination of } 942, 408. \end{aligned}$$

(a) Using this method, find integers x and y with $17x + 97y = \gcd(17, 97)$.

(b) Find integers x and y with $161x + 63y = \gcd(161, 63)$.

11. (*) Suppose a, b are positive integers with $\gcd(a, b) = 1$. Find, with proof, all possible values of $\gcd(a + b, a - b)$.

12. (*) Define the nth **Fermat number** by the rule $F_n = 2^{2^n} + 1$. Prove that for any two distinct nonnegative integers m and n, we have $\gcd(F_m, F_n) = 1$.