Math 4000/6000 – Homework #2

posted August 30, 2018; due at the **start of class** on September 11, 2018

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. 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.

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

3. 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.

4. Let a and b be positive integers with $\gcd(a, b) = 1$. Prove that if n is an integer for which $a \mid n$ and $b \mid n$, then $ab \mid n$.

5. Using the unique factorization theorem, prove that the only pair of integers a and b satisfying the equation

$$a^3 = 9b^3$$

is $a = 0, b = 0$.

6. Exercise 1.3.12.

7. (Divisibility in Pythagorean triples) Recall that an ordered triple of integers x, y, z is called **Pythagorean** if $x^2 + y^2 = z^2$.
   (a) Show that in any Pythagorean triple, at least one of x, y, z is a multiple of 3.
   (b) Do part (a) again but with "3" replaced by "4", and then do it once more with "3" replaced by "5".

8. 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 $161x + 63y = \gcd(161, 63)$.

9. Let $m \in \mathbb{Z}^+$. Suppose we wish to find all integers x that solve the congruence $ax \equiv b \pmod{m}$, where $a, b \in \mathbb{Z}$ are given. Let $d = \gcd(a, m)$. Show:

   (a) If $d \nmid b$, then there are no integer solutions.

   (b) If $d \mid b$, then there does exist a solution. Moreover, if x_0 is any solution, then the set of all solutions consists precisely of those $x \equiv x_0 \pmod{m/d}$.

   Hint: (a) and (b) were illustrated in class with specific examples. Show that the method used in those examples goes through in general.

10. (Fermat's little theorem again) Complete the proof from class that when p is prime, $a^p \equiv a \pmod{p}$ for **all** integers a. Remember that in class, we only handled the case when $a \in \mathbb{Z}^+$.

    Hint: Don't reinvent the wheel. Find a way to deduce the general result from the case handled in class.

11. Exercise 1.3.20(a,c,e,g)

12. Exercise 1.3.21(a,c,e,g)

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

14. (*) 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 $\gcd(F_m, F_n) = 1$.