Math 4000/6000 – Homework #2

posted January 28, 2019; due at the **start of class** on February 4, 2019

> 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 (1916–2006)

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 $a, b \in \mathbb{Z}^+$. In class, we defined $\gcd(a, b)$ to be the largest positive integer that divides both a and b. We showed in class that the set of common divisors of a and b is the same as the set of divisors of $\gcd(a, b)$. From that theorem, we see that the number $d = \gcd(a, b)$ has the following property:

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

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

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

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

4. Exercise 1.2.8.

   Hint: One approach starts by proving the following lemma: $\gcd(A, B) > 1$ if and only if there is a common prime p dividing both A and B.

5. Let a and b be positive integers with $\gcd(a, b) = 1$. (In this case, we say a and b are *relatively prime*.) Prove that if c is an integer for which $a \mid c$ and $b \mid c$, then $ab \mid c$.

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 n be a positive integer. Suppose that the decimal digits of n — read from right-to-left — are $a_0, a_1, \ldots, a_k$. Show that

$$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \pmod{11}.$$

Use this to determine the remainder when 2016 is divided by 11.

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 [will have] 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. (*) 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 $\gcd(F_m, F_n) = 1$. Use this to give a proof that there are infinitely many prime numbers.