Math 4000/6000 – Homework #3

posted February 6, 2018; due at the **start of class** on February 12, 2018

> I hope some animal never bores a hole in my head and lays its eggs in my brain, because later you might think you're having a good idea but it's just eggs hatching.
> – Jack Handey

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. We know that each $n \in \mathbb{Z}^+$ can be written uniquely as a product of primes. (The number $n = 1$ is viewed here as the empty product of primes.) For each prime p, define $v_p(n)$ as the number of copies of p appearing in the factorization of n, and put $v_p(n) = 0$ if p does not appear. For example, for $n = 171$, we have

$$171 = 3 \cdot 3 \cdot 19,$$

so that $v_3(171) = 2$, $v_{19}(171) = 1$, and $v_p(171) = 0$ for all other primes p.

(a) Show that if $a = bc$, where $a, b, c \in \mathbb{Z}^+$, then $v_p(a) = v_p(b) + v_p(c)$ for all primes p.

(b) Deduce from (a) that if $a \mid b$ (with $a, b \in \mathbb{Z}^+$), then $v_p(a) \leq v_p(b)$ for all primes p.

(c) Prove the converse of (b): if a and b are positive integers with $v_p(a) \leq v_p(b)$ for all primes p, then $a \mid b$.

2. (Uniqueness of inverses mod m) Suppose b and c are both multiplicative inverses of a modulo m, meaning that $ab \equiv 1 \pmod{m}$ and $ac \equiv 1 \pmod{m}$. Show that $b \equiv c \pmod{m}$.

3. 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.

4. (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.

5. (More on Fermat)

(a) Show that if p is prime and a is an integer not divisible by p, then $a^{p-1} \equiv 1 \pmod{p}$.

(b) Show that if p, q are distinct primes, and a is an integer with $\gcd(a, pq) = 1$, then $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$.

Hint: First Show that $a^{(p-1)(q-1)}$ is both 1 mod p and 1 mod q.

6. Exercise 1.3.14.

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

8. Exercise 1.3.21(b,c,e,g). *Hint:* Look at Theorem 3.8 for parts (e), (g).

9. (More on 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".

10. Let R be any ring. We say that a nonzero element a of R is a **zero divisor** if there is a nonzero $b \in R$ with $ab = 0$ or $ba = 0$. (This is the same definition of "zero divisor" as the one on p. 38 of your textbook, but there it is stated in a somewhat confusing way.) Now do Exercise 1.4.3.

11. Exercise 1.4.6.

    Hint: Look back at your notes from the first few classes, and your old HW.

12. (*) Let N be an integer with $N > 1$. Show that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{N}$ is not an integer.

    Hint: Let L be the least common multiple of the numbers $1, 2, 3, \ldots, N$. Then $L \cdot (1 + \frac{1}{2} + \cdots + \frac{1}{N})$ is an integer. Is that integer even or odd?