Math 4000/6000 – Homework #3
posted September 9, 2015; due at the **start of class** on September 14, 2015

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 $n \in \mathbb{N}$ can be written uniquely as a product of primes. Collecting all copies of the same prime allows us to write n as a product of prime powers,

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

where the p_i are primes and the e_i are positive integers. Moreover, this representation is unique up a reordering of the prime powers. For each prime p, define $v_p(n)$ as the power of p appearing in this representation of n, and put $v_p(n) = 0$ if p does not appear (i.e., if p does not divide n). For example, when $n = 171$, we have

$$171 = 3^2 \cdot 19,$$

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 $a, b, c \in \mathbb{N}$, then $v_p(a) = v_p(b) + v_p(c)$ for all primes p.

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

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

(d) Show that for any two natural numbers a and b,

$$\gcd(a, b) = \prod_p p^{\min\{v_p(a), v_p(b)\}}.$$

Here the product is over all primes p dividing both a and b. The notation $\min\{\cdot, \cdot\}$ means the smaller of two numbers.

(e) If a and b are two natural numbers, their *least common multiple*, denoted $\operatorname{lcm}(a, b)$, is the smallest natural number divisible by both of them. Show that

$$\operatorname{lcm}(a, b) = \prod_p p^{\max\{v_p(a), v_p(b)\}}.$$

Here the product is over all primes p dividing either a or b. The notation $\max\{\cdot, \cdot\}$ means the larger of two numbers.

(f) Using (d), show that if $a, b \in \mathbb{N}$ and M is any natural number divisible by a and b, then $\operatorname{lcm}(a, b) \mid M$. That is, the least common multiple divides every common multiple.

2. (Uniqueness of inverses) Suppose integers b and c are both inverses of a modulo m. Show that $b \equiv c \pmod{m}$.

3. (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 $a \in \mathbb{N}$.

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

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

5. Suppose p is a prime and that a is an integer satisfying $a \equiv 1 \pmod{p}$. Show that $a^p \equiv 1 \pmod{p^2}$, $a^{p^2} \equiv 1 \pmod{p^3}$ and in general $a^{p^k} \equiv 1 \pmod{p^{k+1}}$.

   Hint: Start by writing $a = 1 + pk$. Then apply the binomial theorem. Iterate.

6. Exercise 1.3.14.

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

8. Exercise 1.3.21(b,c,e,g).

9. (More on Pythagorean triples) Recall that an ordered triple of integers x, y, z is called **Pythagorean** if $x^2 + y^2 = z^2$. We showed in class that in every Pythagorean triple, at least one of x, y, z is a multiple of 3.

   (a) Show that in any Pythagorean triple, at least one of x, y, z is a multiple of 5.

   (b) Show that in any Pythagorean triple, at least one of x, y, z is a multiple of 4.

10. (Simultaneous congruences, the general case) Suppose we are given a system of congruences

$$\left\{\begin{array}{ll} x \equiv a_1 & \pmod{m_1} \\ x \equiv a_2 & \pmod{m_2} \\ \vdots & \\ x \equiv a_k & \pmod{m_k} \end{array}\right\}.$$

   (Here the a_i and m_i are integers, and we suppose each $m_i > 0$.) We say that this system is **admissible** if the following condition holds: Whenever d is an integer dividing a pair of moduli m_i and m_j, then $a_i \equiv a_j \pmod{d}$.

   (a) Show that each of the three systems

$$\left\{\begin{array}{ll} x \equiv 0 & \pmod{2} \\ x \equiv 1 & \pmod{2} \end{array}\right\}, \left\{\begin{array}{ll} x \equiv 3 & \pmod{9} \\ x \equiv 6 & \pmod{18} \end{array}\right\}, \quad \text{and} \quad \left\{\begin{array}{ll} x \equiv 15 & \pmod{35} \\ x \equiv 11 & \pmod{20} \end{array}\right\}$$

is **not** admissible. Do this by exhibiting, in each case, a value of d for which the admissibility criterion fails.

(b) Prove that if a system is not admissible, then it has no solution $x \in \mathbb{Z}$.

11. (continuation, *) Prove that if a system of congruences is admissible, then there **is** a solution $x \in \mathbb{Z}$.

    Hint: One approach is to reduce to the case when all the moduli are prime powers.

12. (*) Fix a positive integer $N \geq 3$. Prove that there are infinitely many primes p that are **not** congruent to 1 mod N.

    Hint: Try to adapt Euclid's proof of the infinitude of primes. If you already know primes $p_1, \ldots, p_k$ not 1 mod N, find another by examining the number $Np_1 \cdots p_k - 1$.