MATH 310 Midterm Exam 10/23/13 2:10–3:00 p.m.

Show complete work—that is, all the steps needed to completely justify your answer. Simplify your answers as much as possible. You may refer to theorems in the class notes.

1. (a) Define what $a \equiv b \pmod{m}$ means.

   (b) Find all solutions to $2x \equiv 2 \pmod{16}$.

   (c) Find all solutions to $5x \equiv 2 \pmod{210}$.

   Solution:

   (a) (5 points) See class notes.

   (b) (10 points) There are $\gcd(2, 16) = 2$ solutions modulo 16. The congruence can be reduced to $x \equiv 1 \pmod 8$, so the original congruence has the two solutions $x \equiv 1, 9 \pmod{16}$.

   (c) (10 points) $\gcd(5, 210) = 5$ does not divide 2, so there is no solution.

2. Suppose $\gcd(a, 561) = 1$.

   (a) Prove that $a^{560} \equiv 1 \pmod{m}$ for $m = 3$, 11, and 17.

   (b) Deduce that $a^{560} \equiv 1 \pmod{561}$.

   Solution:

   (a) (15 points) Because $561 = 3 \cdot 11 \cdot 17$, $\gcd(a, 561) = 1$ means that a is relatively prime to any of these m's. So we can use Fermat's Little Theorem:

$$\begin{aligned} a^{560} &= \left(a^2\right)^{280} \equiv 1 \pmod 3 \\ a^{560} &= \left(a^{10}\right)^{56} \equiv 1 \pmod{11} \\ a^{560} &= \left(a^{16}\right)^{35} \equiv 1 \pmod{17} . \end{aligned}$$

   (b) (10 points) This means that 3, 11, and 17 divide $a^{560} - 1$, and hence (because 3, 11, and 17 are pairwise relatively prime) so does $561 = 3 \cdot 11 \cdot 17$. (One could also invoke the Chinese Remainder Theorem here.)

   (You might read that a composite number m is called a *Carmichael number* if the congruence $a^{m-1} \equiv 1 \pmod{m}$ is true for all a that are relatively prime to m. We just proved that 561 is a Carmichael number.)

3. (a) Define the arithmetic functions $\tau(n)$ and $\mu(n)$.

   (b) Show that $\sum_{d|n} \mu(d)\, \tau(\frac{n}{d}) = 1$.

   Solution:

   (a) (10 points) See class notes.

   (b) (15 points) By definition, $\tau(n) = \sum_{d|n} 1$, so $\sum_{d|n} \mu(d)\, \tau(\frac{n}{d}) = 1$ follows by Möbius inversion (because the constant function 1 is multiplicative, as is $\tau(n)$, which we have proved in class.

4. (a) Define a primitive root mod m.

   (b) Find all primitive roots mod 7.

   Solution:

   (a) (10 points) See class notes.

   (b) (15 points) 3 is a primitive root because $3^2 \equiv 2$, $3^3 \equiv 6$ (and those are the only powers we need to check to not give 1 modulo 7). Thus there are $\phi(\phi(7)) = 2$ primitive roots modulo 7, the other one being $3^5 \equiv 5 \bmod 7$.