Math 437/537—Group Work #4
Wednesday, October 5, 2016

**Group work criteria:** Start from the top and understand one problem fully before moving on to the next one; quality is more important than quantity (although these group work problems are designed so that ideally you will be able to finish them all). I will be going from group to group during the hour, paying attention to the following aspects.

1. Effective communication—including both listening and speaking, with respect for other people and their ideas
2. Engagement with, and curiosity about, the material (for instance, how far might something generalize?)
3. Boldness—suggesting ideas, and trying plans even when they’re incomplete
4. Obtaining valid solutions (which are understood by everyone in the group) to the given problems

1. Warm-up question: for each of the moduli \( m \in \{1, 2, 4, 8\} \), find all the orders of all the reduced residue classes. Which of these moduli have primitive roots?

(Residue classes can be represented by any of their integers, of course, but that doesn’t change things like their order. Things are weird modulo 1: the residue class containing 0 is a reduced residue class, for one thing!)

(a) Modulo 1: the unique (reduced) residue class, represented by 1 for example, has order 1. Since \( \phi(1) = 1 \), that residue class is a primitive root (mod 1).

(b) Modulo 2: the unique reduced residue class is represented by 1 and has order 1. Since \( \phi(1) = 1 \), that residue class is a primitive root (mod 2).

(c) Modulo 4: the residue class represented by 1 has order 1, while the residue class represented by 3 (or by \(-1\)) has order 2. Since \( \phi(4) = 2 \), the latter residue class is a primitive root (mod 4).

(d) Modulo 8: the residue class represented by 1 has order 1, while the other three reduced residue classes (represented by 3, 5, and 7) all have order 2. Since \( \phi(8) = 4 \), there is no primitive root (mod 8).

(continued on next page)
2. In this question, we’ll figure out the orders of elements modulo higher powers of 2. We’ll use the notation $p^r \parallel n$ (pronounced “$p^r$ exactly divides $n$”) to mean that $p^r \mid n$ but $p^{r+1} \nmid n$, or equivalently that $v_p(n) = r$.

(a) Let $a$ be an odd integer. Show that for every $r \geq 3$, we have $2^r \mid (a^{2^{r-2}} - 1)$.

(b) Suppose that $a \equiv \pm 3 \pmod{8}$. Adapt your proof in part (a) to show that for every $r \geq 3$, we have $2^r \parallel (a^{2^{r-2}} - 1)$.

(c) Let $r \geq 3$. Show that the integers $\{5, 5^2, 5^3, \ldots, 5^{2^{r-2}}\}$ lie in distinct residue classes modulo $2^r$.

(d) Let $r \geq 3$. Show that the integers $\{\pm 5, \pm 5^2, \pm 5^3, \ldots, \pm 5^{2^{r-2}}\}$ form a reduced residue system modulo $2^r$.

(e) Show that there are no primitive roots modulo $2^r$ for $r \geq 3$.

(a) We proceed by induction on $r$. For the base case, $r = 3$, we must show $8 \mid (a^2 - 1)$ for every odd integer $a$; this is easily done by hand (splitting the odd integers into the four reduced residue classes modulo 8), and in fact was done in question #1 above. Alternatively, note that $a^2 - 1 = (a + 1)(a - 1)$ is the product of two consecutive even integers, and one of them must be divisible by (at least) 4 while the other one is of course divisible by 2. For the induction step, see the middle paragraph on page 103 of Niven, Zuckerman, & Montgomery.

(b) The facts from earlier parts of this question show that the order of every element (mod $2^r$) divides $2^{r-2}$ (when $r \geq 3$). Since $\phi(2^r) = 2^{r-1}$, this shows that there are no primitive roots (mod $2^r$). See also the middle paragraph on page 103 of Niven, Zuckerman, & Montgomery.

3. In this question, we’ll find some moduli that do not have primitive roots.

(a) Suppose that $m$ is an integer that can be written as $m = cd$ with $c, d \geq 3$ and $(c, d) = 1$. Show that every reduced residue class modulo $m$ has order dividing $\frac{1}{2}\phi(m)$. (Hint: look modulo $c$ and modulo $d$ separately.) Conclude that there are no primitive roots modulo $m$.

(b) Describe all integers that have not been ruled out in parts (a) or (b). (These are the moduli that could possibly have primitive roots; but you don’t have to determine whether they actually do have primitive roots or not.) We will see soon that all of these moduli do in fact have primitive roots.

(a) See the paragraph spanning pages 103–4 of Niven, Zuckerman, & Montgomery.

(b) The only integers not of the forms described in parts (a) and (b) are: 1, 2, and 4; powers of odd primes $p^k$ (including the primes $p^1$ themselves); and twice powers of odd primes $2p^k$. 