Math 437/537—Group Work #4
Tuesday, October 8, 2024

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). (The purposes of this part was to test that we know the exact rigorous definitions, in addition to their general gist.)
(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 classe 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 convenient reduced residue systems modulo higher powers of 2*. We'll use the notation* $p^r \| n$ *(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* $2^r \mid \left(a^{2^{r-2}} - 1\right)$*. (Hint: the right-hand side is a difference of squares and hence factors; use induction on* r*.)*

(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* $2^r \| \left(a^{2^{r-2}} - 1\right)$*. (Hint: a congruence modulo* 2^{r+1} *can detect whether* 2^r *exactly divides an integer.)*

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

(d) *Let* $r \geq 3$*. Show that the integers* $\left\{\pm 5, \pm 5^2, \pm 5^3, \ldots, \pm 5^{2^{r-2}}\right\}$ *form a reduced residue system modulo* 2^r*. (Hint: if two integers are distinct modulo* 4*, then they are distinct modulo* 2^r *for all* $r \geq 3$*.)*

(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 (in the excerpt in the following pages).

For proofs of parts (b)–(d), see the proof of Theorem 2.43 in Niven, Zuckerman, & Montgomery.

(e) 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.

Related remark—congruences modulo p^{r+1} can distinguish among the following possibilities for an integer n:

$$p \nmid n,\ p \| n,\ p^2 \| n,\ \ldots,\ p^{r-1} \| n,\ p^r \| n,\ p^{r+1} \mid n.$$

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 $2p^k$.

$\beta = 1, 2, \cdots$, or $\alpha - 1$. To prove that $\beta = \alpha - 1$, it suffices to show that

$$g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}. \tag{2.9}$$

We use induction to show that this holds for all $\alpha \geqslant 2$. By hypothesis, the order of $g \pmod{p^2}$ is $\phi(p^2) = p(p-1)$. Hence $g^{p-1} \not\equiv 1 \pmod{p^2}$, and we have (2.9) when $\alpha = 2$. By Fermat's congruence $g^{p-1} \equiv 1 \pmod{p}$, so we may write $g^{p-1} = 1 + b_1 p$ with $p \nmid b_1$. By the binomial theorem,

$$g^{p(p-1)} = (1 + b_1 p)^p = 1 + \binom{p}{1} b_1 p + \binom{p}{2} b_1^2 p^2 + \cdots.$$

Since $p > 2$ by hypothesis, $\binom{p}{2} = p(p-1)/2 \equiv 0 \pmod{p}$, and hence the above is $\equiv 1 + b_1 p^2 \pmod{p^3}$. This gives (2.9) when $\alpha = 3$. Thus we may write $g^{p(p-1)} = 1 + b_2 p^2$ with $p \nmid b_2$. We raise both sides of this to the pth power and repeat this procedure to find that $g^{p^2(p-1)} \equiv 1 + b_2 p^3 \pmod{p^4}$, which gives (2.9) for $\alpha = 4$. Continuing in this way, we conclude that (2.9) holds for all $\alpha \geqslant 2$, and the proof is complete.

The prime $p = 2$ must be excluded, for $g = 3$ is a primitive root (mod 4), but not (mod 8). Indeed it is easy to verify that $a^2 \equiv 1 \pmod{8}$ for any odd number a. As $\phi(8) = 4$, it follows that there is no primitive root (mod 8). Suppose that a is odd. Since $8 | (a^2 - 1)$ and $2 | (a^2 + 1)$, it follows that $16 | (a^2 - 1)(a^2 + 1) = a^4 - 1$. That is, $a^4 \equiv 1 \pmod{16}$. On repeating this argument we see that $a^8 \equiv 1 \pmod{32}$, and in general that $a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$ for $\alpha \geqslant 3$. Since $\phi(2^\alpha) = 2^{\alpha-1}$, we conclude that if $\alpha \geqslant 3$ then

$$a^{\phi(2^\alpha)/2} \equiv 1 \pmod{2^\alpha} \tag{2.10}$$

for all odd a, and hence that there is no primitive root $(\bmod 2^\alpha)$ for $\alpha = 3, 4, 5, \cdots$.

Suppose that p is an odd prime and that g is a primitive root $(\bmod p^\alpha)$. We may suppose that g is odd, for if g is even then we have only to replace g by $g + p^\alpha$, which is odd. The numbers $g, g^2, \cdots, g^{\phi(p^\alpha)}$ form a reduced residue system $(\bmod p^\alpha)$. Since these numbers are odd, they also form a reduced residue system $(\bmod 2p^\alpha)$. Thus g is a primitive root $(\bmod 2p^\alpha)$.

We have established that a primitive root exists modulo m when $m = 1$, 2, 4, p^α, or $2p^\alpha$, (p an odd prime), but that there is no primitive root $(\bmod 2^\alpha)$ for $\alpha \geqslant 3$. Suppose now that m is not a prime power or twice a prime power. Then m can be expressed as a product, $m = m_1 m_2$

with $(m_1, m_2) = 1$, $m_1 > 2$, $m_2 > 2$. Let $e = \text{l.c.m.}(\phi(m_1), \phi(m_2))$. If $(a, m) = 1$ then $(a, m_1) = 1$, so that $a^{\phi(m_1)} \equiv 1 \pmod{m_1}$, and hence $a^e \equiv 1 \pmod{m_1}$. Similarly $a^e \equiv 1 \pmod{m_2}$, and hence $a^e \equiv 1 \pmod{m}$. Since $2 | \phi(n)$ for all $n > 2$, we see that $2 | (\phi(m_1), \phi(m_2))$, so that by Theorem 1.13,

$$e = \frac{\phi(m_1)\phi(m_2)}{(\phi(m_1), \phi(m_2))} < \phi(m_1)\phi(m_2) = \phi(m).$$

Thus there is no primitive root in this case. We have now determined precisely which m possess primitive roots.

Theorem 2.41 *There exists a primitive root modulo m if and only if $m = 1, 2, 4, p^\alpha$, or $2p^\alpha$, where p is an odd prime.*

Theorem 2.37 (and its proof) generalizes to any modulus m possessing a primitive root.

Corollary 2.42 *Suppose that $m = 1, 2, 4, p^\alpha$, or $2p^\alpha$, where p is an odd prime. If $(a, m) = 1$ then the congruence $x^n \equiv a \pmod{m}$ has $(n, \phi(m))$ solutions or no solution, according as*

$$a^{\phi(m)/(n, \phi(m))} \equiv 1 \pmod{m} \tag{2.11}$$

or not.

For the general composite m possessing no primitive root, we factor m and apply the above to the prime powers dividing m.

Example 15 Determine the number of solutions of the congruence $x^4 \equiv 61 \pmod{117}$.

Solution We note that $117 = 3^2 \cdot 13$. As $\phi(9)/(4, \phi(9)) = 6/(4, 6) = 3$ and $61^3 \equiv (-2)^3 \equiv 1 \pmod{9}$, we deduce that the congruence $x^4 \equiv 61 \pmod{9}$ has $(4, \phi(9)) = 2$ solutions. Similarly $\phi(13)/(4, \phi(13)) = 3$ and $61^3 \equiv (-4)^3 \equiv 1 \pmod{13}$, so the congruence $x^4 \equiv 61 \pmod{13}$ has $(4, \phi(13)) = 4$ solutions. Thus by Theorem 2.20, the number of solutions modulo 117 is $2 \cdot 4 = 8$.

This method fails in case the modulus is divisible by 8, as Corollary 2.42 does not apply to the higher powers of 2. In order to establish an analogue of Corollary 2.42 for the higher powers of 2, we first show that 5 is nearly a primitive root $(\text{mod } 2^\alpha)$.

Theorem 2.43 *Suppose that* $\alpha \geqslant 3$. *The order of* $5 \pmod{2^\alpha}$ *is* $2^{\alpha-2}$. *The numbers* $\pm 5, \pm 5^2, \pm 5^3, \cdots, \pm 5^{2^{\alpha-2}}$ *form a system of reduced residues* $\pmod{2^\alpha}$. *If* a *is odd, then there exist* i *and* j *such that* $a \equiv (-1)^i 5^j \pmod{2^\alpha}$. *The values of* i *and* j *are uniquely determined* $\pmod 2$ *and* $\pmod{2^{\alpha-2}}$, *respectively.*

Proof We first show that $2^\alpha \| (5^{2^{\alpha-2}} - 1)$ for $\alpha \geqslant 2$. This is clear for $\alpha = 2$. If $a \equiv 1 \pmod 4$ then $2 \| (a+1)$, and hence the power of 2 dividing $a^2 - 1 = (a-1)(a+1)$ is exactly one more than the power of 2 dividing $a - 1$. Taking $a = 5$, we deduce that $2^3 \| (5^2 - 1)$. Taking $a = 5^2$, we then deduce that $2^4 \| (5^4 - 1)$, and so on. Now let h denote the order of $5 \pmod{2^\alpha}$. Since $h \mid \phi(2^\alpha)$ and $\phi(2^\alpha) = 2^{\alpha-1}$, we know that $h = 2^\beta$ for some β. But the least β for which $5^{2^\beta} \equiv 1 \pmod{2^\alpha}$ is $\beta = \alpha - 2$. Thus 5 has order $2^{\alpha-2} \pmod{2^\alpha}$, so that the numbers $5, 5^2, 5^3, \cdots, 5^{2^{\alpha-2}}$ are mutually incongruent $(\mathrm{mod}\, 2^\alpha)$. Of the $2^{\alpha-1}$ integers in a reduced residue system $(\mathrm{mod}\, 2^\alpha)$, half are $\equiv 1 \pmod 4$, and half are $\equiv 3 \pmod 4$. The numbers 5^j are all $\equiv 1 \pmod 4$. Since the powers of 5 lie in $2^{\alpha-2}$ distinct residue classes $(\mathrm{mod}\, 2^\alpha)$, and since $2^{\alpha-2}$ of the integers $(\mathrm{mod}\, 2^\alpha)$ are $\equiv 1 \pmod 4$, for any $a \equiv 1 \pmod 4$ there is a j such that $a \equiv 5^j \pmod{2^\alpha}$. For any integer $a \equiv 3 \pmod 4$, we observe that $-a \equiv 1 \pmod 4$, and hence that $-a \equiv 5^j \pmod{2^\alpha}$ for some j.

Corollary 2.44 *Suppose that* $\alpha \geqslant 3$ *and that* a *is odd. If* n *is odd, then the congruence* $x^n \equiv a \pmod{2^\alpha}$ *has exactly one solution. If* n *is even, then choose* β *so that* $(n, 2^{\alpha-2}) = 2^\beta$. *The congruence* $x^n \equiv a \pmod{2^\alpha}$ *has* $2^{\beta+1}$ *solutions or no solution according as* $a \equiv 1 \pmod{2^{\beta+2}}$ *or not.*

Proof Since a is odd, we may choose i and j so that $a \equiv (-1)^i 5^j \pmod{2^\alpha}$. As any x for which $x^n \equiv a \pmod{2^\alpha}$ is necessarily odd, we may suppose that $x \equiv (-1)^u 5^v \pmod{2^\alpha}$. The desired congruence then takes the form $(-1)^{nu} 5^{nv} \equiv (-1)^i 5^j \pmod{2^\alpha}$. By Theorem 2.43, this is equivalent to the pair of congruences $nu \equiv i \pmod 2$, $nv \equiv j \pmod{2^{\alpha-2}}$. If n is odd, then by Theorem 2.17 there exists exactly one $u \pmod 2$ for which the first congruence holds, and exactly one $v \pmod{2^{\alpha-2}}$ for which the second congruence holds, and hence there exists precisely one solution x in this case.

Suppose now that n is even. We apply Theorem 2.17 two more times. If $i \equiv 0 \pmod 2$ then the congruence $nu \equiv i \pmod 2$ has two solutions. Otherwise it has none. If $j \equiv 0 \pmod{2^\beta}$ then the congruence $nv \equiv j \pmod{2^{\alpha-2}}$ has exactly 2^β solutions. Otherwise it has none. Thus the congruence $x^n \equiv a \pmod{2^\alpha}$ has $2^{\beta+1}$ solutions or no solution, according as $a \equiv 5^j \pmod{2^\alpha}$, $j \equiv 0 \pmod{2^\beta}$, or not. From Theorem 2.43 we know