Abstract Algebra
Day 12 Class Work Solutions

1. Consider $3 \in U_7$. We've seen that $\text{ord}(3) = 6$.

   (a) Find 3^{48}. Explain how you found it.

   ← Computing 3^{48} is not highly recommended.

   Solution. We have $48 = 6 \cdot 8$ so that $3^{48} = (3^6)^8 = 1^8 = 1$.

   (b) In U_7, determine whether it's possible that $3^{263} = 1$. Explain your reasoning.

   Solution. No, since 6 is not a divisor of 263. See Problem #5 for more details.

2. Let g be an element of a group with $\text{ord}(g) = 6$.

   (a) Find g^{48}. Explain how you found it.

   Solution. We have $48 = 6 \cdot 8$ so that $g^{48} = (g^6)^8 = \varepsilon^8 = \varepsilon$.

   (b) Determine whether it's possible that $g^{263} = \varepsilon$. Explain your reasoning.

   Solution. No, since 6 is not a divisor of 263. See Problem #5 for more details.

3. **Prove:** Let g be an element of a group with $\text{ord}(g) = n$. If $n \mid k$, then $g^k = \varepsilon$.

   Hint: See part (a) in each of the two problems above.

   Proof. Assume $n \mid k$, so that $k = n \cdot q$ for some integer q. Since $\text{ord}(g) = n$, we have $g^n = \varepsilon$. Thus, $g^k = g^{n \cdot q} = (g^n)^q = \varepsilon^q = \varepsilon$, as desired. ■

4. Our friends are trying to find the remainder when dividing 263 by 6.

   (a) Elizabeth: "$263 = 6 \cdot 42 + 11$, so the remainder is 11." How would you respond?

   (b) Anita: "$263 = 6 \cdot 44 + (-1)$, so the remainder is -1." How would you respond?

   ← Anita's "remainder" is useful in number theory.

   (c) What is the correct remainder anyway?

   Solution. The remainder r must be (a) less than the divisor, i.e., $r < 6$ and (b) non-negative, i.e., $r \geq 0$. Thus, Elizabeth's remainder is too big, and Anita's remainder is negative. We have $263 = 6 \cdot 43 + 5$, so the correct remainder is 5.

5. Once again, let's g be an element of a group with $\text{ord}(g) = 6$.

   (a) Use your result from Problem #4(c) to explain why $g^{263} = g^5$.

   Solution. We have $g^{263} = g^{6 \cdot 43 + 5} = (g^6)^{43} \cdot g^5 = \varepsilon^{43} \cdot g^5 = g^5$.

   (b) Explain why $g^5 \neq \varepsilon$.

   ← $\text{ord}(g) = 6$ means...

   Solution. Since $\text{ord}(g) = 6$, we know that $n = 6$ is the *smallest* positive exponent such that $g^n = \varepsilon$. That means g^1, g^2, g^3, g^4, g^5 are all *not* equal to ε.

   (c) Use parts (a) and (b) to explain why $g^{263} \neq \varepsilon$.

   Solution. In parts (a) and (b), we showed that $g^{263} = g^5$ and $g^5 \neq \varepsilon$. Thus, $g^{263} \neq \varepsilon$.

6. **Prove:** Let g be an element of a group with $\text{ord}(g) = n$. If $n \nmid k$, then $g^k \neq \varepsilon$.

   Note: $n \nmid k$ is a short-hand for "n is *not* a divisor of k."

   Proof. Assume $n \nmid k$. Then $k = n \cdot q + r$ for some q, $r \in \mathbb{Z}$ with $0 < r < n$ (i.e., r is a nonzero remainder). We have $g^k = g^{n \cdot q + r} = (g^n)^q \cdot g^r = \varepsilon^q \cdot g^r = g^r$, so that $g^k = g^r$. Since r is positive and less than $n = \text{ord}(g)$, we know that $g^r \neq \varepsilon$. Thus $g^k \neq \varepsilon$, as desired. ■

7. (a) In U_7, find the value of 3^{-220}. (That's 3 raised to the power -220.) **Ans:** $3^{-220} = 2$.

   Solution. We have $6 \mid 222 \implies 3^{222} = 1$. Thus, $3^{-220} = 3^{-220} \cdot 3^{222} = 3^2 = 2$.

   (b) Again, let g be an element of a group with $\mathrm{ord}(g) = 6$. Find the smallest non-negative integer k such that $g^{-220} = g^k$. **Ans:** $k = 2$.

   Solution. We have $6 \mid 222 \implies g^{222} = \varepsilon$. Thus, $g^{-220} = g^{-220} \cdot g^{222} = g^2$, so $k = 2$.

8. Yet again, let g be an element of a group with $\mathrm{ord}(g) = 6$. (Or just use $g = 3$ in U_7.)

   (a) Are g^{20} and g^{32} equal? Why or why not?

   Solution. Yes. We have $g^{32} = g^{20+6\cdot 2} = g^{20} \cdot (g^6)^2 = g^{20} \cdot \varepsilon^2 = g^{20}$.

   (b) What about g^{123405} and g^{123465}? How do you know?

   Solution. Yes. We have

   $$g^{123465} = g^{123405+6\cdot 10} = g^{123405} \cdot (g^6)^{10} = g^{123405} \cdot \varepsilon^{10} = g^{123405}.$$

   (c) What about g^{800} and g^{862}? How do you know? **Ans to (c):** No.

   Solution. No, the difference of the exponents, namely 62, is not divisible by 6.

   (d) What about g^{-241} and g^{359}? How do you know?

   Solution. Yes, the difference of the exponents, namely 600, is divisible by 6.

   (e) What's going on here? Can you generalize and justify?

   Solution. See Problem #9 below.

9. Consider the following theorem:

   Theorem. Let g be an element of a group with $\mathrm{ord}(g) = n$. Then $n \mid (k - \ell)$ if and only if $g^k = g^\ell$.

   (a) Come up with a few examples to illustrate the theorem.

   Solution. See Problem #8 above.

   (b) Prove the theorem. Note that you have two implications to prove here.

10. Let g be an element of a group with $\mathrm{ord}(g) = 18$. Find each of the following.

    (a) $\mathrm{ord}(g^3)$ (b) $\mathrm{ord}(g^2)$ (c) $\mathrm{ord}(g^4)$ (d) $\mathrm{ord}(g^{10})$ (e) $\mathrm{ord}(g^7)$

    What conjecture do you have? Can you *prove* it?

    Solution. We have $\mathrm{ord}(g^3) = 6$, $\mathrm{ord}(g^2) = 9$, $\mathrm{ord}(g^4) = 9$, $\mathrm{ord}(g^{10}) = 9$, and $\mathrm{ord}(g^7) = 18$.

11. Let a, b be elements of a commutative group.

    (a) Suppose $\mathrm{ord}(a) = 3$ and $\mathrm{ord}(b) = 5$. Explain why $(ab)^{15} = \varepsilon$.

    Solution. Since the group is commutative, we have $(ab)^{15} = a^{15}b^{15}$. Furthermore, $a^3 = \varepsilon$ and $b^5 = \varepsilon$, since $\mathrm{ord}(a) = 3$ and $\mathrm{ord}(b) = 5$. Therefore, we have

    $$(ab)^{15} = a^{15}b^{15} = (a^3)^5(b^5)^3 = \varepsilon^5\varepsilon^3 = \varepsilon.$$

    (b) Suppose $\mathrm{ord}(a) = 4$ and $\mathrm{ord}(b) = 9$. Explain why $(ab)^{36} = \varepsilon$.

    Solution. We have $a^4 = \varepsilon$ and $b^9 = \varepsilon$. So, $(ab)^{36} = a^{36}b^{36} = (a^4)^9(b^9)^4 = \varepsilon^9\varepsilon^4 = \varepsilon$.

(c) Suppose $\text{ord}(a) = 4$ and $\text{ord}(b) = 6$. Explain why $(ab)^{24} = \varepsilon$.

Solution. We have $a^4 = \varepsilon$ and $b^6 = \varepsilon$. So, $(ab)^{24} = a^{24}b^{24} = (a^4)^6(b^6)^4 = \varepsilon^6\varepsilon^4 = \varepsilon$.

(d) Elizabeth says, "In part (c), I showed $(ab)^{24} = \varepsilon$. That means $\text{ord}(ab) = 24$." Do you agree or disagree with her? Explain your reasoning.

Solution. Disagree. For a group element g, if $g^{24} = \varepsilon$, then we can conclude that $\text{ord}(g)$ is a *divisor of* 24 (by the contrapositive of the implication in Problem #6). However, $\text{ord}(g)$ does not need to be *equal to* 24.

12. Let a, b be elements of a commutative group, each with finite order. Using a counterexample, show that the following statement is false: $\text{ord}(ab) = \text{ord}(a) \cdot \text{ord}(b)$.

13. **Prove:** Let a, b be elements of a commutative group with $m = \text{ord}(a)$ and $n = \text{ord}(b)$. If $\gcd(m, n) = 1$, then $\text{ord}(ab) = mn$.