Abstract Algebra
Day 12 Class Work

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

2. Let g be an element of a group with $\text{ord}(g) = 6$.
   (a) Find g^{48}. Explain how you found it.
   (b) Determine whether it's possible that $g^{263} = \varepsilon$. Explain your reasoning.

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.

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?

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 $g^{263} = g^5$.
   (b) Explain why $g^5 \neq \varepsilon$. ← $\text{ord}(g) = 6$ means...
   (c) Use parts (a) and (b) to explain why $g^{263} \neq \varepsilon$.

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."

7. (a) In U_7, find the value of 3^{-220}. (That's 3 raised to the power -220.) **Ans:** $3^{-220} = 2$.
   (b) Again, let g be an element of a group with $\text{ord}(g) = 6$. Find the smallest non-negative integer k such that $g^{-220} = g^k$. **Ans:** $k = 2$.

8. Yet again, let g be an element of a group with $\text{ord}(g) = 6$. (Or just use $g = 3$ in U_7.)
   (a) Are g^{20} and g^{32} equal? Why or why not?
   (b) What about g^{123405} and g^{123465}? How do you know?
   (c) What about g^{800} and g^{862}? How do you know? **Ans to (c):** No.
   (d) What about g^{-241} and g^{359}? How do you know?
   (e) What's going on here? Can you generalize and justify?

9. Consider the following theorem:

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

   (a) Come up with a few examples to illustrate the theorem.
   (b) Prove the theorem. Note that you have two implications to prove here.

© 2022 Ryota Matsuura

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

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

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

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

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

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

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

    (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.

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 $\text{ord}(ab) = mn$.