

Session 8, July 18**Units, Orders, and Fermat's Little Theorem**

1. Find the order of each element in \mathbf{U}_7 .
2. Find the order of each element in \mathbf{U}_{11} .
3. Find the order of each element in \mathbf{U}_9 .
4. Find the order of each element in \mathbf{U}_{15} .
5. What is the order of 4 in \mathbf{Z}_{12} ? What is the order of 5 in \mathbf{Z}_{10} ? Explain.
6. Which elements in \mathbf{Z}_{18} have orders? Explain.
7. If u is some element in \mathbf{U}_{29} , what could the order of u be? Explain.
8. If u is some element in \mathbf{U}_{35} , what could the order of u be? Explain.
9. In \mathbf{U}_5 , find $1^4, 2^4, 3^4$, and 4^4 .
10. In \mathbf{U}_7 , find $1^6, 2^6, 3^6, 4^6, 5^6$, and 6^6 .
11. In \mathbf{U}_9 , find $1^6, 2^6, 4^6, 5^6, 7^6$, and 8^6 .
12. In \mathbf{U}_{12} , find $1^4, 5^4, 7^4$, and 11^4 .
13. In \mathbf{U}_{13} , find the smallest natural number n such that $u^n = 1 \pmod{13}$ for all u .
14. Do the same as in Problem 13 for \mathbf{U}_{15} and for \mathbf{U}_{18} . Any conjectures?

Fermat's Little Theorem (as opposed to his last?) states the following:

Let p be prime. For any $u \in \mathbf{U}_p$, $u^{p-1} = 1 \pmod{p}$.

15. Generalize the statement of FLT for any unit group \mathbf{U}_n (where n is not necessarily prime).
16. Prove the following statement. You may assume FLT and its generalization.

Let $u \in \mathbf{U}_n$ and suppose $k = \text{order of } u$. Then $k \mid \varphi(n)$. (In other words, the order of an element divides the order of the group.)

Hint: Use concrete examples. What goes wrong if, in \mathbf{U}_{11} , the order of 3 were 7?

17. Consider $\mathbf{U}_7 = \{1, 2, 3, 4, 5, 6\}$. For any $u \in \mathbf{U}_7$, define $u \cdot \mathbf{U}_7$ as the set $\{u \cdot 1, u \cdot 2, u \cdot 3, u \cdot 4, u \cdot 5, u \cdot 6\}$. For example, $4 \cdot \mathbf{U}_7 = \{4 \cdot 1, 4 \cdot 2, 4 \cdot 3, 4 \cdot 4, 4 \cdot 5, 4 \cdot 6\}$. Find $u \cdot \mathbf{U}_7$ for $u = 1, 2, 3, 4, 5$, and 6. Any conjectures?
18. Prove Fermat's Little Theorem. Hint: Use your results from Problem 17.

Take a breather before going to the next page.

Time to put on some major thinking caps! (As if you haven't thought enough already...)

19. How are unit groups, order, and Fermat's Little Theorem related to the decimal expansion problems that you did on Days 1-3? Be as specific as possible, using concrete examples.
20. For each n , find the order of 10 (mod n). Compare the order to the period of $\frac{1}{n}$ in base 10. Explain what is going on and why.
- (a) $n = 7$ (b) $n = 11$ (c) $n = 13$
 (d) $n = 8$ (e) $n = 22$ (f) $n = 5$
 (g) $n = 41$
21. Predict the period of the repeating decimal for $\frac{1}{107}$. How many possibilities are there?

Some exploratory problems to keep you entertained...

22. Consider the factorization of $x^4 - 1$ in $\mathbf{Z}_5[x]$.

$$\begin{aligned}
 x^4 - 1 &= (x^2 - 1)(x^2 + 1) \\
 &= (x + 1)(x - 1)(x^2 + 1) \\
 &= (x - 4)(x - 1)(x^2 - 4) && \text{(Why?)} \\
 &= (x - 4)(x - 1)(x + 2)(x - 2) \\
 &= (x - 4)(x - 1)(x - 3)(x - 2) && \text{(Why?)} \\
 &= (x - 1)(x - 2)(x - 3)(x - 4)
 \end{aligned}$$

Factor $x^6 - 1$ in $\mathbf{Z}_7[x]$. Factor $x^{10} - 1$ in $\mathbf{Z}_{11}[x]$. How is this related to Fermat's Little Theorem?

23. Let's check if 1413 is divisible by 9. Let $\rho(n)$ be the sum of the digits of n . So, $\rho(1413) = 1 + 4 + 1 + 3 = 9$. Since 9 divides $\rho(1413)$, it follows that 9 divides 1413, also. Explore this divisibility test. Does it always work? If so, why?
- Hint: Think base 10 and mod 9.
24. What is the order of 28 in \mathbf{U}_{29} ? of 16 in \mathbf{U}_{29} ? of $28 \cdot 16$ in \mathbf{U}_{29} ? Now consider \mathbf{U}_{71} . What is the order of 7, of 2, of $7 \cdot 2$, of 54, of 51, of $54 \cdot 51$? Any conjectures?