Math 6 – Modular Arithmetic (WS #1)

Let $\mathbf{Z}_m$ be the set of integers taken "modulo m." Arithmetic in $\mathbf{Z}_m$ is the same as normal integer arithmetic with the extra rule that $m = 0$. We have seen that $\mathbf{Z}_m$ has exactly m elements, which we can write as $0, 1, 2, \ldots, m-1$.

Getting practice with arithmetic

1. What are the answers to the following arithmetic problems in $\mathbf{Z}_m$? Express your answer as one of $0, 1, 2, \ldots, m-1$.

$$1 + 1 = \underline{\qquad} \text{ (in } \mathbf{Z}_2\text{)}, \quad 113 + 189 = \underline{\qquad} \text{ (in } \mathbf{Z}_3\text{)}, \quad -23 \cdot 19 = \underline{\qquad} \text{ (in } \mathbf{Z}_7\text{)}$$

2. (continued below) Compute the sequence $1 = 2^0, 2^1, 2^2, 2^3, 2^4, 2^5, \ldots$ modulo 15 until you notice a pattern. What is that pattern? Do the same for powers of 3.
3. We saw that $2x = 1$ had the solution $x = 6$ in $\mathbf{Z}_{11}$. Without checking by hand all the other elements of $\mathbf{Z}_{11}$, can you show that $x = 6$ is the only solution to $2x = 1$? [Hint: what happens if you multiply both sides of the $\mathbf{Z}_{11}$-equation $2x = 1$ by 6.]

Homework

1. Which integers from 1 to 50 are the same as -3 in $\mathbf{Z}_7$?
2. Find the following elements in $\mathbf{Z}_5$: $-1, \frac{1}{2}, \frac{1}{3}$ and the square roots of -1. Which of these can you find in $\mathbf{Z}_6$? in $\mathbf{Z}_{10}$? in $\mathbf{Z}_{11}$? in $\mathbf{Z}_{13}$?
3. Pick ten positive integers m between 5 and 30. For each of these m, determine which of $0, 1, 2, \ldots, m-1$ are units modulo m, expressing your answers in a table like the following (which is an example for $m = 12$):

	0	1	2	3	4	5	6	7	8	9	10	11
unit in $\mathbf{Z}_{12}$?		✓				✓		✓				✓

   Formulate a guess as to when an element of $\mathbf{Z}_m$ is a unit mod m. Be sure that your guess agrees with your data so far!

4. Let a be an element of $\mathbf{Z}_{15}$. (Thus a is one of $0, 1, 2, \ldots, 14$.) For which of these a does the list $a, a^2, a^3, \ldots$ contain 1? (For example, you should have found when working out the 2nd practice problem above that the list contains 1 when $a = 2$ but not when $a = 3$.)
5. (**Zero product property**) A familiar fact from ordinary arithmetic is that whenever two integers multiply to be zero, one (or both) of them is zero. We say that the system of integers has the *zero product property.*

   Here we investigate whether the zero product property holds for our new systems of arithmetic. Let $m = 11$. Is it true that if two numbers in $\mathbf{Z}_{11}$ multiply to 0, then one of them has to be zero to start with? [1]

   What if we ask the same question for $\mathbf{Z}_{10}$?

   For every m from $m = 2$ to $m = 20$, determine whether or not $\mathbf{Z}_m$ has the zero product property. On the basis of this data, formulate a guess as to exactly when $\mathbf{Z}_m$ has the zero product property.

[1] Example/explanation: $22 \cdot 3 = 66$, and $66 = 0$ in $\mathbf{Z}_{11}$, so we have an example of two numbers multiplying to zero in $\mathbf{Z}_{11}$. But in this case one of the two numbers is 0, because $22 = 0$ in $\mathbf{Z}_{11}$. So this example *does not* contradict the zero product property.