Discrete Structures

Worksheet 10

Spring 2022
February 4

Recall the following notation:

$$a \equiv b \pmod{n} \iff \left(\begin{array}{c}\text{there exists some } k \in \mathbf{Z} \text{ so} \\ \text{that } a = kn + b, \text{ for } b \in [0, n)\end{array}\right)$$

This means that $11 \equiv 2 \pmod{3}$ and $5 \equiv 2 \pmod{3}$, and also $11 \equiv 5 \pmod{3}$.

---

1. **Warm up:** Explain in your own words (not using textbook definitions) what the following expressions mean. All variables $a, \ldots, \ell$ are integers.

   (a) $a \mid b$

   (b) $c \mod d = e$

   (c) $\lfloor \frac{f}{2} \rfloor$

   (d) $(ghijk)_\ell$

2. Let $n \in \mathbf{N}$.

   (a) Prove that $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

   (b) If $n \geqslant 2$, prove that $n^4 + n^2 + 1$ is composite.

3. Complete the rows in the table below by converting numbers to different bases.

base 2	base 8	base 10	base 16
1010101			
	767676		
		90909	
			AF6446FA

4. A 12 digit number $x_1 x_2 \cdots x_{12}$ is named a *valid UPC* (Universal Product Code), or a barcode, iff the digits satisfy the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{12}.$$

   Replace the digit `X` in the following number to make it a valid UPC: `780194 55330X`.

5. This question is about $\mathbf{Z}_{14} = \{0, 1, 2, \ldots, 13\}$, with the associated multiplication and addition functions.

   (a) How many elements are in the following sets:

$$M_2 = \{2n \mod 14 \; : \; n \in \mathbf{Z}_{14}\},$$
$$M_3 = \{3n \mod 14 \; : \; n \in \mathbf{Z}_{14}\},$$
$$M_7 = \{7n \mod 14 \; : \; n \in \mathbf{Z}_{14}\}?$$

   Can you explain why the sizes are as they are? *Hint: Note that* $14 = 7 \cdot 2$.

   (b) The *order* of an element $n \in \mathbf{Z}_{14}$ is the minimum positive power $k \in \mathbf{Z}$ such that $n^k \equiv n \pmod{14}$. Find the order of the elements $2, 3, 7$ (you may use a calculator). Can you explain why the orders are as they are?

---

6. Complete the following tasks for next lab (Tuesday). They will be presented at the beginning of the lab.

   (a) Let n and k be positive integers.

      i. Express $\lceil \frac{n}{k} \rceil = a$ and $\lfloor \frac{n}{k} \rfloor = b$ as statements without the ceiling and floor symbols, and beginning with "There exists...".

      ii. Prove that $\lceil \frac{n}{k} \rceil = \lfloor \frac{n-1}{k} \rfloor + 1$.

   (b) Let a, b, c be positive integers. Show that if $a \mid b$ and $b \mid c$, then $a \mid c$.

   (c) *(from Cummings Ex 9.25)* Let $a, b \in \mathbf{Z}$. For each of the following relations, explain why it is an equivalence relation, or give a counterexample showing it is not an equivalence relation.

      i. $a \sim b$ whenever $a \equiv b \pmod 2$ and $a \equiv b \pmod 3$

      ii. $a \sim b$ whenever $a \equiv b \pmod 2$ or $a \equiv b \pmod 3$

   (d) *(from Cummings Ex 2.40)* Consider the following statement (by Evelyn Lamb):

   Every prime number greater than 3 is precisely 1 number away from a multiple of 3!

   Prove that this statement is true both when the exclamation mark is considered as punctuation (not a factorial) or as mathematics (as a factorial).