Math 302 Worksheet 6: Congruence and modular arithmetic

Consider the following table of integers:

0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15
16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59

Problem 6.1. How are integers within the same column related? Can you write an algebraic formula which represents all the integers in a single column?

Problem 6.2. Explain how the table could be extended to include every integer. In which column does 1533 belong? What about -756?

Problem 6.3. Two integers a and b are said to be *congruent modulo* 4 if they lie in the same column. In this case, we write $a \equiv b \pmod 4$. Give an algebraic definition of congruence modulo 4 (that is, a definition which does not refer to position in the table).

Problem 6.4. When you add two numbers in the first column, in which column does the sum lie? Is the same true if you add two numbers in one of the other columns? What about two numbers from different columns? Complete the addition table below using the column headings 0, 1, 2, and 3.

+	0	1	2	3
0				
1				
2				
3				

Problem 6.5. Repeat your experimentation from the previous problem, this time with multiplication. Complete the multiplication table below.

×	0	1	2	3
0				
1				
2				
3				

Problem 6.6. Let a and b be integers, and n a natural number. Give a definition of $a \equiv b \pmod{n}$.

Problem 6.7. Which of the following congruence statements are true?

(a) $7 \equiv 19 \pmod{3}$
(b) $21 \equiv -8 \pmod{6}$
(c) $53 \equiv 108 \pmod{7}$
(d) $-58 \equiv 14 \pmod{8}$

Problem 6.8. Find all integers $n \geq 1$ for which $29 \equiv 47 \pmod{n}$.

Definition. Let a and n be integers with $n > 0$. The *least nonnegative residue of a modulo n* is the unique integer $0 \leq b < n$ with $a \equiv b \pmod{n}$.

Problem 6.9. Let a and n be integers with $n > 0$. Why does a have a unique least nonnegative residue modulo n?

Problem 6.10. Fill in the blanks below with the least nonnegative residue of each sum or product.

(a) $19 + 42 \equiv$ ____ $\pmod{8}$
(b) $437 \cdot 234 \equiv$ ____ $\pmod{5}$
(c) $15(34 + 11)(25 + 62) \equiv$ ____ $\pmod{3}$

There is a way to do these quickly in your head without a calculator. Can you see how?

Definition. Let n be a natural number. A set of integers $A = \{a_1, a_2, \ldots, a_k\}$ is called a *complete residue system modulo n* if every integer is congruent modulo n to exactly one element of A.

Problem 6.11. Which of the following are complete residue systems modulo 6? Why or why not?

(a) $\{0, 1, 2, 3, 4, 5\}$
(b) $\{1, 8, 15, 22, 29\}$
(c) $\{-6, 21, 32, 57, 61, 102, 117, 213\}$
(d) $\{-5, -2, 0, 14, 19, 27\}$
(e) $\{-68, -12, -7, 14, 27, 85\}$