21-110: Problem Solving in Recreational Mathematics

Homework assignment 5 solutions

Problem 1. Make an addition table and a multiplication table for the integers modulo 7 (in other words, for remainders after division by 7).

Solution. There are only seven integers modulo 7 (in other words, there are only seven possible remainders after division by 7). These integers are 0, 1, 2, 3, 4, 5, and 6. So our addition and multiplication tables need only include these entries.

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

These tables indicate, for example, that $4 + 5 \equiv 2 \pmod 7$ and $3 \times 6 \equiv 4 \pmod 7$. □

Problem 2. The country of Euclidia has an awkward currency system. The basic unit of currency there is called the yakblat. There are only two kinds of coins: the pizpaz, which is worth 24 yakblats, and the burbox, which is worth 57 yakblats. (In particular, there is no such thing as a one-yakblat coin.)

When I visited Euclidia, I went into a shop to buy a piece of bubble gum, which cost 15 yakblats. Paying for such an item in Euclidia requires the making of change: I significantly overpaid when I handed the cashier my coins, and then the cashier handed me the proper amount of change so that my net purchase came out to 15 yakblats. Fortunately the cashier and I both had big buckets of coins, so we had as many pizpazzes and burboxes as we required.

Your goal is to find a way to pay exactly 15 yakblats in such a transaction.

(a) Write a linear Diophantine equation representing this situation. You will need to introduce appropriate variables. Explain, carefully and precisely, what quantities your variables represent.

(b) Find a solution to the linear Diophantine equation you wrote in part (a). You might use the extended Euclidean algorithm described on the handout given in class, or the method described on pages 127–137 of *Problem Solving Through Recreational Mathematics.* Or you can use a different method.

(c) Interpret your solution from part (b). In other words, what coins should I hand the cashier, and what coins should the cashier give me as change?

Solution.

(a) Let P represent the number of pizpazzes I should give to the cashier, and let B represent the number of burboxes I should give to the cashier. A negative value for P or B will represent coins given back to me by the cashier. Note that it does not make sense for me to give the cashier some pizpazzes and then get some pizpazzes back in change; I might as well have not given those pizpazzes at all. So either I will give the cashier only pizpazzes and receive only burboxes back in change, or else I will give the cashier only burboxes and receive only pizpazzes back in change. Therefore, one of P or B will be positive, and the other will be negative.

Each pizpaz is worth 24 yakblats, so the number of yakblats I give to the cashier in the form of pizpazzes is $24P$. Similarly, each burbox is worth 57 yakblats, so the number of yakblats I give to the cashier in the form of burboxes is $57B$. (One of these will be negative, of course.) In all, the total number of yakblats I give to the cashier is $24P + 57B$. This should equal 15, since my goal is to pay exactly 15 yakblats. So a linear Diophantine equation representing this situation is

$$24P + 57B = 15.$$

(b) To solve the Diophantine equation $24P + 57B = 15$, we will use the extended Euclidean algorithm. The process of this algorithm is presented below in a table, in the same way as the example in the handout (available online at `http://www.math.cmu.edu/~bkell/21110-2010s/extended-euclidean.html`). We are using $a = 57$ and $b = 24$. (Note that this variable b is different from the variable B we are using to represent the number of burboxes I should give to the cashier.)

	c	d	q	r	Conclusion
Step 1	57	24			
Step 2	57	24	2	9	$9 = 57 - 2(24)$ $= a - 2b$
Step 4	24	9			
Step 2	24	9	2	6	$6 = 24 - 2(9)$ $= b - 2(a - 2b)$ $= b - 2a + 4b$ $= -2a + 5b$
Step 4	9	6			
Step 2	9	6	1	3	$3 = 9 - 1(6)$ $= (a - 2b) - 1(-2a + 5b)$ $= a - 2b + 2a - 5b$ $= 3a - 7b$
Step 4	6	3			
Step 2	6	3	2	0	$0 = 6 - 2(3)$ $= (-2a + 5b) - 2(3a - 7b)$ $= -2a + 5b - 6a + 14b$ $= -8a + 19b$
Step 3	$\gcd(57, 24) = 3 = 3(57) - 7(24)$				

So we have found that

$$24(-7) + 57(3) = 3.$$

Multiplying both sides of this equation by 5, we get

$$24(-35) + 57(15) = 15.$$

Therefore, one solution to the linear Diophantine equation $24P + 57B = 15$ is $P = -35$, $B = 15$.

(c) The solution $P = -35$, $B = 15$ means that, in order to pay exactly 15 yakblats, I should give the cashier 15 burboxes and receive 35 pizpazzes in change. This checks out, because 15 burboxes are worth 855 yakblats, and 35 pizpazzes are worth 840 yakblats. □

[Note: There are infinitely many possible solutions to the Diophantine equation $24P + 57B = 15$. The solution $P = -35$, $B = 15$ is not the simplest. At the end of the extended Euclidean algorithm, we found that $0 = -8a + 19b = 24(19) + 57(-8)$. Since this is zero, we can add this to any solution to obtain another solution. If we do this twice to the solution we found, we can get a solution that requires fewer coins to change hands:

$$\begin{array}{rc} & 24(-35) + 57(15) = 15 \\ + \big[& 24(19) + 57(-8) = 0 \quad \big] \\ \hline & 24(-16) + 57(7) = 15 \\ + \big[& 24(19) + 57(-8) = 0 \quad \big] \\ \hline & 24(3) + 57(-1) = 15. \end{array}$$

This solution ($P = 3$, $B = -1$) means that I can pay 15 yakblats by handing the cashier 3 pizpazzes and receiving 1 burbox as change.]

Problem 3. Let

$$\begin{aligned} A &= \{1,2,3,4,5\}, \\ B &= \{\, x \mid x \text{ is even} \,\}, \\ C &= \{\, x \mid x \text{ is a multiple of } 3 \,\}, \text{ and} \\ D &= \{\, x \mid x \text{ is prime} \,\}, \end{aligned}$$

where the universal set is the set of all positive integers no greater than 20.

(a) What is $A \cup C$? What is the cardinality of $A \cup C$?

(b) What is $B \cap C$? What is the cardinality of $B \cap C$?

(c) What are $A \setminus D$ and $D \setminus A$? What are the cardinalities of these sets?

(d) What is $\overline{A}$? What is the cardinality of $\overline{A}$?

(e) What is $(B \cup D) \cap \overline{A}$? What is the cardinality of this set?

Solution.

(a) First, it is helpful to explicitly write out the elements of the set C:

$$C = \{3, 6, 9, 12, 15, 18\}.$$

Now $A \cup C$ is the set of all numbers that are in A or C (or both), so

$$A \cup C = \{1, 2, 3, 4, 5, 6, 9, 12, 15, 18\}.$$

The cardinality of this set is 10, because it has 10 elements. In symbols, we can write $|A \cup C| = 10$.

(b) The elements of $B \cap C$ are the numbers that are in both B and C, that is, the numbers that are both even and multiples of 3. So

$$B \cap C = \{6, 12, 18\} = \{\, x \mid x \text{ is a multiple of } 6 \,\}.$$

The cardinality of this set is 3, i.e., $|B \cap C| = 3$.

(c) The elements of the set D are

$$D = \{2, 3, 5, 7, 11, 13, 17, 19\}.$$

The set $A \setminus D$ is the set of all elements of A that are not elements of D, so

$$A \setminus D = \{1, 4\}.$$

Similarly, the set $D \setminus A$ is the set of all elements of D that are not elements of A, so

$$D \setminus A = \{7, 11, 13, 17, 19\}.$$

The cardinalities of these sets are

$$|A \setminus D| = 2 \qquad \text{and} \qquad |D \setminus A| = 5.$$

(d) The set $\overline{A}$, i.e., the complement of A, is the set of all elements of the universal set that are not elements of A. So

$$\overline{A} = \{6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}.$$

The cardinality of this set is 15, i.e., $\left|\,\overline{A}\,\right| = 15$.

(e) First we should find $B \cup D$. The set $B \cup D$ is the set of all numbers that are in either B or D (or both), that is, the set of all numbers that are either even or prime. So

$$B \cup D = \{2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20\}.$$

Now $(B \cup D) \cap \overline{A}$ is the set of all elements that are in the set above and also in the set $\overline{A}$, so

$$(B \cup D) \cap \overline{A} = \{6, 7, 8, 10, 11, 12, 13, 14, 16, 17, 18, 19, 20\}.$$

The cardinality of this set is 13, i.e., $|(B \cup D) \cap \overline{A}| = 13$. □

Problem 4. Let $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{3\}$, and $D = \{1, 2, 3\}$.

(a) Use set-builder notation to describe D.

(b) Which of these sets are subsets of which other of these sets? In other words, list all true statements of the form $X \subseteq Y$, where X and Y are to be replaced with A, B, C, or D.

Solution.

(a) There are several ways to use set-builder notation to describe D. One way to describe D is to say that it is the set of all natural numbers less than or equal to 3 (remember that we agreed 0 is not a natural number), so we can write

$$D = \{\, x \in \mathbb{N} \mid x \leq 3 \,\}.$$

Alternatively, we can describe D as the set of all integers that are greater than or equal to 1 and less than or equal to 3, so we can write

$$D = \{\, x \in \mathbb{Z} \mid 1 \leq x \leq 3 \,\}.$$

(b) The following statements are all true:

$$A \subseteq D, \qquad B \subseteq D, \qquad C \subseteq B, \qquad C \subseteq D.$$

Since every set is a subset of itself, the following four statements are also true:

$$A \subseteq A, \qquad B \subseteq B, \qquad C \subseteq C, \qquad D \subseteq D.$$

These are all of the true statements of the form $X \subseteq Y$ if X and Y are to be replaced with A, B, C, or D. □

Problem 5. Write a short story that explains or demonstrates the ideas of modular arithmetic (in particular, how addition and multiplication work). Ideally, this should be a story that could be illustrated and made into a children's book. Be creative.

Solution. (Work in progress.)

Problem 6. Prove that the Diophantine equation $n^2 = 3k + 2$ has no integer solutions.

Solution. We will show that no integer n can satisfy the given equation if k is an integer. To do this, we will look at the equation modulo 3. In other words, we will look at the remainders of each side of the equation after division by 3.

First, we observe that the right-hand side, $3k + 2$, must be congruent to 2 modulo 3 (if k is an integer), because 3 divides $3k$ evenly, leaving a remainder of 2. In symbols, we have $3k + 2 \equiv 2 \pmod 3$. Therefore, in order for n to be a solution of the equation, we need $n^2 \equiv 2 \pmod 3$.

Every integer is congruent to either 0, 1, or 2 modulo 3. Let's examine each of these cases individually.

Suppose $n \equiv 0 \pmod 3$. Then $3 \mid n$, so $n = 3m$ for some integer m. This means that

$$n^2 = (3m)^2 = 9m^2 = 3(3m^2) + 0 \equiv 0 \pmod 3.$$

So, if $n \equiv 0 \pmod 3$, then $n^2 \equiv 0 \pmod 3$.

Suppose $n \equiv 1 \pmod 3$. Then $n = 3m + 1$ for some integer m. So

$$n^2 = (3m + 1)^2 = 9m^2 + 6m + 1 = 3(3m^2 + 2) + 1 \equiv 3 \pmod 3.$$

Therefore, if $n \equiv 1 \pmod 3$, then $n^2 \equiv 1 \pmod 3$.

Finally, suppose $n \equiv 2 \pmod 3$. Then $n = 3m + 2$ for some integer m. So

$$n^2 = (3m + 2)^2 = 9m^2 + 12m + 4 = 3(3m^2 + 4m + 1) + 1 \equiv 1 \pmod 3.$$

So, if $n \equiv 2 \pmod 3$, then $n^2 \equiv 1 \pmod 3$.

Since every integer n must fall into one of these three cases, we see that there is no integer n such that $n^2 \equiv 2 \pmod 3$, and therefore there is no integer solution to the equation $n^2 = 3k + 2$. □

Problem 7. Let d be a fixed positive integer, with $d \geq 2$. We saw in class that remainders after division by d can be added, subtracted, and multiplied; in other words, arithmetic modulo d makes sense. Mathematicians use the word *ring* to describe a "place" where we can add, subtract, and multiply. So another way to express the fact that remainders after division by d can be added, subtracted, and multiplied is to say that the integers modulo d form a ring.

What about division? A ring in which division also makes sense (except division by zero) is called a *field*. Does it make sense to divide remainders after division by d? In other words, do the integers modulo d form a field? This is the question we will explore in this problem.

What does division mean, anyway? Division should be the opposite of multiplication, so the division problem $a \div b \equiv c \pmod d$ should mean that $b \times c \equiv a \pmod d$. This is how you should think about division for the purposes of this problem.

(a) Part of Problem 1 is to make a multiplication table for the integers modulo 7. (If you haven't done Problem 1 yet, it is probably worthwhile to do it now.) Let's consider the division problem $a \div b$, where a and b are integers modulo 7 and $b \neq 0$. (Division by zero is always bad.) If $a \div b$ is to make sense, there should be some value for c (an integer modulo 7) such that $b \times c \equiv a \pmod 7$. Using the multiplication table from Problem 1, show that, no matter which values are chosen for a and b (as long as $b \neq 0$), there is exactly one value for c such that $b \times c \equiv a \pmod 7$. Explain why this means that division makes sense modulo 7.

(b) What is $3 \div 5 \pmod 7$?

(c) Now make a multiplication table for the integers modulo 6. Show that there is no value for c such that $3 \times c \equiv 5 \pmod 6$, and explain why this means that the division problem $3 \div 5 \pmod 6$ does not have an answer.

These examples show that the integers modulo d form a field for *some* values of d, but not all. In fact, it turns out that the integers modulo d form a field if and only if the number d is prime.

Solution.

(a) The multiplication table for the integers modulo 7 is given again below.

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Notice that each of the numbers 0 through 6 appears exactly once in every row and every column (except the row and column for 0). In other words, for every nonzero value of b, and every value for a, there is exactly one value for c such that $b \times c \equiv a \pmod 7$. This unique value of c is the answer to the division problem $a \div b \pmod 7$; since the answer always exists and is unique, division (except division by zero) makes sense modulo 7. Hence the integers modulo 7 form a field.

(b) We want to find $3 \div 5 \pmod 7$. In other words, we want to find the value of c such that $5 \times c \equiv 3 \pmod 7$. In the row corresponding to 5 in the multiplication table above, we see that 3 appears in the column for 2, so $5 \times 2 \equiv 3 \pmod 7$. Therefore, $3 \div 5 \equiv 2 \pmod 7$.

(c) The multiplication table for the integers modulo 6 appears below.

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

From this table, we see that the only products of the form $3 \times c$, that is, the only entries in the row corresponding to 3, are 0 and 3. In other words, for any value of c, either $3 \times c \equiv 0 \pmod 6$ or $3 \times c \equiv 3 \pmod 6$. In particular, there is no value of c such that $3 \times c \equiv 5 \pmod 6$, so the division problem $3 \div 5 \pmod 6$ does not have an answer.

Other division problems modulo 6 also cause difficulties. For instance, there are *two* values of c such that $2 \times c \equiv 4 \pmod 6$, namely, $2 \times 2 \equiv 4 \pmod 6$ and $2 \times 5 \equiv 4 \pmod 6$. This means that the division problem $4 \div 2 \pmod 6$ has *two* possible answers (2 and 5), so the answer is not unique.

On the other hand, some division problems modulo 6 do have unique answers. There is only one value of c such that $5 \times c \equiv 5 \pmod 6$, namely, $5 \times 1 \equiv 5 \pmod 6$.

This state of confusion shows that division modulo 6 is not well defined. Some division problems have one answer, some have more than one answer, and some have no answer at all. So the integers modulo 6 do *not* form a field; division does not make sense here. □

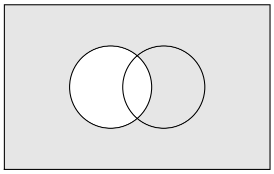
Problem 8. Let A, B, and C be sets.

(a) Write an expression for $A \cap B$ without using the $\cap$ symbol. (You can use unions, complements, set differences, and parentheses. Be sure to use parentheses if you need them to avoid ambiguity.)

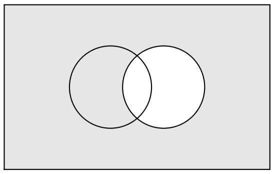
(b) Write an expression for $A \cap B \cap C$ without using the $\cap$ symbol.

Solution.

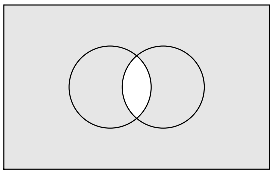
(a) There are many ways to do this. It is helpful to draw Venn diagrams. In the diagrams below, the left circle represents the set A and the right circle represents the set B. The labels below each diagram show which set has been shaded. The set $A \cap B$, which is our goal, is the lens-shaped region that is common to both circles. Proceeding step by step, we have the following:



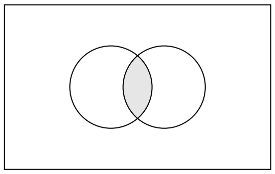
$\overline{A}$



$\overline{B}$



$\overline{A} \cup \overline{B}$

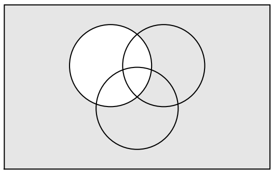


$\overline{\left(\overline{A} \cup \overline{B}\right)}$

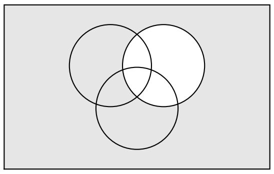
Therefore, $A \cap B = \overline{\left(\overline{A} \cup \overline{B}\right)}$. [This is a variation of one of a pair of fundamental identities in set theory known as *De Morgan's laws*.]

This is not the only possibility. Another way to write $A \cap B$ is $A \setminus \overline{B}$. Can you see why?

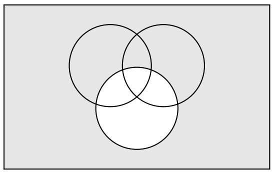
(b) Again, there are many ways in which this can be done. We shall draw Venn diagrams again, this time for three sets. In the diagrams below, the upper left circle represents the set A, the upper right circle represents the set B, and the lower circle represents the set C. Our goal is the set $A \cap B \cap C$, which is the small triangular region common to all three circles.



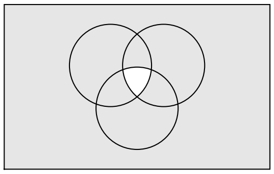
$\overline{A}$



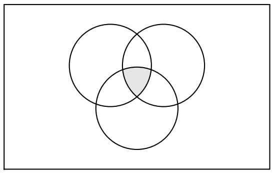
$\overline{B}$



$\overline{C}$



$\overline{A} \cup \overline{B} \cup \overline{C}$



$\overline{\left(\overline{A} \cup \overline{B} \cup \overline{C}\right)}$

So we see that $A \cap B \cap C = \overline{\left(\overline{A} \cup \overline{B} \cup \overline{C}\right)}$.

As in part (a), this is not the only correct answer. We can also write $A \cap B \cap C$ as $\left(A \setminus \overline{B}\right) \setminus \overline{C}$. Can you see why? □