Math 310 Homework 5

Jacob Shiohira

February 22, 2017

Note: This homework took a total of 6 hours. I initially did it alone, but I did review with Jacob Warner.

Problem 1. Non-book problem

Proposition Let $S = \{(a, b)|a, b \in \mathbb{Z} \text{ and } b \neq 0\}$. Let $(a, b) \sim (c, d)$ if and only if $ad = bc$. Prove that $\sim$ is an equivalence relation on S.

Let $S = \{(a, b)|a, b \in \mathbb{Z} \text{ and } b \neq 0\}$. In order to prove that $\sim$ is an equivalence relation, we must show that it retains the reflexive, symmetric, and transitive properties.

1. Reflexive: For all $a, b \in \mathbb{Z}(b \neq 0)$, let (a, b) be an ordered pair. Multiplication of integers is commutative, so $(a, b), (a, b) \iff ab = ba$. This shows S is reflexive.

2. Symmetric: For all $a, b, c, d \in \mathbb{Z}(bd \neq 0)$, let (a, b) and (c, d) be ordered pairs. So, by the commutative property of multiplication, $(a, b) \sim (c, d) \iff ad = bc \iff cb = da \iff (a, b)(c, d) \sim (a, b)$. This shows S is symmetric.

3. Transitive: For all $a, b, c, d, e, f \in \mathbb{Z}(bdf \neq 0)$, let (a, b), (c, d), and (e, f) be ordered pairs. If $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$, then $ad = bc$ and $cf = de$. Multiplying yields $adcf = bcde$. By the associativity of multiplication, $af(cd) = be(cd)$. Suppose $cd \neq 0$. Then, we can divide both sides by cd. Then, $af = be$ and $(a, b) \sim (e, f)$, so S is transitive.

We see that since $\sim$ satisfies all three properties, it is in fact an equivalence relation. $\square$

Problem 2. Section 2.1 #3

Every published book has a ten-digit ISBN-10 number that is usually in the form x_1-$x_2x_3x_4$-$x_5x_6x_7x_8x_9$-x_{10} (where each x_i is a single digit). The first 9 digits identify the book. The last digit x_{10} is a check digit. It is chosen so that

$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + 1x_{10} \equiv 0(\text{mod} 11).$$

If an error is made when scanning or keying an ISBN number into a computer, the left side of the congruence will not be congruent to 0 modulo 11, and the number will be rejected as invalid. Which of the following are apparently valid ISBN numbers? (*Note*: Treat the letter X as if it were the number 10.)

1. 3-540-90518-9

$$\begin{aligned} 10(3)+9(5)+8(4)+7(0)+6(9)+5(0)+4(5)+3(1)+2(8)+1(9) &\equiv 0(\text{mod} 11) \\ 30+45+32+0+54+0+20+3+16+9 &\equiv 0(\text{mod} 11) \\ 209 &\equiv \end{aligned}$$

   209 is divisible by 11, so 3-540-90518-9 is a valid ISBN.

2. 0-031-10559-5

$$\begin{aligned} 10(0)+9(0)+8(3)+7(1)+6(1)+5(0)+4(5)+3(5)+2(9)+1(5) &\equiv 0(\text{mod} 11) \\ 0+0+24+7+6+0+20+15+18+5 &\equiv \\ 95 &\equiv \end{aligned}$$

   95 is not divisible by 11, so 0-031-10559-5 is not a valid ISBN.

3. 0-385-49596-X

$$\begin{aligned} 10(0)+9(3)+8(8)+7(5)+6(4)+5(9)+4(5)+3(9)+2(6)+1(X) &\equiv 0(\text{mod} 11) \\ 0+27+64+35+24+45+20+27+12+10 &\equiv 0(\text{mod} 11) \\ 264 &\equiv \end{aligned}$$

   264 is divisible by 11, so 0-385-49596-X is a valid ISBN.

Problem 3. Section 2.1 #6

Proposition: If $a \equiv b(\text{mod } n)$ and $k|n$, is it true that $a \equiv b(\text{mod } k)$? Justify your answer.

As per a normal implication, we will assume both $a \equiv b(\text{mod } n)$ and $k|n$ are true and try to show that $a \equiv b(\text{mod } k)$. From the definition of congruence, we know that $n|a-b$. Then, the definition of divisibility tells us that $a-b=np$ and $n=kq$ for integers p,q. By substituting for n,

$$a-b=(kq)p.$$

By associativity of multiplication,

$$a-b=k(qp).$$

We now see that $k|a-b$ is also true. So, $a \equiv b(\text{mod } k)$. $\square$

Problem 4. Section 2.1 #13

Proposition: $a \equiv b(\text{mod } n)$ if and only if a and b leave the same remainder when divided by n.

Since the proposition contains a biconditional statement, we will proceed by first showing that the forward implication holds, and then show that the backward implication holds. The forward implication says

If $a \equiv b(\text{mod } n)$, then a and b leave the same remainder when divided by n.

As for any implication, we assume that $a \equiv b(\text{mod } n)$ is true. We then want to show a and b leave the same remainder when divided by n is also true. By definition of congruence, we know that $n|a-b$ and the definition of the divisibility yields $a-b = nk$ for some integer k. Then, by the Fundamental Theorem of Arithmetic, we know if $n|a-b$, then $n|b$ and $n|a$. By the division algorithm, we know that when a number x divides another y, there exist unique integers q, r such that

$$y = xq + r,\ 0 \leq r < x.$$

Then for integers q_1, q_2, r_1, r_2,

$$a = nq_1 + r_1,\ 0 \leq r_1 < n,$$
$$b = nq_2 + r_2,\ 0 \leq r_2 < n.$$

We can then reference $a - b = nk$ that we stated earlier and substitute our new values of a and b,

$$nq_1 + r_1 - nq_2 - r_2 = nk.$$

By rearranging the equation,

$$r_1 - r_2 = nk - nq_1 + nq_2.$$

By factoring of addition,

$$r_1 - r_2 = n(k - q_1 + q_2).$$

Since the integers are closed under addition and multiplication, $k - q_1 + q_2$ is an integer. By the definition of divisibility, we know that n divides $r_1 - r_2$. Well, r_1 and r_2 are both strictly less than n, and $r_2 - r_1$ will be strictly less than n. So, the only way that n divides $r_1 - r_2$ is if $r_1 - r_2 = 0$. Thus, we have that $r_1 = r_2$, and a and b leave the same remainder when divided by n.

The backward implication says

If a and b leave the same remainder when divided by n, then $a \equiv b(\text{mod} n)$.

Again, we assume that a and b leave the same remainder when divided by n is true. We then want to show that $a \equiv b(\text{mod } n)$ is also true. By the division algorithm, we know that division leaves a remainder value,

a divided by n: $a = np + r$ for some integer p,
b divided by n: $b = nq + r$ for some integer q.

However, we know that both a divided by n and b divided by n yield the same remainder. So, we can rearrange both equations for r,

$$a - np = b - nq.$$

By rearranging,

$$a - b = np - nq.$$

By factoring,

$$a - b = n(p - q).$$

Since the integers are closed under addition and multiplication, $p - q$ is an integer. Thus, $n|a - b$ and we have that $a \equiv b(\text{mod } n)$.

Problem 5. Section 2.1 #14

(a) Prove or disprove: If $ab \equiv 0(\text{mod}n)$, then $a \equiv 0(\text{mod}n)$ or $b \equiv 0(\text{mod}n)$.

We will disprove by giving a single counter-example, which is sufficient because we are showing a single instance in which the proposition does not hold. Thus, it cannot hold for for all integers. By the definition of congruence, $ab - 0 = np$ for some integer p. Consider $a = 5, b = 6, n = 10$,

$$\begin{aligned} ab - 0 &= np, \\ (5)(6) - 0 &= (10)p, \\ 30 - 0 &= 10p, \\ 30 &= 10p. \end{aligned}$$

We see that $p = 3$ with a remainder of 0. Let us now consider $a \equiv 0(\text{mod}n)$ and $b \equiv 0(\text{mod}n)$. Again, by the definition of congruence, $a - 0 = np$ and $b - 0 = nq$ for some integers p, q. However,

$$\begin{aligned} a - 0 &= np, \\ 5 - 0 &= (10)p, \\ 5 &= 10p. \end{aligned}$$

and

$$\begin{aligned} b - 0 &= np, \\ 6 - 0 &= (10)p, \\ 6 &= 10p. \end{aligned}$$

We see that there is no integer value p that can satisfy the final equations. Thus, we must reference the division algorithm and consider remainders of $r_1 = 5$ when $a = 5$ and $r_2 = 6$ when $b = 6$. Thus, we have disproved the proposition.

(b) Do part (a) when n is prime.

If $ab \equiv 0(\text{mod } n)$, we know $ab - 0 = nk$ for some integer k by the definition of congruence. We can simplify $ab - 0$ to just ab. By Theorem 1.5, if $ab = nk$, which is equivalent to $n|ab$, then either $n|a$ or $n|b$. We then proceed in two cases,

If $n|a$, then, by the definition of divisibility, we know $a = np$ for some integer p. Then, let us subtract 0 from both sides, $a - 0 = np - 0$. The 0 on the RHS can be considered taken away since it has no effect, and we are left with $a - 0 = np$. By the definition of congruence, we have $a \equiv 0(\text{mod } n)$.

If $n|b$, then, by the definition of divisibility, we know $b = nq$ for some integer q. Then, let us subtract 0 from both sides, $b - 0 = nq - 0$. The 0 on the RHS can be considered taken away since it has no effect, and we are left with $b - 0 = nq$. By the definition of congruence, we have $b \equiv 0(\text{mod } n)$.

We have seen that if $ab \equiv 0(\text{mod } n)$ and n is prime, either $a \equiv 0(\text{mod } n)$ or $b \equiv 0(\text{mod } n)$. This proves our proposition. $\square$

Problem 6. Section 2.1 #21

(a) Show that $10^n \equiv 1(\text{mod}9)$ for every positive n.

Choose an arbitrary integer n. Consider the equality,

$$10^n \equiv 1(\text{mod}9).$$

We know that $10 \equiv 1(\text{mod } 9)$ by the definition of congruence $9|10 - 1$. Then, we can cite Theorem 2.2 because our congruence turns into $10^n \equiv 1^n(\text{mod } 9)$. $\square$

(b) Prove that every positive integer is congruent to the sum of its digital mod 9[for example, $38 \equiv 11(\text{mod}9)$].

We proved in part a that $10^n \equiv 1(\text{mod } 9)$. So, if we could figure out a way to represent integers with terms of 10^n, where n is an integer, we could prove that the sum of its digits is congruent to the sum mod 9. So, in the example of 38, it can be expanded as a number represented by coefficients of powers of 10 by $8 \cdot 10^0 + 3 \cdot 10^1$. Then, $11 = 1 \cdot 10^0 + 1 \cdot 10^1$, and the congruence would be $8 \cdot 10^0 + 3 \cdot 10^1 \equiv 1 \cdot 10^0 + 1 \cdot 10^1(\text{mod } 9)$. By the definition of congruence, $9|(8 - 1) \cdot 10^0 + (3 - 1) \cdot 10^1$, and we know this is true since $10^n \equiv 1(\text{mod } 9)$. So, an arbitrary integer n can be represented by

$$\begin{aligned} n &= a_0 \cdot 10^0 + a_1 \cdot 10^1 + \cdots + a_{n-1} \cdot 10^{n-1} + a_n \cdot 10^n \\ &= \sum_{i=1}^{n} a_i \cdot 10^i \\ &\equiv \text{mod } 9. \end{aligned}$$

Now, each term is represented by 10^i for some integer i, so by part a, any positive integer is congruent to the sum of its digits mod 9. □

Problem 7. Section 2.2 #3

Solve the equation,

$$x^2 = [1] \text{ in } \mathbb{Z}_8.$$

The possible equivalence classes of $\mathbb{Z}_8$ are $[0], [1], [2], [3], [4], [5], [6], [7]$. So, we test each equivalence class to see if if satisfies the equation

$$x^2 = [1].$$

We will just use an exhaustive method and try all 8 possibilities,

- $[0]$: $[0^2] = [0] \neq 1$
- $[1]$: $[1^2] = [1] = 1$
- $[2]$: $[2^2] = [3] \neq 1$
- $[3]$: $[3^2] = [9] = [1] = 1$
- $[4]$: $[4^2] = [16] = [0] \neq 1$
- $[5]$: $[5^2] = [25] = [1] = 1$
- $[6]$: $[6^2] = [36] = [4] \neq 1$
- $[7]$: $[7^2] = [49] = [1] = 1$

We see that $[1], [3], [5], [7]$ all satisfy the equation $x^2 = [1]$ in $\mathbb{Z}_8$. □

Problem 8. Section 2.2 #5

Solve the equation,

$$x^2 \oplus [3] \odot x \oplus [2] = [0] \text{ in } \mathbb{Z}_6.$$

The possible equivalence classes of $\mathbb{Z}_6$ are $[0], [1], [2], [3], [4], [5]$. So, we test each equivalence class to see if if satisfies the equation

$$x^2 \oplus [3] \odot x \oplus [2] = [0].$$

We will just use an exhaustive method and try all 6 possibilities,

- $[0]$: $[0]^2 \oplus [3] \odot [0] \oplus [2] = [2] \neq [0]$

- $[1]$: $[1]^2 \oplus [3] \odot [1] \oplus [2] = [6] = [0]$

- $[2]$: $[2]^2 \oplus [3] \odot [2] \oplus [2] = [12] = [0]$

- $[3]$: $[3]^2 \oplus [3] \odot [3] \oplus [2] = [20] \neq [0]$

- $[4]$: $[4]^2 \oplus [3] \odot [4] \oplus [2] = [30] = [0]$

- $[5]$: $[5]^2 \oplus [3] \odot [5] \oplus [2] = [42] = [0]$

We see that $[1], [2], [4], [5]$ all satisfy the equation $x^2 \oplus [3] \odot x \oplus [2] = [0]$ in $\mathbb{Z}_6$. $\square$