Mathematics 243, section 2 – Mathematical Structures
Solutions for Sample Exam Questions – Exam 2
October 30, 2017

I. Let $[a] \in \mathbf{Z}/18\mathbf{Z}$ and let $m_{[a]} : \mathbf{Z}/18\mathbf{Z} \to \mathbf{Z}/18\mathbf{Z}$ be the mapping defined by $m_{[a]}([x]) = [a] \cdot [x] = [a \cdot x]$.

A) Is $m_{[12]}$ an injective mapping? Why or why not? Is it a surjective mapping? Why or why not?
Solution: The $m_{[12]}$ is *not* an injective mapping because, for instance $[x] = [0]$ and $[x] = [3]$ satisfy

$$m_{[12]}([0]) = [0] = m_{[12]}([3])$$

but $[0] \neq [3]$ in $\mathbf{Z}/18\mathbf{Z}$.

B) Is $m_{[5]}$ an injective mapping? Why or why not?
Solution: Yes, $m_{[5]}$ is an injective mapping. Note that $\gcd(5, 18) = 1$, so $[5]$ has a multiplicative inverse in $\mathbf{Z}/18\mathbf{Z}$. In fact, we can see that $[5]^{-1} = [11]$ since $[5] \cdot [11] = [55] = [1]$ in $\mathbf{Z}/18\mathbf{Z}$. Hence, if $[x]$ and $[x']$ are in $\mathbf{Z}/18\mathbf{Z}$ and $m_{[5]}([x]) = m_{[5]}([x'])$, then

$$\begin{aligned} [5][x] &= [5][x'], \text{ so} \\ [11]([5][x]) &= [11]([5][x']), \text{ and hence} \\ ([11][5])[x] &= ([11][5])[x'], \text{ by associativity, so} \\ [1][x] &= [1][x'], \text{ which shows} \\ [x] &= [x']. \end{aligned}$$

This shows $m_{[5]}$ is an injective mapping.

C) Prove that $m_{[a]}$ is injective if and only if $[a]$ has a multiplicative inverse in $\mathbf{Z}/18\mathbf{Z}$.
Solution: The proof that if a multiplicative inverse $[a]^{-1}$ exists in $\mathbf{Z}/18\mathbf{Z}$, then $m_{[a]}$ is injective is just the same as the proof given for the case $a = 5$ in part B. For the converse, suppose that $m_{[a]}$ is injective. Since $m_{[a]}$ is injective, its range will contain 18 distinct elements of $\mathbf{Z}/18\mathbf{Z}$. But there are only 18 different elements in this structure: $\mathbf{Z}/18\mathbf{Z} = \{[0], [1], \ldots, [17]\}$. Hence there must be an element $[x]$ such that $[a][x] = [1]$. This shows that $[a]$ has a multiplicative inverse.

D) Prove the $m_{[a]}$ is injective if and only if $m_{[a]}$ is surjective.
Solution: The proof that $m_{[a]}$ injective implies it is also surjective is the same as part of the proof for part C: If $m_{[a]}$ is injective, then its range contains exactly 18 distinct elements in $\mathbf{Z}/18\mathbf{Z}$. But there *are only* 18 distinct elements altogether, so the range must consist of all of $\mathbf{Z}/18\mathbf{Z}$, and that shows the mapping is surjective. Conversely, if the mapping $m_{[a]}$ is surjective, then there must be 18 different elements in the range. But since the domain consists of only 18 elements altogether, then those elements of the domain must map to 18 distinct images. (Alternatively, in the contrapositive form, if $m_{[a]}$ is not injective, then two distinct elements of the domain must map to the same element in $\mathbf{Z}/18\mathbf{Z}$. But that means there are no more than 17 distinct elements in the range, so the range cannot be all of $\mathbf{Z}/18\mathbf{Z}$ and the mapping is not surjective.)

II.

A) Given integers a, and $b > 0$, prove that there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$. (You may apply the Well-Ordering Principle without justifying that.)
Solution: See class notes and/or Theorem 4.8 in the text.

B) Find the quotient q and the remainder r as in part A for $a = 4578$ and $b = 235$.
Solution: $q = 19$ and $r = 113$.

III.

A) Prove that if $S = \langle a, b\rangle = \{x \in \mathbf{Z} : x = ma + nb, m, n \in \mathbf{Z}\}$, then the smallest positive integer d in S satisfies the properties:

1. d divides a and d divides b.
Solution: We claim that in fact d divides *every element* of $\langle a, b\rangle$. This will imply the required statement since $a = 1 \cdot a + 0 \cdot b$ and $b = 0 \cdot a + 1 \cdot b$ are both elements of $\langle a, b\rangle$. So let $x = ma + nb$, $m, n \in \mathbf{Z}$, be any element of $\langle a, b\rangle$ and divide x by d using the division algorithm: $x = qd + r$ where $0 \leq r < d$. Now we have $d = m_0 a + n_0 b$ for some $m_0, n_0 \in \mathbf{Z}$. Hence
$$r = x - qd = ma + nb - q(m_0 a + n_0 b) = (m - qm_0)a + (n - qn_0)b$$
Now $m - qm_0$ and $n - qn_0$ are clearly in $\mathbf{Z}$ so by definition, $r \in \langle a, b\rangle$. But d was the smallest positive element in $\langle a, b\rangle$, so since $0 \leq r < d$, the only possibility is that $r = 0$. Hence d divides x.
2. If c divides a and c divides b, then c divides d.
Solution: If c divides a and c divides b, then we have $a = cs$ and $b = ct$ for some integers s, t. But then because $d = m_0 a + n_0 b$, we can substitute to get
$$d = m_0 cs + n_0 ct = c(m_0 s + n_0 t).$$
Since $m_0 s + n_0 t$ is clearly in $\mathbf{Z}$, this shows c divides d.

B) Find the integer $d = \gcd(488, 376)$ and express d in the form $d = m \cdot 488 + n \cdot 76$ for integers m, n.
Solution: By the Euclidean algorithm,
$$\begin{aligned} 488 &= 1 \cdot 376 + 112 \\ 376 &= 3 \cdot 112 + 40 \\ 112 &= 2 \cdot 40 + 32 \\ 40 &= 1 \cdot 32 + 8 \end{aligned}$$
and 8 divides 32, so the final nonzero remainder is the gcd: $\gcd(488, 376) = 8$. To find the required m, n, use the Extended Euclidean algorithm:
$$\begin{array}{cccc} & & 1 & 0 \\ & & 0 & 1 \\ 1 & 1 & -1 & \\ 3 & -3 & 4 & \\ 2 & 7 & -9 & \\ 1 & -10 & 13 & \end{array}$$

This gives the equation $(-10)\cdot(488)+(13)\cdot(376)=8$.

C) Prove that if there is a solution of the congruence $ax \equiv b \pmod{n}$ (where $n>1$), then $\gcd(a,n)|b$.
Solution: If there is a solution x of the congruence $ax \equiv b \bmod n$, then $ax-b=ny$ for some integer y. But this implies $ax+n(-y)=b$, so $b \in \langle a,n\rangle$ in $\mathbf{Z}$. Since the gcd is the smallest positive element of $\langle a,n\rangle$, the argument given in the solution for III A above shows that $\gcd(a,n)|b$.

IV.

A) Show that for all $n \geq 1$, $8|(9^n-1)$. (Hint: Show first that $9^{k+1}-1=9^k\cdot 8+(9^k-1)$.)
Solution: We argue by *mathematical induction* on n. The base case is $n=1$, and $8|(9-1)$ is clear because $9-1=8$. For the induction step, suppose $8|(9^k-1)$ and consider $9^{k+1}-1$. Note that

$$9^{k+1}-1=9^k\cdot 9-1=9^k\cdot(8+1)-1=9^k\cdot 8+9^k-1.$$

Now if $8|(9^k-1)$ then we have $9^k-1=8\cdot\ell$ for some integer ℓ. Hence

$$9^{k+1}-1=9^k\cdot 8+8\cdot\ell=8\cdot(9^k+\ell).$$

Since $9^k+\ell \in \mathbf{Z}$, this shows $8|(9^{k+1}-1)$, and the proof is complete.

B) Restate the result of part A as a congruence.
Solution: The result from part A is the same as saying

$$9^n \equiv 1 \bmod 8$$

for all $n \geq 1$. (It's also true for $n=0$, of course!)

C) (Extra Credit-type question) Suppose we used base 9 rather than base 10 to represent integers. How could you test numbers for divisibility by 8 using the base 9 digits? How could you test numbers for divisibility by 10 using the base 9 digits?
Solution: Write integers in base 9:

$$N=a_0+a_1\cdot 9+a_2\cdot 9^2+\cdots+a_k9^k,$$

where the base-9 digits $a_i \in \{0,1,\ldots,8\}$ for all $i \geq 0$. Then the congruence from part B shows that $N \equiv S \bmod 8$ where

$$S=a_0+a_1+\cdots+a_k$$

is the sum of the base-9 digits. Hence

$$N \equiv 0 \bmod 8 \Leftrightarrow S \equiv 0 \bmod 8.$$

In words, a number is divisible by 8 if and only if the sum of its base-9 digits is divisible by 8.

Similarly $9 \equiv -1 \bmod 10$, so N written in base 10 is divisible by 10 if the alternating sum of its base-9 digits is zero:

$$N \equiv 0 \bmod 10 \Leftrightarrow a_0 - a_1 + a_2 + \cdots + (-1)^k a_k \equiv 0 \bmod 10.$$

V. Show that $[x]$ has a multiplicative inverse in $\mathbf{Z}/n\mathbf{Z}$ (that is, a $[y]$ such that $[x][y] = [1] = [y][x]$) if and only if $\gcd(x, n) = 1$.

Solution: If $\gcd(x, n) = 1$, then there are integers y, t such that $xy + nt = 1$, this shows $xy - 1 = (-t)n$. Hence, by definition,

$$xy \equiv 1 \bmod n,$$

which implies that $[x][y] = [1]$ in $\mathbf{Z}/n\mathbf{Z}$. Conversely, if $[x][y] = [1]$ in $\mathbf{Z}/n\mathbf{Z}$, then there is an equation $xy - 1 = kn$ for some integer k. Rearranging this equation gives $xy + (-k)n = 1$. This implies that $1 \in \langle x, n\rangle$. But $\gcd(x, n)$ is the smallest positive element of $\langle x, n\rangle$. That implies $\gcd(x, n) = 1$.

VI.

A) Find all integer solutions of the congruence $12x \equiv 7 \bmod 331$.
Solution: Since $\gcd(12, 331) = 1$, we can solve this by finding $[12]^{-1}$ in $\mathbf{Z}/331\mathbf{Z}$. This is the same sort of computation as in III B above. The answer is $[12]^{-1} = [138]$. So $[x] = [138][7] = [304]$. Since the question says find all $x \in \mathbf{Z}$ that satisfy the congruence, we have the set of solutions $304 + 331\mathbf{Z} = \{x : x = 304 + 331j, j \in \mathbf{Z}\}$.

B) Find all solutions $[x]$ of the equation $[17][x] + [4] = [2]$ in $\mathbf{Z}/29\mathbf{Z}$.
This is equivalent to the congruence $17x \equiv -2 \equiv 27 \bmod 29$. Since $\gcd(17, 29) = 1$, we have $[17]^{-1}$ exists in $\mathbf{Z}/29\mathbf{Z}$. Proceeding as in question III B above, we have $[17]^{-1} = [12]$. We find $[x] = [12][27] = [5]$. (If the question said find all $x \in \mathbf{Z}$ that satisfy the congruence, we would have the set of solutions $5 + 29\mathbf{Z} = \{x : x = 5 + 29j, j \in \mathbf{Z}\}$.)

C) Which $[x] \in \mathbf{Z}/18\mathbf{Z}$ have multiplicative inverses?
Solution: All the $[a]$ with $\gcd(a, 18) = 1$. This gives

$$(\mathbf{Z}/18\mathbf{Z})^\times = \{[1], [5], [7], [11], [13], [17]\}.$$