College of the Holy Cross, Fall Semester 2017
MATH 243 – Mathematical Structures, section 2
Solutions for Exam 2 – November 3

I. Let $f : \mathbb{Z}/29\mathbb{Z} \to \mathbb{Z}/29\mathbb{Z}$ be the mapping defined by $f([x]) = [x] + [12]$.

(A) (10) Show that f is injective.

Solution: If $f([x_1]) = f([x_2])$, then we have $[x_1] + [12] = [x_2] + [12]$. The element [12] has an *additive* inverse in $\mathbb{Z}/29\mathbb{Z}$, namely, [17], since $[12] + [17] = [0]$. If we add that additive inverse to both sides of the equation $[x_1] + [12] = [x_2] + [12]$, and use the fact that addition is associative in $\mathbb{Z}/29\mathbb{Z}$, then we get $[x_1] + [0] = [x_2] + [0]$, so $[x_1] = [x_2]$. This shows f is injective.

(B) (10) Is f surjective? Why or why not?

Solution: Yes, f is surjective. *Proof 1:* Use the result from part (A). Since f maps distinct elements of $\mathbb{Z}/29\mathbb{Z}$ to distinct elements, there are 29 different elements of the range of the mapping. But there are only 29 elements of $\mathbb{Z}/29\mathbb{Z}$ in all, so the range must contain all the elements of $\mathbb{Z}/29\mathbb{Z}$, and f is surjective by definition.

Proof 2: Another, alternative, way to show this is to note that given any $[y] \in \mathbb{Z}/29\mathbb{Z}$, we can solve the equation $f([x]) = [x] + [12] = [y]$ for $[x]$ by taking $[x] = [y] + [17]$, since [17] is the additive inverse of [12]. This also shows that the map f is surjective.

II.

(A) (20) Give a precise statement of the Division Algorithm in $\mathbb{Z}$, and prove *both* the Existence and Uniqueness parts.

Solution: Let N and $n > 0$ be integers. There exist unique integers q, r such that $N = qn + r$ with $0 \le r < n$.

Existence: Consider the set $S = \{N - kn \mid k \in \mathbb{Z}\}$. Then $S \cap (\mathbb{Z}^+ \cup \{0\}) \neq \emptyset$. (The reason here is that if $N > 0$, then we can just take $k = 0$ to get a positive element of S. On the other hand if $N \le 0$, we just need to take k to be a negative integer with absolute value large enough that $-N < -kn$.) Now by the Well-Ordering property, $S \cap (\mathbb{Z}^+ \cup \{0\})$ contains a smallest element. Call this smallest element r, and write $r = N - qn$ (that is, $k = q$ for some particular integer q from the definition of the set S). This gives $N = qn + r$ as required and we only need to show $0 \le r < n$. Now, $r \ge 0$ is automatic by the way r was produced (it's the smallest non-negative element of S). Suppose that $r \ge n$. Then in the set S we also have $N - (q+1)n = N - qn - n = r - n \ge 0$ but $r - n < r$. This contradicts the choice of r as the smallest non-negative element in S. With this proof by contradiction, we have shown $r \le n$. Hence both of the required conditions hold and the existence part of the proof is complete.

Uniqueness: If $N = q_1 n + r_1$ and also $N = q_2 n + r_2$, where r_1 and r_2 both satisfy the statement of the theorem but $r_1 \neq r_2$, then we can assume $r_1 > r_2$. Setting the two expressions for N equal, we have $q_1 n + r_1 = q_2 n + r_2$, so $(q_2 - q_1)n = r_1 - r_2$. Now $r_1 - r_2 > 0$ but also $r_1 - r_2 \leq r_1 < n$. Hence $r_1 - r_2$ is a multiple of n that lies strictly between 0 and n. But that is a clear contradiction. Hence $r_1 = r_2$, and hence $q_1 = q_2$ as well.

(B) (15) Use the Euclidean algorithm to find the integer $d = \gcd(585, 108)$ and express d in the form $d = m \cdot 585 + n \cdot 108$ for some integers m, n.

Solution: We have

$$\begin{aligned} 585 &= 5 \cdot 108 + 45 \\ 108 &= 2 \cdot 45 + 18 \\ 45 &= 2 \cdot 18 + 9, \end{aligned}$$

but $9|18$, so the final nonzero remainder is 9. This gives $9 = \gcd(585, 108)$. Now applying the Extended Euclidean Algorithm:

	1	0
	0	1
5	1	-5
2	-2	11
2	5	-27

So $5 \cdot 585 + (-27) \cdot 108 = 9$.

III. (10) Let a, b, c be integers. Show that if $\gcd(a, b) = 1$ and $a|(bc)$, then $a|c$.

Solution: Since $\gcd(a, b) = 1$, there is an equation $ma + nb = 1$ where $m, n \in \mathbb{Z}$. Multiply both sides by c:

$$mac + nbc = c.$$

Now we know that $a|(bc)$, so $bc = aq$ for some $q \in \mathbb{Z}$. Hence substituing for the bc in the second term of the last displayed equation, we have

$$mac + naq = a(mc + nq) = c$$

This shows that $a|c$ because $mc + nq$ is also an integer.

IV. (15) Find a solution x of the congruence $31x \equiv 6 \bmod 64$ with $0 \leq x < 64$.

Solution: We have $\gcd(31, 64) = 1$, so $[31]^{-1}$ exists in $\mathbb{Z}/64\mathbb{Z}$ To find it, we proceed as in question II (B) above. By the Euclidean algorithm:

$$\begin{aligned} 64 &= 2 \cdot 31 + 2 \\ 31 &= 15 \cdot 2 + 1 \end{aligned}$$

and that is the final nonzero remainder. Hence the Extended Euclidean Algorithm table here is

	1	0
	0	1
2	1	-2
15	-15	31

Hence $(-15)\cdot 64+(31)\cdot(31)=1$. This shows $[31]^{-1}=[31]$ in $\mathbb{Z}/64\mathbb{Z}$. We have $[x]=[31][6]=[186]=[58]$ (since $186=2\cdot 64+58$). Hence the required solution is $x=58$.

V. (15) Construct the *multiplication* table for $(\mathbb{Z}/12\mathbb{Z})^{\times}$.

Solution: By definition, $(\mathbb{Z}/12\mathbb{Z})^{\times}$ is the subset of $\mathbb{Z}/12\mathbb{Z}$ consisting of the $[a]$ for which multiplicative inverses $[a]^{-1}$ exist in $\mathbb{Z}/12\mathbb{Z}$. This is equivalent to the condition $\gcd(a,12)=1$, so

$$(\mathbb{Z}/12\mathbb{Z})^{\times}=\{[1],[5],[7],[11]\}.$$

The multiplication table is computed by taking products modulo 12 and the result is

$\cdot$	[1]	[5]	[7]	[11]
[1]	[1]	[5]	[7]	[11]
[5]	[5]	[1]	[11]	[7]
[7]	[7]	[11]	[1]	[5]
[11]	[11]	[7]	[5]	[1]

For example $[5]\cdot[7]=[35]=[11]$, since $35=2\cdot 12+11$.