Mathematics 243, section 1 – Algebraic Structures
Solutions for Exam 2, November 1, 2006

I. Think of $\mathbf{R}^2$ (the set of ordered pairs of real numbers) as the ordinary Cartesian coordinate plane. Let R be the relation on $\mathbf{R}^2$ defined by

$$(x_1, y_1)R(x_2, y_2) \Leftrightarrow 3x_1 + y_1 = 3x_2 + y_2$$

A) (15) Show that R is an equivalence relation on $\mathbf{R}^2$.

Solution: R is *reflexive* because for all points $(x, y) \in \mathbf{R}^2$, $3x + y = 3x + y$, hence $(x, y)R(x, y)$.

R is *symmetric* because if $(x_1, y_1)R(x_2, y_2)$, then $3x_1 + y_1 = 3x_2 + y_2$, so $3x_2 + y_2 = 3x_1 + y_1$, and $(x_1, y_1)R(x_2, y_2)$.

R is *transitive* because if $(x_1, y_1)R(x_2, y_2)$ and $(x_2, y_2)R(x_3, y_3)$, then $3x_1 + y_1 = 3x_2 + y_2$ and $3x_2 + y_2 = 3x_3 + y_3$, so $3x_1 + y_1 = 3x_3 + y_3$.

B) (5) Draw a picture of the equivalence class $[(2, 3)]$ for this relation.

Solution: The equivalence class of the point $(2, 3)$ is the set of all points (x, y) such that $(x, y)R(2, 3)$, so $3x + y = 9$. This is the *line* $y = -3x + 9$ with slope -3 and y-axis intercept at $(0, 9)$.

II. (20) Prove by mathematical induction: For all $n \geq 1$,

$$1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1). \tag{1}$$

Solution: The base case is $n = 1$. For $n = 1$, the left side of the formula (1) is $1^3 = 1$, and the right side is $1^2(2 \cdot 1 - 1)$ so the formula is true for $n = 1$.

For the induction step assume that (1) is true for $n = k$. Then with $n = k + 1$, by the induction hypothesis and the binomial theorem we have

$$\begin{aligned} 1^3 + 3^3 + 5^3 + \cdots + (2k-1)^3 + (2(k+1)-1)^3 &= k^2(2k^2 - 1) + (2(k+1)-1)^3 \\ &= 2k^4 - k^2 + (2k+1)^3 \\ &= 2k^4 - k^2 + 8k^3 + 12k^2 + 6k + 1 \\ &= 2k^4 + 8k^3 + 11k^2 + 6k + 1 \end{aligned}$$

On the other hand, we are trying to show that this is the same as the right side of (1) with $n = k + 1$, namely,

$$\begin{aligned} (k+1)^2(2(k+1)^2 - 1) &= (k^2 + 2k + 1)(2k^2 + 4k + 1) \\ &= 2k^4 + 8k^3 + 11k^2 + 6k + 1 \end{aligned}$$

Since the two sides of (1) agree for $n = k + 1$, the formula is true for all $n \geq 1$ by the Principle of Mathematical Induction.

III.

A) (15) Give the precise statement of the division algorithm in $\mathbf{Z}$, and prove the existence part.

Solution: The statement is that for all integers a and $b > 0$, there exist unique integers q, r such that

$$a = qb + r \qquad \text{and} \qquad 0 \leq r < b. \tag{2}$$

We must show that q, r as in (2) exist. So consider the set of integers

$$S = \{a - qb : q \in \mathbf{Z}\}$$

If $0 \in S$, then $a = qb + 0$ for some q and both parts of (2) are satisfied. So this case is done, and for the rest of the proof we will assume $0 \neq S$.
If a is positive then S contains positive elements such as $a - 0q = a$. If a is negative, we will still have positive elements in S by taking q negative with sufficiently large absolute value. Hence $S \cap \mathbf{N} \neq \emptyset$. The Well-Ordering Principle implies that $S \cap \mathbf{N}$ has a smallest element. Call this smallest positive element r. Then we have $r = a - qb$ for some $q \in \mathbf{Z}$ and the first statement in (2) is true since $a = qb + r$. The remainder of the proof (cue laugh-track!) is to show that $0 < r < b$. (Note that we have ruled out the case $r = 0$ above.) If $r \geq b$, then we claim that a contradiction results. This is because

$$\begin{aligned} r \geq b &\Rightarrow a - qb = r \geq b \\ &\Rightarrow a - (q+1)b = r - b \geq 0 \end{aligned}$$

The integer $a - (q + 1)b$ is also in the set S by definition. Hence either $0 \in S$ which is ruled out above, or else $r - b > 0$ is in S. But $r - b < r$ since $b > 0$. This is a contradiction to the way we found r (it was supposed to be the smallest positive element in S). Hence if $r \neq 0$, then $0 < r < b$ (which is another way of saying $0 \leq r < b$).

B) (15) Use the Euclidean algorithm to find the integer $d = \gcd(576, 99)$ and express d in the form $d = m \cdot 576 + n \cdot 99$ for some integers m, n.

Solution: We first carry out the divisions:

$$\begin{aligned} 576 &= 5 \cdot 99 + 81 \\ 99 &= 1 \cdot 81 + 18 \\ 81 &= 4 \cdot 18 + 9 \\ 18 &= 2 \cdot 9 + 0 \end{aligned}$$

The last non-zero remainder is $9 = \gcd(576, 99)$. (Note that $5 + 7 + 6 = 18 = 9 + 9$ so we could tell both numbers are divisible by 9 by the "sum of digits" test.) Then

k	q_k	m_k	n_k
-1		1	0
0		0	1
1	5	1	-5
2	1	-1	6
3	4	5	-29

which shows that

$$5 \cdot 576 + (-29) \cdot 99 = 9 = \gcd(576, 99).$$

IV. (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 exist integers m, n such that $1 = ma + nb$. Multiply both sides of this equation by c to obtain

$$c = mac + nbc. \tag{3}$$

Since $a|(bc)$, there is some integer q such that $bc = qa$. Hence from (3),

$$c = mac + nbc = mac + nqa = a(mc + nq),$$

which shows $a|c$.

V.

A) (10) Find a solution x of the congruence $31x \equiv 2 \bmod 64$ with $0 \leq x < 63$.

Solution: Since $\gcd(31, 64) = 1$, there will be a unique solution and we want a multiplicative inverse of 31 mod 64 to find it.

$$64 = 2 \cdot 31 + 2$$
$$31 = 15 \cdot 2 + 1$$

Hence

k	q_k	m_k	n_k
-1		1	0
0		0	1
1	2	1	-2
2	15	-15	31

So $[31] = [31]^{-1}$ in $\mathbf{Z}_{64}$, since $(-15) \cdot 64 + 31 \cdot 31 = 1$. We obtain $x \equiv 2 \cdot 31 \bmod 64$ so $x = 62$ is one solution. (The others are the integers $x = 62 + 64\ell$ for all $\ell \in \mathbf{Z}$.)

B) (10) For which $[b] \in \mathbf{Z}_{16}$ do solutions $[x] \in \mathbf{Z}_{16}$ of the equation $[12][x] = [b]$ exist? Explain how you can tell.

Solution: By problem 35 from section 2.5, in order for $ax \equiv b \bmod n$ to have a solution, b must be divisible by $\gcd(a, n)$. Here $\gcd(12, 16) = 4$, so there are solutions when $b = 0, 4, 8, 12$. (For instance, with $b = 0$ we can take $x = 0$; with $b = 4$ we can take $x = 3$; with $b = 8$ we can take $x = 2$; with $b = 12$ we can take $x = 1$. There are other solutions too in each case, which can be found by the process in problem 36 from section 2.5.)