PMAT 315
SOLUTIONS TO ASSIGNMENT 1
WINTER 2010

1. §1.1, #15. *Prove the well-ordering axiom by strong induction.* 7 marks

Solution. Let X be a nonempty set of non-negative integers, and assume X has no smallest member. We show this leads to a contradiction. Let p_n be the statement "n is not a member of X". Then p_0 is true since, if 0 were in X, it would be the smallest member of X. If all of $p_0, p_1, \dots, p_k$ are true, then none of the numbers $0, 1, \dots, k$ lie in X. But then, $k+1$ is not in X (it would be the smallest member) so p_{k+1} is true. Hence p_k is true for all $k \geq 1$, that is, $k \notin X$ for all k. This means X is empty, the desired contradiction.

2. §1.2, #14. *Show that* $gcd(m+n, m) = gcd(m, n)$. 7 marks

Solution. Write $d = gcd(m, n)$ and $d' = gcd(m+n, m)$. Then $d \mid m$ and $d \mid n$, so $d \mid (m+n)$ and $d \mid m$. Hence $d \mid d'$ by the definition of d'. Similarly, $d' \mid (m+n)$ and $d' \mid m$, so $d' \mid [(m+n) - m] = n$ and $d' \mid m$. Hence $d' \mid d$ by the definition of d. So both $d \mid d'$ and $d' \mid d$, whence $d' = \pm d$. But both d and d' are positive (by definition), so $d' = d$.

3. §1.2, #17. *If* $gcd(m, n) = 1$ *and* $gcd(k, n) = 1$, *show that* $gcd(mk, n) = 1$. 6 marks

Solution 1. By hypothesis (and Theorem 3) write $1 = xm + yn$ and $1 = zk + wn$ where x, y, z, w are in $\mathbb{Z}$. Multiplying these gives $1 = xz(mk) + (xmw + ykz + ywn)n$, so $gcd(mk, n) = 1$ by Theorem 4.

Solution 2. If $gcd(mk, n) \neq 1$ then it has a prime divisor, say $p \mid gcd(mk, n)$. Hence $p \mid mk$, so either $p \mid m$ or $p \mid k$ (by Theorem 5 §1.2). Since $p \mid n$, this contradicts the assumption that $gcd(m, n) = 1 = gcd(k, n)$. So $gcd(mk, n) = 1$ after all.

4. §1.3, #22(c). *In* $\mathbb{Z}_{20}$ *find the inverse of* $\overline{11}$ *and use it to solve* $\overline{11}x = \overline{16}$. 6 marks

Solution. Clearly $gcd(11, 20) = 1$. The euclidean algorithm gives $20 = 1 \cdot 11 + 9$, $11 = 1 \cdot 9 + 2$, $9 = 4 \cdot 2 + 1$. Eliminating remainders we get

$$1 = 9 - 4(11 - 1 \cdot 9) = 5 \cdot 9 - 4 \cdot 11 = 5(20 - 11) - 4 \cdot 11 = 5 \cdot 20 - 9 \cdot 11.$$

Hence the inverse of $\overline{11}$ in $\mathbb{Z}_{20}$ is $-\bar{9} = \overline{11}$. So multiplying the given equation by $\overline{11}$ gives $\overline{11} \cdot \overline{11}x = \overline{11} \cdot \overline{16}$, that is $x = \bar{1}x = \overline{176} = \overline{16}$ in $\mathbb{Z}_{20}$.

5. §1.3, #29(b). *Show that* $\bar{a}$ *is invertible in* $\mathbb{Z}_n$ *if and only if* $\bar{a}\bar{b} = \bar{0}$ *implies* $\bar{b} = \bar{0}$. 7 marks

Solution. If $\bar{a}$ is invertible in $\mathbb{Z}_n$, say $\bar{c}\bar{a} = \bar{1}$, and if $\bar{a}\bar{b} = \bar{0}$, then multiplication by $\bar{c}$ gives $\bar{c}\bar{a}\bar{b} = \bar{c}\bar{0}$, that is $\bar{1}\bar{b} = \bar{0}$, that is $\bar{b} = \bar{0}$.

Conversely, suppose that $\bar{a}\bar{b} = \bar{0}$ implies that $\bar{b} = \bar{0}$; we show that $gcd(a, n) = 1$ and apply Theorem 5. If $d = gcd(a, n)$, write $a = qd$ and $n = sd$ where $q, s \in \mathbb{Z}$. Then $as = (qd)s = qn \equiv 0\,(mod\ n)$, so $\bar{a}\bar{s} = \bar{0}$ in $\mathbb{Z}_n$. Hence $\bar{s} = \bar{0}$ by hypothesis, so $n \mid s$. Since $s \mid n$ also holds, this means that $s = \pm n$. It follows that $n = \pm nd$, so $d = \pm 1$. As $d \geq 1$ this means $d = 1$, as required.

6. §1.4, #26. *Let* γ *be any cycle of length* r. *If* $\sigma \in S_n$, *show that* $\sigma\gamma\sigma^{-1}$ *is also a cycle of length* r.

More precisely, if $\gamma = (k_1\ k_2\ \cdots\ k_r)$ *show that* $\sigma\gamma\sigma^{-1} = (\sigma k_1\ \sigma k_2\ \cdots\ \sigma k_r)$. 7 marks

Solution. Since σ is invertible, it suffices to show $\sigma(k_1 k_2 \dots k_r) = (\sigma k_1\ \sigma k_2\ \dots \sigma k_r)\sigma$. If $k \in X_n = \{1, 2, \dots, n\}$ we must show that both $\sigma(k_1 k_2 \dots k_r)$ and $(\sigma k_1\ \sigma k_2\ \dots \sigma k_r)\sigma$ have the same effect on k.

Case 1. If $k = k_i$, we have (writing $k_{r+1} = k_1$),

$$[\sigma(k_1 k_2 \dots k_r)]k = \sigma(k_1 k_2 \dots k_r)k_i = \sigma(k_{i+1}),$$
$$[(\sigma k_1\ \sigma k_2\ \dots \sigma k_r)\sigma](k) = (\sigma k_1\ \sigma k_2\ \dots \sigma k_r)\sigma k_i = \sigma k_{i+1}.$$

Hence each side carries k to σk_{i+1}.

Case 2. If $k \notin \{k_1, \dots, k_r\}$, one shows similarly that each side carries k to σk.

Total: 40 marks