PMAT 315
SOLUTIONS TO ASSIGNMENT 1
WINTER 2005

1. P.34, #11. Guess a divisor of $a_n = 2^{3n} - 1$ for $n \geq 0$, and prove your conjecture.

   $a_0 = 0$, $a_1 = 7$, $a_2 = 63$, $a_3 = 511 = 7 \cdot 73$. So we conjecture that $2^{3n} - 1$ is a multiple of 7 for each $n \geq 0$. We have it for $n = 0$. If $2^{3k} - 1 = 7q$, then

   $$2^{3(k+1)} - 1 = 2^{3k} \cdot 8 - 1 = (1 + 7q) \cdot 8 - 1 = 7(8q + 1)$$

   as required.

2. P.46, #14. Show that $gcd(m + n, m) = gcd(m, n)$.

   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 deønition 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 deønition of d. So both $d \mid d'$ and $d' \mid d$, whence $d' = \pm d$. But both d and d' are positive (by deønition), so $d' = d$.

3. P.47, #17. If $gcd(m, n) = 1$ and $gcd(k, n) = 1$, show that $gcd(mk, n) = 1$.

   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. P.59, #22(c). In $\mathbb{Z}_{20}$ ønd the inverse of $\overline{11}$ and use it to solve $\overline{11}x = \overline{16}$.

   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 $\bar{1}x = \overline{176} = \overline{16}$ in $\mathbb{Z}_{20}$.

5. P59, #28(b). Show that $\bar{a}$ is invertible in $\mathbb{Z}_n$ if and only if $\bar{a}\bar{b} = \bar{0}$ implies $\bar{b} = \bar{0}$.

   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 $s \mid n$ 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. P 74, #15(b). List one permutation in S_6 of each cycle structure.

   (123456), (12345), (1234), (1234)(56), (123), (123)(456), (123)(45), (12), (12)(34)(56), (12)(34), $(1) = \varepsilon$.

7. P75, #25. Show that every even permutation is a product of 3-cycles.

   Every even permutation is a product of pairs of transpositions, and each of these is a product of 3-cycles: $(ab)(ac) = (acb)$, $(ab)(cd) = (acb)(acd)$.