Mathematics 243, section 3 – Algebraic Structures
Solutions for Problem Set 5
due: October 19, 2012

'A' Section

1. Apply the division algorithm to find q, r satisfying $a = qb + r$ and $0 \leq r < b$:

   a. $a = 326$, $b = 17$

   Solution: $326 = 19 \cdot 17 + 3$, so $q = 19$ and $r = 3$.

   b. $a = 1245$, $b = 249$

   Solution: $1245 = 5 \cdot 249$, so $q = 5$ and $r = 0$. (Note this shows $249|1245$).

   c. $a = -3432$, $b = 29$.

   Solution: $-3432 = -119 \cdot 29 + 19$, so $q = -119$ and $r = 19$.

2. a. Find all the positive common divisors of $a = 240$ and $b = 450$. (Hint: Factoring a, b as much as possible may be helpful here.)

   Solution: We have $240 = 2^4 \cdot 3 \cdot 5$ and $450 = 2 \cdot 3^2 \cdot 5^2$. So the common divisors of 240 and 450 are $1, 2, 3, 5, 6, 10, 15, 30$.

   b. What is the smallest positive element of the set

$$S = \{240m + 450n \mid m, n \in \mathbb{Z}\}?$$

   Solution: By Theorem 2.12, this number is $\gcd(240, 450) = 30$.

   c. Apply the Euclidean algorithm to find $\gcd(240, 450)$. What are the integers m, n such that $240m + 450n = \gcd(240, 450)$?

   Solution: Computing by the Euclidean process:

$$\begin{aligned} 450 &= 1 \cdot 240 + 210 \\ 240 &= 1 \cdot 210 + 30 \\ 210 &= 7 \cdot 30 + 0. \end{aligned}$$

   The last nonzero remainder is 30, so $\gcd(240, 450) = 30$. By the "back-substitution" method, we have

$$\begin{aligned} 30 &= 240 - 1 \cdot 210 \\ &= 240 - 1 \cdot (450 - 1 \cdot 240) \\ &= 2 \cdot 240 + (-1) \cdot 450. \end{aligned}$$

   So $m = 2$ and $n = -1$.

3. Repeat all the parts of question 2 for $a = 2312$ and $b = 584$.

   a. Find all the positive common divisors of $a = 2312$ and $b = 584$. (Hint: Factoring a, b as much as possible may be helpful here.)

      Solution: We have $2312 = 2^3 \cdot 17^2$ and $584 = 2^3 \cdot 73$. So the common divisors of 2312 and 584 are $1, 2, 4, 8$.

   b. What is the smallest positive element of the set

$$S = \{2312m + 584n \mid m, n \in \mathbb{Z}\}?$$

      Solution: By Theorem 2.12, this number is $\gcd(2312, 584) = 8$.

   c. Apply the Euclidean algorithm to find $\gcd(2312, 584)$. What are the integers m, n such that $584m + 2312n = \gcd(2312, 584)$?

      Solution: Computing by the Euclidean process:

$$\begin{aligned}
2312 &= 3 \cdot 584 + 560 \\
584 &= 1 \cdot 560 + 24 \\
560 &= 23 \cdot 24 + 8 \\
24 &= 3 \cdot 8 + 0.
\end{aligned}$$

      The last nonzero remainder is 8, so $\gcd(2312, 584) = 8$. By the "back-substitution" method, we have

$$\begin{aligned}
8 &= 560 - 23 \cdot 24 \\
&= 560 - 23 \cdot (584 - 1 \cdot 560) \\
&= 24 \cdot 560 - 23 \cdot 584 \\
&= 24 \cdot (2312 - 3 \cdot 584) - 23 \cdot 584 \\
&= 24 \cdot 2312 - 95 \cdot 584.
\end{aligned}$$

      So $n = -95$ and $m = 24$.

'B' Section

1. Let f, g, h be permutations of a set A. In this problem, the notation $h^0 = I_A$, the identity mapping on A, and for $n \geq 1$, h^n means the n-fold composition of h with itself:

$$h^n = h \circ h \circ \cdots \circ h \quad (n \text{ copies of } h).$$

   a. Show by mathematical induction that h^n is a permutation of A for all $n \geq 0$. You may use facts we proved before here; look back at Chapter 1 or your notes as necessary.

Solution: The base case here is $n = 0$ and $h^0 = I_A$ by definition. This is a permutation of A since it is one-to-one and onto. Now assume that h^k is a permutation and consider $h^{k+1} = h^k \circ h$. By the induction hypothesis this is a composition of permutations of A. But every composition of permutations of A is also a permutation of A by Theorems 1.16 and 1.17 (in the special case that $A = B = C$).

b. Show that for all $n \geq 1$
$$(f \circ g \circ f^{-1})^n = f \circ g^n \circ f^{-1}.$$

Solution: When $n = 1$, there is nothing to prove, since $f \circ g \circ f^{-1} = f \circ g \circ f^{-1}$. So the base case is established. Now assume that $(f \circ g \circ f^{-1})^k = f \circ g^k \circ f^{-1}$ and consider $(f \circ g \circ f^{-1})^{k+1}$:

$$\begin{aligned}
(f \circ g \circ f^{-1})^{k+1} &= (f \circ g \circ f^{-1})^k \circ (f \circ g \circ f^{-1}) \text{ by the def.} \\
&= (f \circ g^k \circ f^{-1}) \circ (f \circ g \circ f^{-1}) \text{ by the induction hypothesis} \\
&= f \circ g^k \circ (f^{-1} \circ f) \circ g \circ f^{-1} \text{ by associativity of composition} \\
&= f \circ g^k \circ I_A \circ g \circ f^{-1} \text{ by definition of inverse mappings} \\
&= f \circ g^k \circ g \circ f^{-1} \text{ by associativity and identity} \\
&= f \circ g^{k+1} \circ f^{-1} \text{ by definition.}
\end{aligned}$$

Hence the formula is true for all $n \geq 1$ by induction.

2. Let $a, b, c, d \in \mathbb{Z}$.

a. Show that if $a|c$ and $b|d$, then $(ab)|(cd)$.

Solution: If $a|c$ then there is some integer k such that $c = ak$. Similarly, since $b|d$, there is some integer ℓ such that $d = b\ell$. Hence $cd = (ak)(b\ell) = (ab)(k\ell)$ by associativity and commutativity of multiplication in $\mathbb{Z}$. Since $k\ell \in \mathbb{Z}$, this shows $(ab)|(cd)$.

b. Is it true that $a|(bc)$ implies $a|b$ or $a|c$? Prove or give a counterexample.

Solution: This is *not true*. A counterexample: Let $a = 4$, $b = 6, c = 10$. Then $4|60$ is true, but 4 does not divide either 6 or 10.

c. Give two different proofs that $(a - b)|(a^n - b^n)$ for all $n \geq 1$, one using mathematical induction, one not using mathematical induction.

Solution: Induction proof: The statement is clearly true for $n = 1$, so the base case is established. Assume that $(a - b)|(a^k - b^k)$ and consider $a^{k+1} - b^{k+1}$. We can apply the induction hypothesis by rewriting this by "adding zero," then rearranging:

$$\begin{aligned}
a^{k+1} - b^{k+1} &= a^{k+1} - a^k b + a^k b - b^{k+1} \\
&= a^k(a - b) + b(a^k - b^k).
\end{aligned}$$

By the induction hypothesis $a - b$ divides $a^k - b^k$ and $a - b$ clearly divides the first part. Hence by a result proved in class, it follows that $(a - b)$ divides the sum and hence $(a - b)|(a^{k+1} - b^{k+1})$. This proves the statement by induction.

Noninduction proof: First we show the factorization formula for a difference of like powers. We claim:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

This is true because if we start on the right and expand out using the distributive law we get

$$\begin{aligned}(a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}) &= a^n + a^{n-1}b + \cdots + a^2b^{n-2} + ab^{n-1} \\ &\quad - a^{n-1}b - \cdots - ab^{n-1} - b^n \\ &= a^n - b^n,\end{aligned}$$

since all the terms except the a^n and the $-b^n$ cancel in pairs. Now, in the factored form, the second factor in the formula is in $\mathbb{Z}$ because a, b are. So this shows $(a-b)|(a^n - b^n)$.

d. Show that $(a+b)|(a^{2n} - b^{2n})$ for all $n \geq 1$.

Solution: (This can be proved in a number of ways. The "slickest" is this one:) Apply the result of part c with a replaced by a^2 and b replaced by b^2. Since $(a^2)^n = a^{2n}$ and similarly for b, this gives the statement that

$$(a^2 - b^2)|(a^{2n} - b^{2n})$$

But by the difference of squares factorization, $a^2 - b^2 = (a+b)(a-b)$, so $a+b$ divides $a^{2n} - b^{2n}$.

3. Suppose $a, b > 0$ and $a = qb + r$ by the division algorithm in $\mathbb{Z}$. What are the quotient and remainder on division of $-a$ by b? Express in terms of q and r, and prove your result.

Solution: If $a = qb + r$ by the division algorithm, then we can multiply both sides of that equation by -1 to get $-a = (-q)b + (-r)$. However, since $0 \leq r < b$, unless $r = 0$, the number $-r$ will not be in the proper range of values for the remainder on division by b. To get a remainder in the proper range of values, we just need to note that if $r \neq 0$, then $-b < -r < 0$, so $0 < -r + b < b$. Hence From $-a = (-q)b + (-r)$, we want to rearrange the right side by adding and subtracting b:

$$-a = (-q-1)b + (-r+b).$$

So by uniqueness of quotient and remainder, if $r \neq 0$, the quotient on division of $-a$ by b is $-(q+1)$, and the remainder is $-r+b$. If $r = 0$, then the new quotient is just $-q$ and the remainder is still 0 for $-a$. So the conclusion (and what we have proved above) is: If $a = qb + r$, then $-a = q'b + r'$, where

$$q' = \begin{cases} -q & \text{if } r = 0 \\ -(q+1) & \text{if } r \neq 0, \end{cases} \qquad r' = \begin{cases} 0 & \text{if } r = 0 \\ b - r & \text{if } r \neq 0. \end{cases}$$

4. Show that if $a, b, c \in \mathbb{Z}$, then $\gcd(\gcd(a,b),c) = \gcd(a, \gcd(b,c))$.

Solution: (Comment: We actually need some additional hypothesis like at least one of a, b, c nonzero here to guarantee that the gcd's exist.) Method 1: Let $d = \gcd(\gcd(a, b), c)$. We want to show that this integer satisfies the right properties to be $\gcd(a, \gcd(b, c))$ (from the definition of a gcd) as well. First, since d is a gcd of two integers, $d \in \mathbb{Z}^+$, so the first requirement is true. Next, $d | \gcd(a, b)$ and $d|c$ by definition. Since $d | \gcd(a, b)$, it also follows that $d|a$ and $d|b$. Then since $d|b$ and $d|c$, we have $d | \gcd(b, c)$. This shows the second requirement is true. Finally, suppose e is any common divisor of a and $\gcd(b, c)$, so $e|a$ and $e | \gcd(b, c)$. Since e divides $\gcd(b, c)$, $e|b$ and $e|c$. But then e is a common divisor of a, b so $e | \gcd(a, b)$ But then since e divides $\gcd(a, b)$ and c, $e | \gcd(\gcd(a, b), c)$ also. This shows $e|d$. Hence $d = \gcd(a, \gcd(b, c))$.

Solution: Method 2: An alternate method is to show that if we let $d = \gcd(\gcd(a, b), c)$ and $d' = \gcd(a, \gcd(b, c))$, then $d|d'$ and $d'|d$. If we know that, then $d = d'$ follows since $d, d' > 0$ by the definition of a gcd. If $d = \gcd(\gcd(a, b), c)$, then $d | \gcd(a, b)$ and $d|c$, so it follows that $d|a, d|b, d|c$. But then by definition of a gcd, $d|a$ and $d | \gcd(b, c)$. Hence $d|d'$. The proof that $d'|d$ is similar.

5. Suppose $\gcd(a, b) = 1$. Is it true that the integers m, n such that $ma + nb = 1$ guaranteed in Theorem 2.12 also satisfy $\gcd(m, n) = 1$? Prove or give a counterexample.

   Solution: If $\gcd(a, b) = 1$, then there are $m, n \in \mathbb{Z}$ such that $ma + nb = 1$ by Theorem 2.12. However, this also says that the smallest positive element of the set

   $$S = \{pm + qn \mid p, q \in \mathbb{Z}\}$$

   is 1, since we get 1 by taking $p = a$ and $q = b$. Hence by the proof of Theorem 2.12, $1 = \gcd(m, n)$ as well.