MTH 310: HW 1 - Solutions

Instructor: Matthew Cha

Due: May 23, 2018

Problems from Hungerford's book (3rd ed.) are labeled by **Hungerford chpt.sec.#.**

1. **(Hungerford 1.1.2)** Find the quotient q and remainder r when a is divided by b.

   (a) $a = -51$; $b = 6$

   (b) $a = 302$; $b = 19$

   (c) $a = 2000$; $b = 17$

   Solution.

   Recall that when a is divided by b the quotient and remainder are the unique integers that satisfy $a = bq + r$ where $0 \le r < b$.

   (a) $-51 = 6(-9) + 3$ so $q = -9$ and $r = 3$.

   (b) $302 = 19(15) + 17$ so $q = 15$ and $r = 17$.

   (c) $2000 = 17 * 117 + 11$ so $q = 117$ and $r = 11$.

2. **(Hungerford 1.1.7)** Use the Division Algorithm to prove that the square of any integer a is either of the form $3k$ or of the form $3k + 1$ for some integer k.

   Solution.

   Let $a \in \mathbb{Z}$. By the Division Algorithm(DA), there exist unique $q, r \in \mathbb{Z}$ such that $a = 3q + r$ where $0 \le r < 3$. Thus, the possible values for the remainder r are $0, 1$ and 2. Let's treat each case separately. (We want to show that a^2 when divided by 3 has a remainder of 0 or 1.)

   Case 1: $(r = 0)$ We have that $a^2 = (3q)(3q) = 3(3q^2)$. So a^2 is of the form $3k$.

   Case 2: $(r = 1)$ $a^2 = (3q+1)(3q+1) = (3q)^2 + 2(3q) + 1 = 3(3q^2 + 2q) + 1$. So a^2 is of the form $3k+1$.

   Case 3: $(r = 2)$ $a^2 = (3q + 2)(3q + 2) = (3q)^2 + 4(3q) + 4 = 3(3q^2 + 4q + 1) + 1$. So a^2 is of the form $3k + 1$.

   Therefore, a^2 is of the form $3k$ or $3k + 1$.

3. **(Hungerford 1.1.10)** Let n be a positive integer. Prove that a and c leave the same remainder when divided by n if and only if $a - c = nk$ for some integer k.

   Solution.

   $(\implies)$ Suppose a and c leave the same remainder when divided by n. Then there exists $q_1, q_2, r \in \mathbb{Z}$ such that

   $$\begin{aligned} a &= nq_1 + r \\ c &= nq_2 + r \qquad\qquad 0 \le r < n. \end{aligned}$$

   Subtracting the second equation from the first we get

   $$a - c = n(q_1 - q_2) + (r - r) = n(q_1 - q_2).$$

($\Longleftarrow$) Suppose $a - c = nk$ for some $k \in \mathbb{Z}$. By uniqueness of the remainder in the DA, we have that $a - c$ when divided by n leaves a unique remainder $r = 0$.

Now, apply the DA for a and c, respectively, when divided by n. There exist unique $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that

$$a = nq_1 + r_1 \qquad 0 \leq r_1 < n,$$
$$c = nq_2 + r_2 \qquad 0 \leq r_2 < n.$$

(We want to show that $r_1 = r_2$.) Without loss of generality (WLOG) suppose that $r_1 \geq r_2$, (otherwise just relabel). Subtracting the second equation from the first we get

$$a - c = n(q_1 - q_2) + (r_1 - r_2),$$

where $0 \leq r_1 - r_2 \leq r_1 < n$. By assumption, we know that $a - c$ when divided by n must leave a unique remainder $r = 0$. It follows that $r_1 - r_2 = 0$, and therefore, $r_1 = r_2$.

4. **(Hungerford 1.2.9)** If $a|c$ and $b|c$, must $ab|c$? Justify your answer.

   Solution.

   No. Consider $a = b = c > 1$. We have that $a|a$ but $a^2|a$ if and only if $a = \pm 1$.

5. **(Hungerford 1.2.11)** If $n \in \mathbb{Z}$, what are the possible values of the greatest common divisor

   (a) $(n, n+2)$
   (b) $(n, n+6)$

   Solution.

   (a) Let $d = (n, n+2)$. Recall that by definition, $d|n$ and $d|n+2$. So there are $k_1, k_2 \in \mathbb{Z}$ such that $n = dk_1$, and $n + 2 = dk_2$ with $1 \leq d \leq |n|$. Subtracting the first equation from the second and simplifying we have $2 = d(k_2 - k_1)$, and thus, $d|2$. The possible values of d are therefore 1 and 2. For example, the gcd of $(5, 7) = 1$ and $(6, 8) = 2$.
   (b) Let $d = (n, n+6)$. Recall that by definition, $d|n$ and $d|n+6$. So there are $k_1, k_2 \in \mathbb{Z}$ such that $n = dk_1$, and $n + 6 = dk_2$ with $1 \leq d \leq |n|$. Subtracting the first equation from the second and simplifying we have $6 = d(k_2 - k_1)$, and thus, $d|6$. Therefore, the possible values of d are $1, 2, 3, 6$. For example, the gcd of $(5, 11) = 1$, $(8, 14) = 2$, $(9, 15) = 3$, and $(6, 12) = 6$.

6. Prove that if k is a positive odd integers, then any sum of k consecutive integers is divisible by k.

   Solution.

   Let $n \in \mathbb{Z}$ and define S to be the sum of k consecutive integers starting from $n + 1$, that is,

$$S = \sum_{j=1}^{k} n + j = (n+1) + (n+2) + \cdots + (n+k).$$
$$= \left(\sum_{j=1}^{k} n\right) + \left(\sum_{j=1}^{k} j\right) = kn + \frac{k(k+1)}{2},$$

   where for the last equality we use the basic property that $\sum_{j=1}^{k} 1 = k$ and $\sum_{j=1}^{k} j = k(k+1)/2$.

   If k is odd then $k + 1$ is even, that is, $k + 1 = 2l$ for some $l \in \mathbb{Z}$. Substituting back into the previous equation, we have

$$S = kn + \frac{k(2l)}{2} = k(n + l).$$

   Therefore $k|S$.

7. **(Hungerford 1.2.20)** Prove that $(a,b) = (a, b+at)$ for every $t \in \mathbb{Z}$.

   Solution.

   Let $d = (a,b)$. Then, there exist $k_1, k_2 \in \mathbb{Z}$ be such that $dk_1 = a$ and $dk_2 = b$. By substitution and factoring, it follows that

$$\begin{aligned} b + ta &= dk_2 + tdk_1 \\ &= d(k_2 + tk_1). \end{aligned}$$

   Therefore, $d|a$ and $d|(b+ta)$.

   Suppose $c|a$ and $c|(b+ta)$. (We want to show that $c \le d$). Let $k_1, k_2 \in \mathbb{Z}$ be such that $ck_1 = a$ and $ck_2 = b + ta$. By substitution, we have $ck_2 = b + tck_1$ and simplifying gives

$$c(k_2 - tk_1) = b.$$

   Therefore, $c|a$ and $c|b$, and by the definition of greatest common divisor $d = (a,b)$, it follows that $c \le d$. We have shown that $d = (a, b+ta)$.

8. **(Hungerford 1.2.28)** Prove that a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3. [*Hint*: $10^3 = 999 + 1$ and similarly for other powers of 10.]

   Solution.

   Let $n \in \mathbb{Z}$ be positive. First, we prove the following lemma.

   Lemma 1. Let $n \in \mathbb{Z}$ be positive. Then, n can be written in terms of its digits, that is, there exist unique $m \ge 0$ and $0 \le k_1, k_2, \cdots k_m < 10$ such that

$$n = k_m 10^m + k_{m-1} 10^{m-1} + \cdots + k_1 10 + k_0 = \sum_{j=0}^{m} k_j 10^j.$$

   Proof. This follows from a repeated application of the DA: First, divide n by 10

$$n = 10q_1 + k_0, \qquad 0 \le k_0 < 10.$$

   If $0 \le q_1 < 10$ then stop, otherwise divide q_1 by 10 to get,

$$n = 10(10q_2 + k_1) + k_0 = q_2 10^2 + k_1 10 + k_0.$$

   If $0 \le q_2 < 10$ then stop, otherwise divide q_2 by 10. This process terminates when $0 \le q_m < 10$. ☐

   (The number k_j is called the 10^j's–*digit* of n. For example, $4357 = 4(10^3) + 3(10^2) + 5(10) + 7$.)

   Using the hint we have that $10^j = 99 \cdots 9 + 1$, and thus, $10^j = 3q_j + 1$ where $q_j = 33 \cdots 3$. Writing n in terms of its digits we have

$$n = \sum_{j=0}^{m} k_j 10^j = \sum_{j=0}^{m} k_j (3q_j + 1) = 3\left(\sum_{j=0}^{m} k_j q_j\right) + \sum_{j=0}^{m} k_j.$$

   Let $z = \sum_{j=0}^{m} k_j q_j$. It follows that $n = 3z + \sum_{j=0}^{m} k_j$.

   ($\Longrightarrow$) If $3|n$ then $3d = n$ for some $d \in \mathbb{Z}$. Thus, $3(d - z) = \sum_{j=0}^{m} k_j$, and therefore, $3| \sum_{j=0}^{m} k_j$.

   ($\Longleftarrow$) If $3| \sum_{j=0}^{m} k_j$ then $3d = \sum_{j=0}^{m} k_j$ for some $d \in \mathbb{Z}$. Thus, $3(d+z) = n$, and therefore, $3|n$.

9. **(Hungerford 1.2.34)** Prove that

   (a) $(a,b)|(a+b, a-b)$;

   (b) if a is odd and b is even, then $(a,b) = (a+b, a-b)$.

Solution.

(a) Let gcd of $(a, b) = d$ and $(a+b, a-b) = e$. By definition, $d|a$ and $d|b$, so that $dm = a$ and $dn = b$ for some $m, n \in \mathbb{Z}$. By substitution and factoring we have

$$a + b = dm + dn = d(m + n)$$
$$a - b = dm - dn = d(m - n).$$

Thus, $d|a + b$ and $d|a - b$ is a common divisor. Therefore, by Corollary 1.3 we have that $d|e$. Moreover, $d \leq e$.

(b) Suppose that a is odd and b is even. Write $a = 2j + 1$ and $b = 2k$ for some $j, k \in \mathbb{Z}$. Then, $a + b = 2(j + k) + 1$ and $a - b = 2(j - k) + 1$ are both odd. Since $e|a + b$ and $e|a - b$ we conclude that e must be odd. This implies that the gcd of $(e, 2) = 1$.

Let

$$em = a + b, \qquad en = a - b$$

for some $m, n \in \mathbb{Z}$. Adding and substracting both equations and factoring give, respectively,

$$e(m + n) = 2a$$
$$e(m - n) = 2b.$$

Thus, $e|2a$ and $e|2b$.

We have collectively shown that $e|2a$ and $e|2b$ and gcd of $(e, 2) = 1$. Therefore, by Theorem 1.4 we have that $e|a$ and $e|b$. By the definition for gcd of $d = (a, b)$ it follows that $e \leq d$. Combined with the first part of the problem $d \leq e$, we conclude $d = e$.