CISC-102 Winter 2019

Homework 6
Solutions

1. Find the quotient q and remainder r, as given by the Division Algorithm theorem for the following examples.

   (a) a = 500, b = 17
   $500 = 29 \times 17 + 7$

   (b) a = -500, b = 17
   $-500 = -30 \times 17 + 10$

   (c) a = 500, b = -17
   $500 = -29 \times -17 + 7$

   (d) a = -500, b = -17
   $-500 = 30 \times -17 + 10$

2. Show that $c|0$, for all $c \in \mathbb{Z}, c \neq 0$.

   Observe that $0 = c \times 0$ for for all $c \in \mathbb{Z}, c \neq 0$.

3. Show that $1|z$ for all $z \in \mathbb{Z}$.

   Observe that $z = z \times 1$ for all $z \in \mathbb{Z}$.

4. Use the fact that if $a|b$ and $b \neq 0$ then $|a| \leq |b|$ to prove that if $a|b$ and $b|a$ then $|a| = |b|$.

   If $a|b$ then $|a| \leq |b|$, and if $b|a$ then $|b| \leq |a|$, therefore we conclude that $|a| = |b|$.

5. Use the previous two results to prove that if $a|1$ then $|a| = 1$.

   The result of question 3 implies that $1|a$. The result of question 4 implies that since $1|a$ and $a|1$ then $|a| = 1$.

6. Let $a, b, c \in \mathbb{Z}$ such that $c|a$ and $c|b$. Let r be the remainder of the division of b by a, that is there is a $q \in \mathbb{Z}$ such that $b = qa + r, 0 \leq r < |b|$. Show that under these condition we have $c|r$.

   Observe that $c|b$ implies that $c|qa + r$. Recall that if $c|a$ then $c|qa$ for all $q \in \mathbb{Z}$. So if $c|(qa + r)$ and $c|qa$ then $c|(qa + r - qa)$ which simplifies to $c|r$.

7. Consider the function A, such that A(1) = 1, A(2) = 2, A(3) = 3, and for $n \in \mathbb{N}, n \geq 4$, $A(n) = A(n-1) + A(n-2) + A(n-3)$.

   (a) Find values $A(n)$ for $n = 4, 5, 6$.
   $A(4) = 3+2+1 = 6$, $A(5) = 6+3+2 = 11$, and $A(6) = 11+6+3 = 20$

   (b) Use the second form of mathematical induction to prove that $A(n) \leq 3^n$ for all natural numbers n.
   Base: $A(1) = 1 \leq 3^1$, $A(2) = 2 \leq 3^2$, and $A(3) = 3 \leq 3^3$.
   Induction Hypothesis: Assume that $A(j) \leq 3^j$ for $1 \leq j \leq k$.
   Induction Step:

$$\begin{aligned} A(k+1) &= A(k) + A(k-1) + A(k-2) \\ &\leq 3^k + 3^{k-1} + 3^{k-2} \\ &\leq 3 \times 3^k \\ &= 3^{k+1} \quad \square \end{aligned}$$

8. Let a = 1763, and b = 42

   (a) Find g = gcd(a,b). Show the steps used by Euclid's algorithm to find gcd(a,b).
   (1763) = 41(42) + 41
   (42) = 1(41) + 1
   (41) = 41(1) + 0
   gcd(1763,42) = gcd(42,41) = gcd(41,1)= gcd(1,0) = 1

   (b) Find integers m and n such that g = ma + nb

$$\begin{aligned} 1 &= 42 - 1(41) \\ &= 42 - 1[1763 - 41(42)] \\ &= 42(42) + (-1)1763 \end{aligned}$$

   (c) Find lcm(a,b)
   lcm(a,b) = $\frac{ab}{gcd(a,b)}$ = 74046

9. Prove gcd$(a, a+k)$ divides k.

Proof. Let $g = \gcd(a, a+k)$. Therefore $g|a$ and $g|a+k$, and this implies that $g|a+k-a$, that is, $g|k$. $\square$

10. If a and b are relatively prime, that is $\gcd(a, b) = 1$ then we can always find integers x, y such that $1 = ax + by$. This fact will be useful to prove the following proposition.

    Suppose p is a prime such that $p|ab$, that is p divides the product ab, then $p|a$ or $p|b$.

    Proof. We can look at two possible cases.

    Case 1: $p|a$ and then we are done.

    Case 2: $p \nmid a$, and since p is prime we can deduce that p and a are relatively prime. Therefore, there exist integers x, y such that

    $$1 = ax + py. \tag{1}$$

    Now multiply the left and right hand side of equation (1), by b to get:

    $$b = bax + bpy. \tag{2}$$

    We know that $p|ba$ so $p|bax$, and we can also see that $p|bpy$. Therefore, $p|(bax + bpy)$, and by equation (2) we can conclude that $p|b$.

    $\square$