# CISC-102 Fall 2016

## Homework 6
## Solutions

1. Show that any integer value greater than 2 can be written as $3a+4b+5c$, where $a, b, c$ are non-negative integers, that is $a, b, c \in \mathbb{Z}, a, b, c \geq 0$. Hint: Use the second form of induction.

   *Proof.* **Base:** $3 = 3 \times 1 + 4 \times 0 + 5 \times 0$. For this problem we need two additional base cases, that is, when $b > 0$ and when $c > 0$. So we have $4 = 3 \times 0 + 4 \times 1 + 5 \times 0$, and $5 = 3 \times 0 + 4 \times 0 + 5 \times 1$.

   **Induction Hypothesis:** All values $i$ such that, $2 < i \leq k$ can be written as $3a + 4b + 5c$, where $a, b, c$ are non-negative integers.

   **Induction Step:** Consider the value $k+1$, and the value $k$. By the induction hypothesis $k = 3a+4b+5c$ for non-zero integers $a, b, c$. There are 3 cases to consider.

Case 1: $a > 0$ in the expression $k = 3a + 4b + 5c$,
therefore $k + 1 = 3(a - 1) + 4(b + 1) + 5c$.

Case 2: $a = 0$, $b > 0$ in the expression $k = 3a + 4b + 5c$,
therefore $k + 1 = 4(b - 1) + 5(c + 1)$.

Case 3: $a = 0$, $b = 0$, and $c > 0$ in the expression $k = 3a + 4b + 5c$,
therefore $k + 1 = 3(a + 2) + 5(c - 1)$.

Therefore, by the principle of mathematical induction we conclude that any integer value greater than 2 can be written as $3a + 4b + 5c$, where $a, b, c$ are non-negative integers. □

2. Let $a, b \in \mathbb{R}$ . Prove $(ab)^n = a^n b^n$, for all $n \in \mathbb{N}$. Hint: Use induction on the exponent $n$.

*Proof.* **Base:** $(ab)^1 = a^1 b^1$

**Induction Hypothesis:** Assume that $(ab)^k = a^k b^k$ for $k \geq 1$.

**Induction Step:** Consider:

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

Therefore, by the principle of mathematical induction we conclude that $(ab)^n = a^n b^n$, for all $n \in \mathbb{N}$. $\square$

3. 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

4. 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, $g|k$. $\square$

5. 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 $p|b$.

   $\square$