CISC-102 Fall 2017

Homework 6
Solutions

1. 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 $n \in \mathbb{N}$. □

2. 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) $= \frac{ab}{gcd(a,b)} = 74046$

3. 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, $g|k$. □

4. 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 $p|b$.

□