Homework 4 (Due Tues, Feb 18)

Math 2710 – Spring 2014

Professor Hohn

Using the proof techniques we have learned in class, prove each statement.

1. (pg. 50 #74) Show that $\gcd(ab, c) = \gcd(b, c)$ if $\gcd(a, c) = 1$. Is it true in general that

$$\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)\,?$$

Solution:

Proof. Let $a, b, c \in \mathbb{Z}$ and assume that $\gcd(a, c) = 1$. By the Euclidean Algorithm, $a \cdot x + c \cdot y = 1$ for some $x, y \in \mathbb{Z}$. By multiplying both sides of the equation by b, $ab \cdot x + c \cdot by = b$. Let $d = \gcd(ab, c)$. By the definition of gcd, $d \mid ab$ and $d \mid c$. Hence, $d \mid (ab \cdot x + c \cdot by)$ and $d \mid b$. Therefore, d is a common divisor of b and c.

Suppose d is not the greatest common divisor of b and c. Then, there exists a $\hat{d} > d$ that is the greatest common divisor of b and c. By the Euclidean Algorithm, $\exists p, q \in \mathbb{Z}$ such that $ab \cdot p + c \cdot q = d$. By the definition of the gcd, $\hat{d} \mid b$ and $\hat{d} \mid c$, and $\hat{d} \mid (b \cdot ap + c \cdot q)$. Thus, $\hat{d} \mid d$ $\lightning$. It follows that d is the $\gcd(b, c)$. □

Let $a = b = c = 3$. Then, $\gcd(3 \cdot 3, 3) = \gcd(9, 3) = 3$, and $\gcd(3, 3) = 3$. Therefore, if $\gcd(ab, c) = \gcd(a, c) \cdot \gcd(b, c)$, then $3 = 3 \cdot 3$ $\lightning$. So, $\gcd(ab, c) \neq \gcd(a, c) \cdot \gcd(b, c)$ for all $a, b, c \in \mathbb{Z}$.

2. (pg. 50 #84) Prove that the Diophantine equation $ax + by + cz = e$ has a solution if and only if $\gcd(a, b, c) \mid e$.

Solution:

Proof. ($\Longrightarrow$) Let $a, b, c \in \mathbb{Z}$, and suppose $e = ax + by + cz$ for some $x, y, z \in \mathbb{Z}$. Let d be the $\gcd(a, b, c)$. By the definition of gcd, $d \mid a$, $d \mid b$, and $d \mid c$. Hence, $d \mid (ax + by + cz)$ and $d \mid e$. Therefore, $\gcd(a, b, c) \mid e$.

($\Longleftarrow$) Let $d = \gcd(a, b, c)$ and $f = \gcd(b, c)$. By #83 (Homework 3), $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$. By the Euclidean Algorithm, $d = a \cdot m + f \cdot n$ for $m, n \in \mathbb{Z}$. Additionally, $f = b \cdot p + c \cdot q$ for $p, q \in \mathbb{Z}$. Then, $d = a \cdot m + b \cdot np + c \cdot nq$. Suppose $\gcd(a, b, c) \mid e$. By the definition of divides, there exists $k \in \mathbb{Z}$ such that

$$\begin{aligned} e &= d \cdot k \\ &= (a \cdot m + b \cdot np + c \cdot nq) \cdot k \\ &= a \cdot mk + b \cdot npk + c \cdot nqk \\ &= ax + by + cz \end{aligned}$$

where $x = mk$, $y = npk$, and $z = nqk$. Hence, there exists integers x, y, z such that $e = ax + by + cz$. □

3. (pg. 50 #107) Let a, b, c, where a is a positive integer and b and c are odd primes. Prove that if $a \mid (3b+2c)$ and $a \mid (2b+3c)$, then $a = 1$ or 5. Give examples to show that both these values for a are possible.

Solution:

Proof. Let a, b, c, where a is a positive integer and b and c are odd primes, both not equal to 5. Suppose $a \mid (3b + 2c)$ and $a \mid (2b + 3c)$. Then, $a \mid (3(2b + 3c) - 2(3b + 2c))$ and $a \mid (3(3b + 2c) - 2(2b + 3c))$. Hence, $a \mid 5c$ and $a \mid 5b$. Since b and c are odd primes, there exist integers x, y such that $bx + cy = 1$. Since $a \mid 5c$ and $a \mid 5b$, $a \mid (5b \cdot x + 5c \cdot y)$, and $a \mid 5 \cdot 1$. Then, $5 = a \cdot n$ for some $n \in \mathbb{Z}$. By the Unique Factorization Them, 5 is equal to a product of primes. So, either $a = 5$ or $a = 1$. □

Example 1: Let $b = 3$ and $c = 5$. Then, if $a \mid 19$ and $a \mid 21$, then $a = 1$.

Example 2: Let $b = 3$ and $c = 13$. Then, if $a \mid 35$ and $a \mid 45$, then $a = 5$ or $a = 1$.