Written Assignment 3
Math 290, Dr. Walnut

Lucas Bouck

10/13/15

1 Problem 1

Let a and b be natural numbers with $GCD(a, b) = d$. Prove that if the natural number c is a common divisor of a and b, then $GCD\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{d}{c}$.

Proof:

Let a and b be natural numbers with $GCD(a, b) = d$. Assume that the natural number c is common divisor of a and b. We want to show that $GCD\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{d}{c}$. Since $GCD(a, b) = d$, $dm = a$ and $dn = b$ where m and n are integers. By dividing c from both sides, we get $\frac{d}{c}m = \frac{a}{c}$ and $\frac{d}{c}n = \frac{b}{c}$. Since $m, n \in \mathbb{Z}$, $\frac{d}{c}$ divides both $\frac{a}{c}$ and $\frac{b}{c}$. Say there exists an integer k such that k is a common divisor of $\frac{a}{c}$ and $\frac{b}{c}$ and that $k > \frac{d}{c}$. Then, $kx = a/c$ and $ky = b/c$ where x and y are integers. Then, $kxc = a$ and $kyc = b$. Since x and y are integers, kc is a common divisor of a and b. Since $d = GCD(a, b)$, $kc \leq d$. Then, $k \leq d/c$. This contradicts the assumption that $k > d/c$, so there does not exist a common divisor of a/c and b/c that is greater than d/c. Thus, $GCD(\frac{a}{c}, \frac{b}{c}) = \frac{d}{c}$.

2 Problem 2a

Let a, b and c be natural numbers. Prove that if there exists integers x and y such that $ax + by = 1$ then $GCD(a, b) = 1$.

Proof:

Let a, b and c be natural numbers. Assume that there exist integers x and y such that $ax + by = 1$. We want to show that 1 is the greatest common divisor of a and b. Since 1 divides any natural number, $1|a$ and $1|b$. Say there is an integer m such that m divides a and b. Then, $mk = a$, and $ml = b$ for some integers k and l. Then, $mkx = ax$, and $mly = by$. Then, $mkx + mly = m(kx + ly) = ax + by$ Since $k, x, l, y \in \mathbb{Z}$, $kx + ly \in \mathbb{Z}$. Thus, $m|(ax + by)$. Since $ax + by = 1$, $m|1$. Since $m|1$, $m \leq 1$. Since 1 divides both a and b, and 1 is greater than or equal to any other common divisor of a and b, $GCD(a, b) = 1$.

3 Problem 2b

Let a and b be natural numbers. Prove using the result of (a) (and the fact that it was proved in class that the converse of the statement in part (a) is also true) that $GCD(a, b) = 1$ if and only if $GCD(a, b^2) = 1$.

Proof:

($\Rightarrow$) Let a and b be natural numbers. Let $GCD(a, b) = 1$. We want to show that $GCD(a, b^2) = 1$. Since $GCD(a, b) = 1$, there exist integers x and y such that $ax + by = 1$. By subtracting ax from both sides, we know $by = 1 - ax$. By taking the original identity and multiplying it by by, we get $axby + b^2y^2 = by$. Since $by = 1 - ax$, $axby + b^2y^2 = 1 - ax$. By adding ax to both sides, we get $ax + axby + b^2y^2 = a(x + xby) + b^2y^2 = 1$. Let $(x + xby) = m$ and $y^2 = n$. Since $x, b, y \in \mathbb{Z}$, m is an integer. Since y is an integer, n is an integer. Since there exist integers m and n such that $am + b^2n = 1$, $GCD(a, b^2) = 1$.

($\Leftarrow$) (By contrapositive) Let $a, b \in \mathbb{N}$. Let $GCD(a, b) \neq 1$. That means there exists a natural number d such that $GCD(a, b) = d$ and $d \neq 1$. We want to show that $GCD(a, b^2) \neq 1$. Since $d \neq 1$ and $d \in \mathbb{N}$, $d > 1$ Since $GCD(a, b) = d$, $dm = a$ for some integer m, and $dn = b$ for some integer n. Let there exist integers x and y such that $ax + b^2y = GCD(a, b^2)$. By multiplying dn by yb, we get $dnyb = b^2y$. By multiplying dm by x, we get $dmx = ax$. Then, $ax + b^2y = dmx + dnyb = d(mx + nyb)$. Let $mx + nyb = k$. Since $m, x, y, b \in \mathbb{Z}$, $k \in \mathbb{Z}$. Since $dk = ax + b^2y$ where $k \in \mathbb{Z}$, $d|(ax + b^2y)$. Since $d|(ax + b^2y)$, then $d|GCD(a, b^2)$. Since $d|GCD(a, b^2)$, then $d \leq GCD(a, b^2)$. Since $1 < d \leq GCD(a, b^2)$, then $GCD(a, b^2) > 1$. Therefore, $GCD(a, b^2) \neq 1$.

4 Problem 2c

Let a, b and c be natural numbers. Prove that if $GCD(a, b) = 1$ and $a|bc$, then $a|c$.

Proof:

Let a, b and c be natural numbers. Assume that $GCD(a, b) = 1$ and $a|bc$. Since $a|bc$, $am = bc$ for some integer m. Since $GCD(a, b) = 1$, there exist integers x and y such that $ax + by = 1$. By multiplying c to both sides, we get $axc + byc = c$. Since $am = bc$, then $aym = byc$. Then, $axc + byc = axc + aym = a(xc + ym)$. Let $xc + ym = d$. Since $x, c, y, m \in \mathbb{Z}$, $d \in \mathbb{Z}$. Thus, $ad = axc + byc = c$ where d is an integer. Therefore, $a|c$.