MAT 373 Homework 3 (Revised)

Justyce Countryman

February 5, 2024

Problem 1: Prove or disprove that if a, b, c are integers such that $gcd(a, c) = 1 = gcd(b, c)$, then $gcd(ab, c) = 1$.

Proof. Suppose we have integers a, b, c such that $gcd(a, c) = 1 = gcd(b, c)$. This means that there are integers x, y, d, e such that:

$$ax + cy = 1 \tag{1}$$

$$bd + ce = 1 \tag{2}$$

Multiplying both sides of equation (2) by a gives us:

$$abd + ace = a \tag{3}$$

Substituting the left hand side of equation (3) for a into equation (1) yields the following equivalent equations:

$$(abd + ace)x + cy = 1 \tag{4}$$

$$abdx + acex + cy = 1 \tag{5}$$

$$ab(dx) + c(aex + y) = 1 \tag{6}$$

Since we know d, x, a, e, x, y are integers, the expressions dx and $aex + y$ are also integers. Therefore equation (6) allows us to state that if $gcd(a, c) = 1 = gcd(b, c)$, then $gcd(ab, c) = 1$.

$\square$

Problem 2: Prove or disprove that if a, b, c, d are integers such that $gcd(a, b) = 1 = gcd(c, d)$, then $gcd(ac, bd) = 1$.

Counterexample: Suppose a, b, c, d are integers such that $gcd(a, b) = 1 = gcd(c, d)$. Let's say $a = 2$, $b = 11$, $c = 5$, $d = 6$. This example is acceptable since $gcd(a, b) = 1$ and $gcd(c, d) = 1$. Additionally, $ac = 10$ and $bd = 66$, which means that $gcd(ac, bd) = 2 \neq 1$.

Problem 3: Prove if a, b are integers with $gcd(a, b) = 1$, then $gcd(a^2, b) = 1$.

Proof. Suppose a, b are integers with $gcd(a, b) = 1$. We then know that there exists integers x, y such that:

$$ax + by = 1 \tag{7}$$

Squaring both sides of equation (7) gives us:

$$(ax + by)^2 = 1^2$$

$$a^2(x^2) + b(2axy + by^2) = 1 \tag{8}$$

Since a, b, x, y are integers and the sum or product of two integers creates another integer, we can say x^2 and $2axy + by^2$ are both integers. Equation (8) can help us confirm that $gcd(a^2, b) = 1$.

□

Problem 4: Assuming that $gcd(a, b) = 1$, prove that $gcd(a + b, a - b) = 1$ or 2.
Hint: Let $d = gcd(a + b, a - b)$ and show that $d|2a, d|2b$ and thus that $d \leq gcd(2a, 2b) = 2gcd(a, b)$

Proof. Suppose $gcd(a, b) = 1$ and $d = gcd(a + b, a - b)$. Therefore, $d|a + b$ and $d|a - b$. Additionally, $d|2a$ and $d|2b$ because these statements represent a linear combination of $a + b$ and $a - b$. As a result, we can then say $d|2gcd(a, b) = 2$. Thus, $d|2$, meaning the only positive integers of d in which this statement is true are 1 or 2, proving that if $gcd(a, b) = 1$, then $gcd(a + b, a - b) = 1$ or 2.

□

Problem 5: Show that if n is any integer such that $3 \nmid n$, then $3|(n^2 + 2)$. Hint: Division Algorithm

Proof. Suppose that n is any integer such that $3 \nmid n$. This means $n \neq 0$ and n is not a multiple of 3. Now, let's apply the Division Algorithm which states that if we have integers a, b with $a > 0$, then there are unique integers q, r such that:

$$b = aq + r \tag{9}$$

where $0 \leq r < a$. Since we know that 3 and n are both integers, we can apply the Division Algorithm. Additionally, since we know $3 \nmid n$, we can plug in $a = 3$ and $b = n$ into equation (9) and state that:

$$n = 3q + r \tag{10}$$

where $0 < r < 3$. Since we also know that r is an integer, it is only possible that either $r = 1$ or $r = 2$. We thus consider those two cases individually.

For our first case, let's plug in $r = 1$ and square both sides of equation (10), which results in:

$$n^2 = (3q + 1)^2 \tag{11}$$

By expanding the right side of equation (11), we then get:

$$n^2 = 9q^2 + 6q + 1 \tag{12}$$

Finally, let's add 2 to both sides:

$$n^2 + 2 = 9q^2 + 6q + 3 = 3(3q^2 + 2q + 1) \tag{13}$$

Notice that equation (13) can be factored to be in the form of $3k$, where $k = 3q^2 + 2q + 1$, thus making k an integer since we already know q is an integer. Therefore, this allows us to indicate that for when $r = 1$, $3|(n^2 + 2)$.

Applying the same plan for our second case for when $r = 2$ gives us:

$$n^2 = (3q + 2)^2 \tag{14}$$

$$n^2 = 9q^2 + 12q + 4 \tag{15}$$

$$n^2 + 2 = 9q^2 + 12q + 6 = 3(3q^2 + 4q + 2) \tag{16}$$

Equation (16) can also be factored to be in the form of $3k$, where $k = 3q^2 + 4q + 2$. Once again, k is an integer since q is an integer. Thus, for all possible cases of r, $3|(n^2 + 2)$. We can then state that if $3 \nmid n$, then $3|(n^2 + 2)$.

$\square$