Worksheet 5: Biconditionals, Existence and Uniqueness, Bézout's Theorem

Problem 1. Let a be an integer. Show that $a^2 + 4a + 5$ is odd if and only if a is even.

Solution. If a is even, then $a \equiv 0 \bmod 2$, so

$$a^2 + 4a + 5 \equiv 0 + 0 + 5 \equiv 1 \bmod 2$$

so $a^2 + 4a + 5$ is odd. Conversely, if a is odd, then $a \equiv 1 \bmod 2$, so

$$a^2 + 4a + 5 \equiv 1 + 0 + 5 \equiv 0 \bmod 2$$

so $a^2 + 4a + 5$ is even. Thus $a^2 + 4a + 5$ is odd if and only if a is even.

Problem 2. Suppose a and b are real numbers with $a \neq 0$. Show that there exists a unique real number x such that $ax + b = 0$.

Solution. For existence, we take $x = -b/a$, so that

$$a \cdot (-b/a) + b = -b + b = 0$$

as desired. For uniqueness, suppose x and x' are real numbers such that $ax + b = 0$ and $ax' + b = 0$. Then

$$0 = 0 - 0 = (ax + b) - (ax' + b) = a(x - x').$$

Since a is nonzero, this implies that $x - x' = 0$, ie, that $x = x'$.

Problem 3. Suppose a and b are nonzero integers. Show that any common divisor of a and b divides $\gcd(a, b)$.

Solution. Let c be a common divisor of a and b. By Bézout's theorem, we know that there exist x and y such that $ax + by = \gcd(a, b)$. Since $c \mid a$ and $c \mid b$, we have $c \mid ax + by = \gcd(a, b)$ as well.

Problem 4. Show that $\gcd(n, n + 2) \in \{1, 2\}$ for an integer n.

Solution. Note that $2 = (n + 2) - n$ is a linear combination of n and $n + 2$, so $\gcd(n, n + 2) \mid 2$. Since $\gcd(n, n + 2)$ is positive and 2 is prime, this means that $\gcd(n, n + 2)$ must be either 1 or 2.

Problem 5. Suppose a, b, c are integers and $\gcd(a, c) = \gcd(b, c) = 1$. Prove that $\gcd(ab, c) = 1$.

Solution. There exist integers x_1, x_2, y_1, y_2 such that $ax_1 + cx_2 = 1$, and $by_1 + cy_2 = 1$. Thus

$$1 = 1 \cdot 1 = (ax_1 + cx_2)(by_1 + cy_2) = ab(x_1y_1) + c(bx_2y_1 + ax_1y_2 + cx_2y_2)$$

so 1 is a linear combination of ab and c. Thus $\gcd(ab, c) \mid 1$, which means that $\gcd(ab, c) = 1$.

Problem 6. Suppose a, b, c are integers and $a \mid bc$. Then $a \mid \gcd(a, b) \gcd(a, c)$.

Solution. There are integers x_1, x_2, y_1, y_2 such that $\gcd(a, b) = ax_1 + bx_2$ and $\gcd(a, c) = ay_1 + cy_2$. Then

$$\gcd(a, b) \gcd(a, c) = (ax_1 + bx_2)(ay_1 + cy_2) = a(ax_1y_1 + cx_1y_2 + bx_2y_1) + bc(x_2y_2).$$

Clearly a divides the first term, and since it divides bc, it also divides the second term. Thus $a \mid \gcd(a, b) \gcd(a, c)$.

Problem 7. Excised.

Problem 8. Let a and b be integers with $b > 0$. Prove that there exist unique integers q and r such that $a = bq + r$ where $2b \leqslant r < 3b$. *Note.* You may use the existence and uniqueness statement of the division algorithm.

Solution. Let us first prove existence. By the division algorithm, there exist integers q_0 and r_0 such that $a = bq_0 + r_0$ where $0 \leqslant r_0 < b$. Then

$$a = bq_0 - 2b + 2b + r_0 = b(q_0 - 2) + (2b + r_0)$$

so if we let $q = q_0 - 2$ and $r = 2b + r_0$, then $a = bq + r$ where $2b \leqslant r < 3b$.

Let us now prove uniqueness (differently from how we did it in class). Suppose there exist two sets of integers q, r and q', r' such that $a = bq + r$ and $a = bq' + r'$ and $2b \leqslant r, r' < 3b$. Then

$$0 = a - a = (bq + r) - (bq' + r') = b(q - q') + (r - r'),$$

which means that

$$r - r' = b(q' - q).$$

In other words, $b \mid (r - r')$. But since $2b \leqslant r, r' < 3b$, we must have $|r - r'| < b$. The only way a number with absolute value strictly smaller than b can be divisible by b is if it is 0. Thus, $r - r' = 0$, ie, $r = r'$. But then we must also have $b(q' - q) = r - r' = 0$, and since $b > 0$, this means that $q' - q = 0$, ie, $q = q'$. This proves uniqueness.

Problem 9. Let p be an odd prime. Show that, for any integer a, we have

$$\gcd\left(a + 1, \frac{a^p + 1}{a + 1}\right) = 1 \text{ or } p.$$

Possible hint. Since p is odd, we have $a^p + 1 = (a + 1)(a^{p-1} - a^{p-2} + a^{p-3} - \cdots - a + 1)$. This shows that $(a^p + 1)/(a + 1)$ is an integer, and you can also use this to calculate what $(a^p + 1)/(a + 1)$ is congruent to mod $a + 1$.

Solution. Since p is odd, we have

$$\frac{a^p + 1}{a + 1} = a^{p-1} - a^{p-2} + a^{p-3} - \cdots - a + 1.$$

Since $a \equiv -1 \bmod a + 1$, we have

$$\frac{a^p + 1}{a + 1} \equiv (-1)^{p-1} - (-1)^{p-2} + \cdots - (-1) + 1 \equiv 1 + 1 + \cdots + 1 = p \bmod a + 1,$$

where we have used the fact that p is odd again. We now have at least two strategies for completing the proof.

Strategy 1. By problem 10 on worksheet 3, we know that

$$\gcd\left(a + 1, \frac{a^p + 1}{a + 1}\right) = \gcd(a + 1, p).$$

Thus this gcd must divide p, and since p is prime, it must be either 1 or p.

Strategy 2. The fact that $(a^p + 1)/(a + 1) \equiv p \bmod a + 1$ means that there exists there exists an integer k such that

$$\frac{a^p + 1}{a + 1} - (a + 1)k = p.$$

In other words, p is a linear combination of $a + 1$ and $(a^p + 1)/(a + 1)$, so the gcd of these two integers must divide p by Bézout's theorem. Since p is prime, this gcd must be 1 or p.

Problem 10. *Prelude*. The point of this problem is to prove *one direction* of a fact that you may be familiar with from grade school, namely, that a number is rational if and only if its decimal expansion repeats after some point. We'll prove the other direction later. *Problem Statement*. If $a_n, a_{n-1}, a_{n-2}, \ldots, a_1, a_0, a_{-1}, \ldots$ are all in $\{0, 1, \cdots, 9\}$, we use the string

$$a_n \cdots a_1 a_0.a_{-1} a_{-2} \ldots$$

to represent the number

$$A = 10^n a_n + 10^{n-1} a_{n-1} \cdots 10a_1 + a_0 + 10^{-1} a_{-1} + 10^{-2} a_{-2} + \cdots.$$

Suppose there exists an integer $m \leqslant 0$ and an integer $k > 0$ such that $a_i = a_{i-k}$ for all $i > m$. Prove that A is rational. *Suggestion*. Start by proving that the number

$$12.75151515151515151515151 \cdots$$

is rational. Then generalize your argument.

Solution. Observe that A is rational if and only if $10^{-m}A$ is rational. The decimal expansion of $10^{-m}A$ is of the form

$$a_{n-m} \cdots a_1 a_0 \cdots a_{-1} \cdots a_m . a_{m-1} a_{m-2} \cdots$$

where $a_{m-1} = a_{m-1-k}$, $a_{m-2} = a_{m-2-k}$, and so forth. In other words, we have arranged it so that everything after the decimal point repeats with cycle k. Moreover, if B is the integer represented by $a_{n-m} \cdots a_1 a_0$, then $10^m A$ is rational if and only if $10^m A - B$ is rational. Thus it is sufficient to show that $10^m A - B$ is rational.

In other words, we may replace A with $10^m A - B$ without loss of generality, which means that we have $n = m = 0$ and $a_0 = 0$. In other words, A is represented by

$$0.a_{-1} a_{-2} \cdots$$

where $a_{-1} = a_{-1-k}$ and $a_{-2} = a_{-2-k}$ and so forth, and we want to show that this number is rational. Let B be the integer represented by $a_{-1} \cdots a_{-k}$. Then the repeating of the digits implies that

$$10^k A - B = A.$$

Rearranging this equation, we see that $(10^k - 1)A = B$, or

$$A = \frac{B}{10^k - 1}.$$

Sicne B and $10^k - 1$ are both integers, we conclude that A is rational.