MATH403: Homework 1

James Zhang*

September 5, 2024

1. Suppose a and b are integers that divide the integer c. If a and b are relatively prime, show that ab divides c. Show, by example, that if a and b are not relatively prime, then ab need not divide c.

Proof. We're given that $(a|c) \wedge (b|c)$, and that $(a, b) = 1$, where $(\circ, \circ') = GCD(\circ, \circ')$. By definition of relatively prime and Bezout's Lemma, $\exists\ s, t \in \mathbb{Z}$ such that $as+bt = 1$. Multiply both sides of this equation to get

$$c(as + bt) = c \implies cas + cbt = c$$

We want to show that $\exists\ k \in \mathbb{Z}$ such that $c = k(ab)$. Since $(a|c) \wedge (b|c)$, there exists $m, n \in \mathbb{Z}$ such that $c = am$ and $c = bn$. Substituting above bn into the first c and am into the second c, we obtain

$$asbn + btam = c \implies ab(sn + tm) = c$$

Let $k = sn + tm$, which must be in $\mathbb{Z}$ because $s, n, t, m \in \mathbb{Z}$, too. Therefore, $ab|c$, as desired.

If a and b are not relatively prime, then ab neeed not divide c. As a counterexample, consider $a = 4$, $b = 6$, and $c = 12$. 4 divides 12 and 6 divides 12 but their product, 24 does not divide 12. □

*Email: jzhang72@terpmail.umd.edu

2. Prove that there are infinitely many prime numbers.

Proof. On the contrary, assume there are a finite number of prime numbers, denoted as $p_1, \ldots, p_k, k \in \mathbb{N}$. Note that $p_1 = 2$. Importantly, also note that $p_i > 1 \; \forall \; i$. Now consider the integer

$$x = 1 + \prod_{i=1}^{k} p_i$$

By the division algorithm,

$$x = p_i \left(\prod_{j=1, j \neq i}^{k} \right) + 1 \; \forall \; i$$

and so dividing x by all p_i's yields a remainder of 1. Therefore, given our finite set of primes and since all primes do not divide x (and therefore there cannot exist a non-prime number that divides x because all non-prime numbers can be rewritten as a product of primes by the Fundamental Theorem of Arithmetic), and so x itself must be prime, or by the Fundamental Theorem of Arithmetic, since x must also omit a prime factorization decomposition, we must add a new prime to our list of primes. In either case, we have found a new prime, and so therefore, there are infinitely many prime numbers, as desired. □

3. If p is a prime and p divides $a_1 a_2 \cdots a_n$, where each a_i is an integer, prove that p divides a_i for some i.

Proof. First let us prove Euclid's Lemma, which states that if p is a prime and $p|(ab)$, then $(p|a) \vee (p|b)$.

Euclid's Lemma. Suppose p is a prime, $p|(ab)$, and without loss of generality, p does not divide a. We want to show that $p|b$. By Bezout's Lemma, $\exists\, x, y \in \mathbb{Z}$ such that $px + ay = 1$. Therefore, multiplying b on both sides,

$$pbx + aby = b$$

Note that

$$\begin{aligned} p|p &\implies p|pbx \implies mp = pbx \\ p|ab &\implies p|aby \implies np = aby \end{aligned}$$

where $m, n \in \mathbb{Z}$ and $p|(ab)$ by assumption. Therefore, we have $p(m+n) = b$ where $m + n \in \mathbb{Z}$, and so $p|b$, as desired. □

Equipped with the proof of Euclid's Lemma, we are ready to prove the original problem. Suppose p is prime and $p|a_1 a_2 \cdots a_n$. Let $b_1 = a_2 \cdots a_n$. Therefore, by direct substitution, $p|a_1 b_1$. By Euclid's Lemma, $(p|a_1) \vee (p|b_1)$. If $p|a_1$, then we are done. Otherwise, $p|b_1$, but $b_1 \neq a_i \;\forall\; i$. However, since $p|b_1$, this implies that $p|a_2 a_3 \cdots a_n$. Follow a similar procedure as above.

Let $b_2 = a_3 a_4 \cdots a_n$. Thus, $p|a_2 b_2$ and so by Euclid's Lemma, $(p|a_2) \vee (p|b_2)$. If $p|a_2$ then we are done. Continue following this nested, recursive pattern to find the i such that $p|a_i$.

□

4. Define a relation in R as follows:

$$a \sim b \text{ iff } a - b \in \mathbb{Z}$$

Show that $\sim$ is an equivalence relation and describe its equivalence classes. What happens if we replace $\mathbb{Z}$ by $\mathbb{N} \cup \{0\}$ in the definition of our relation?

Proof. Let $R \subset \mathbb{R} \times \mathbb{R}$. First, let us show that this relation $\sim$ is an equivalence relation. For any $a \in \mathbb{R}$, $a - a = 0 \in \mathbb{Z}$, so $a \sim a$ for all $a \in \mathbb{R}$ and reflexivity is satisfied. For symmetry, note that if $a \sim b$, then $a - b \in \mathbb{Z}$ but also $b - a = -(a - b) \in \mathbb{Z}$ and so $b \sim a$, so symmetry is satisfied. Finally, suppose $a \sim b$ such that $a - b = m \in \mathbb{Z}$ and $b \sim c = n \in \mathbb{Z}$. Since $(a - c) = (a - b) + (b - c) = m + n \in ZZ$ then $a - c \in \mathbb{Z}$ and so $a \sim c$. In this original relation, the equivalence class for a number $a \in \mathbb{R}$ is

$$[a] = \{x \in \mathbb{R} \mid x \sim a\} = \{x \in \mathbb{R} \mid x - a \in \mathbb{Z}\}$$

Here are some example equivalence classes.
$[0] = [\ldots, -1, 0, 1, \ldots]$
$[\pi] = [\ldots, -\pi, 0, \pi, \ldots]$
$[1.2] = [\ldots, -2.2, -1.2, -0.2, 0.8, 1.8, 2.8, \ldots]$.

If we replace $\mathbb{Z}$ by $\mathbb{N} \cup \{0\}$ in the definition of our relation, then reflexivity is still satisfied; however, symmetry would no longer be satisfied. As a counter example, let $a = 3, b = 2$, then $a \sim b = a - b = 1$. However, $b - a = -1 \notin \mathbb{N} \cup \{0\}$. Therefore, this new $\sim$ is not an equivalence relation. □

5. Suppose n_1 and n_2 are two natural numbers that are relatively prime. Let a_1 and a_2 be any two integers. Prove that the system

$$\begin{cases} x \equiv a_1 (\text{mod } n_1) \\ x \equiv a_2 (\text{mod } n_2) \end{cases}$$

has a unique solution in $\mathbb{Z}_N$, where $N = n_1 n_2$.

Proof. Let $N = n_1, n_2$ and let

$$y_1 = \frac{N}{n_1} = n_2 \qquad\qquad y_2 = \frac{N}{n_2} = n_1$$

Now let

$$z_1 = y_1^{-1} (\text{mod } n_1) \qquad\qquad z_2 = y_2^{-1} (\text{mod } n_2)$$

Importantly, these exist because n_1, n_2 are relatively prime. Note that the inverse y_i^{-1} is a number that when multiplied by y_1 gives $1 (\text{mod } n_1)$. Numerically, $y_i y_i^{-1} \bmod n_i = 1 \implies y_i y_i^{-1} = n_i k + 1, k \in \mathbb{Z}$. The integer sum $x = a_1 y_1 z_1 + a_2 y_2 z_2$ is a solution to this equation.

$$x \equiv (a_1 y_1 z_1 + a_2 y_2 z_2) \bmod n_1$$

Note that $y_2 \bmod n_1 = 0$ and so the above is equivalent to

$$\begin{aligned} x &\equiv (a_1 y_1 z_1) \bmod n_1 \\ x &\equiv a_1 \bmod n_1 \end{aligned}$$

as desired. The opposite direction is similar to show that $x \equiv a_2 \bmod n_2$. To show that this solution x is unique in $\mathbb{Z}_N$, assume there were two solutions, u and v. By construction, the difference $u - v$ must divide n_1 and n_2. Since u and v are relatively prime, $u - v$ must also divide $N = n_1 n_2$.

$$\begin{aligned} u - v \mid n_1 n_2 \\ u \equiv v \bmod N \end{aligned}$$

Therefore, the solution to this system is indeed unique in $\mathbb{Z}_N$.

□