Nathan Bickel
MATH 574: Section H01
Professor: Dr. Luo
November 6, 2022

MATH 574 Homework 11

Collaboration:

Problem 1 Let $n \in \mathbb{N}$. Prove that if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $ab \equiv cd \pmod{n}$.

Solution.

We have that $x \equiv y \pmod{n}$ if and only if $n|(x-y)$ for $n \in \mathbb{N}$, $x, y, \in \mathbb{Z}$.

Let $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{N}$. Assume that $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, so $n|(a-c)$ and $n|(b-d)$. By definition then, there must exist $k, m \in \mathbb{Z}$ such that $a - c = kn$ and $b - d = mn$. Rearranging, we have $a = mn + c$ and $b = kn + d$. Multiplying, we have

$$ab = (mn + c)(kn + d) = kmn^2 + dmn + ckn + cd.$$

Rearranging again, we must have $k, m \in \mathbb{Z}$ such that

$$ab - cd = kmn^2 + dmn + ckn = n(kmn + dm + ck).$$

Since $kmn + dm + ck$ is simply the product and sum of integers, it is an integer, so we can write $ab - cd$ as an integer multiple of n and thus $n|(ab - cd)$. So $ad \equiv cd \pmod{n}$ by definition. $\square$

Problem 2 Which elements of $\mathbb{Z}_{12}$ are invertible? For each element that is invertible, give its inverse.

Solution.

An element z of $\mathbb{Z}_{12}$ is invertible if and only if z and 12 are co-prime, meaning that $\gcd(z, 12) = 1$. This is the case for $z \in \{1, 5, 7, 11\}$.

- The inverse of 1 is 1: $(1)(1) = 1 \equiv 1 \pmod{12}$.
- The inverse of 5 is 5: $(5)(5) = 25 \equiv 1 \pmod{12}$.
- The inverse of 7 is 7: $(7)(7) = 49 \equiv 1 \pmod{12}$.
- The inverse of 11 is 11: $(11)(11) = 121 \equiv 1 \pmod{12}$.

Problem 3 Let $n \in \mathbb{N}$. Define a function $f : \mathbb{Z}_n \to \mathbb{Z}_n$ by $f([a]) = [a^2]$.
(a) Prove that, if $n = 1$ or $n = 2$, then f is bijective.
(b) Prove that for $n \geq 3$, f is not injective. (Hint: try to find two different elements $[a] \neq [b]$ such that $f([a]) = f([b])$.)

Solution.

(a) We have that $\mathbb{Z}_n = \left\{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\right\}$, and that $[k]_n = \{s : s \equiv k \pmod{n}\}$.

First, let $n = 1$. Then, we have $f : \mathbb{Z}_1 \to \mathbb{Z}_1$ where $\mathbb{Z}_1 = \{[0]_1\}$. Since $f([a]) = [a^2]$, we have

$$f = \left\{ \left([0]_1 , \left[0^2\right]_1 \right) \right\} = \left\{ \left([0]_1 , [0]_1 \right) \right\}.$$

It is easy to see that this is a bijection because $[0]_1$ is mapped to uniquely from $[0]_1$.

Next, let $n = 2$. Then, we have $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ where $\mathbb{Z}_2 = \{[0]_2, [1]_2\}$. Since $f([a]) = [a^2]$, we have

$$f = \left\{ \left([0]_2 , \left[0^2\right]_2 \right), \left([1]_2 , \left[1^2\right]_2 \right) \right\} = \left\{ \left([0]_2 , [0]_2 \right), \left([1]_2 , [1]_2 \right) \right\}.$$

This is also a bijection because $[0]_1$ is mapped to uniquely from $[0]_1$ and $[1]_2$ is mapped to uniquely from $[1]_2$. $\square$

(b) Now let $n \in \mathbb{N}$ such that $n \geq 3$. Then, we have $f\left([n-1]_n\right) = \left[(n-1)^2\right]_n$. We claim that

$$\left[(n-1)^2\right]_n = [1]_n.$$

To prove this, observe that

$$\begin{aligned}
&n|n(n-2) && (n-2 \text{ must be an integer})\\
\implies &n|n^2 - 2n\\
\implies &n|n^2 - 2n + 1 - 1\\
\implies &n|(n-1)^2 - 1\\
\implies &(n-1)^2 \equiv 1 \pmod{n} && (\text{by definition})\\
\implies &\left[(n-1)^2\right]_n = [1]_n. && (\text{both representatives of same class})
\end{aligned}$$

So $f\left([n-1]_n\right) = [1]_n$. We also have that $f([1]_n) = \left[1^2\right]_n = [1]_n$. But since $n > 2$, $[n-1]_n \neq [1]_n$. So f is not injective. $\square$

Problem 4 Suppose $m, n \in \mathbb{Z}$ are not both 0. Let $d = \gcd(m, n)$. Prove that $\gcd(\frac{m}{d}, \frac{n}{d}) = 1$.

Solution.

Without loss of generality, assume $m \neq 0$. If $n = 0$, then $d = \gcd(m, 0) = m$, and $\gcd\left(\frac{m}{m}, \frac{0}{m}\right) = \gcd(1, 0) = 1$.

Now, let $n \neq 0$, and assume that $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) > 1$. Then, there exists some $d' \in \mathbb{N}$ such that $d' | \frac{m}{d}$ and $d' | \frac{n}{d}$. Thus, there exist some $k_1, k_2 \in \mathbb{Z}$ such that $d'k_1 = \frac{m}{d}$ and $d'k_2 = \frac{n}{d}$, and consequently $d'dk_1 = m$ and $d'dk_2 = n$.

So we can write that $d'd|m$ and $d'd|n$, and thus $d'd$ is a common divisor of m and n. Since $d' > 1$, it follows that $d'd > d$. However, d is chosen to be the greatest common divisor of m and n, so this is a contradiction because there cannot be a common divisor larger than d. Thus we must have $d' = \gcd\left(\frac{m}{m}, \frac{0}{m}\right) \leq 1$. Since 1 divides any integer, $\gcd\left(\frac{m}{m}, \frac{0}{m}\right) = 1$. $\square$

Problem 5 Let $a, b \in \mathbb{Z}$ not both zero. Prove or disprove:
(a) If $\gcd(a, b) = 1$, then $\gcd(a^2, b^2) = 1$.
(b) If $\gcd(a, b) = 1$, then $\gcd(a, 2b) = 1$.

Solution.

(a) For $a, b \in \mathbb{N}$ such that $a \geq 2, b \geq 2$: From the fundamental theorem of arithmetic, we can write $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$ as the product of m primes p_i raised to powers α_i and $b = q_1^{\beta_1} q_2^{\beta_2} \dots q_n^{\beta_n}$ as the product of n primes q_i raised to powers β_i. Consequently, $a^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \dots p_m^{2\alpha_m}$ and $b^2 = q_1^{2\beta_1} q_2^{2\beta_2} \dots q_n^{2\beta_n}$.

Since $\gcd(a, b) = 1$, a and b have no factors greater than 1 in common and thus the sets $\{p_1, p_2, \dots, p_m\}$ and $\{q_1, q_2, \dots, q_n\}$ are disjoint (since all of these elements are greater than 1). Since a^2 and b^2 have the same set of factors and simply have powers doubled from a and b, a^2 and b^2 also have no prime factors in common. So $\gcd(a^2, b^2) = 1$.

If a or b are less than -1, we can use the prime factorization of $-a$ or $-b$ with the same reasoning. If $|a| \leq 1$ and $|b| \leq 1$ (with at least one nonzero), then the gcd must be 1 because a number cannot have a factor greater than the absolute value of itself. So in all cases, $\gcd(a, b) = 1 \implies \gcd(a^2, b^2) = 1$. $\square$

(b) This is false. For example, take $a = 2$ and $b = 1$. Then, we can write $\gcd(a, b) = \gcd(2, 1) = 1$, but $\gcd(a, 2b) = \gcd(2, 2) = 2 \neq 1$. $\square$

Problem 6 Let $n \in \mathbb{Z}$. Prove that $\gcd(n, n + 2) = 1$ if and only if n is odd.

Solution.

We first prove that if $\gcd(n, n + 2) = 1$ then n is odd. If n is even, then so is $n + 2$. So if $\gcd(n, n + 2)$ is 1, then n must be odd: if it were even, then $n + 2$ would be as well and the gcd would be at least 2 rather than 1.

We next prove that if n is odd, then $\gcd(n, n + 2) = 1$. Assume that $\gcd(n, n + 2) \neq 1$. Then, we have some $d \in \mathbb{N}, d \geq 2$ such that $d = \gcd(n, n + 2)$. So $d|n$ and $d|(n + 2)$, and by definition there exist $k_1, k_2 \in \mathbb{Z}$ such that $dk_1 = n$ and $dk_2 = n + 2$.

Substituting for n, we can then write $dk_1 = dk_2 - 2$ and subsequently $2 = d(k_2 - k_1)$. Since we assumed $d \geq 2$, we need $d = \frac{2}{k_2 - k_1} \geq 2$, which implies $1 \geq k_2 - k_1$. Since k_2 must be a larger integer than k_1 as dk_2 is larger than dk_1, we must have an equality with $k_2 - k_1 = 1$ or equivalently $k_2 = k_1 + 1$.

Substituting into our original equalities, we get $dk_1 = n$ and $dk_2 = d(k_1 + 1) = dk_1 + d = n + 2$. Thus, $dk_1 = dk_1 + d - 2$, which implies $d = 2$. Since d is the gcd of n and $n + 2$, we must have $2|n$ and thus n is even if $\gcd(n, n + 2) \neq 1$. Therefore, $\gcd(n, n + 2) = 1$ if and only if n is odd. $\square$

Problem 7 Let $a, b \in \mathbb{Z}$ not both zero. If $\gcd(a, b) = 1$ and $a \mid n$ and $b \mid n$, prove that $ab \mid n$.

Solution.

For $a, b, n \in \mathbb{N}$ such that $a \geq 2, b \geq 2, n \geq 2$: From the FTA, we can write $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ as the product of k primes p_i raised to powers α_i and $b = q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$ as the product of m primes q_i raised to powers β_i. Since $\gcd(a, b) = 1$, a and b have no factors greater than 1 in common and thus the sets $\{p_1, p_2, \dots, p_m\}$ and $\{q_1, q_2, \dots, q_n\}$ are disjoint (since all of these elements are greater than 1). We can use the FTA also write $n = r_1^{\gamma_1} r_2^{\gamma_2} \dots r_n^{\gamma_n}$ as the product of n primes r_i raised to powers γ_i.

Since $a|n$ and $b|n$, part of the prime factorization of n must include $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ and another part must include $b = q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}$. Since a and b are coprime, there is no overlap. Thus, we can write $n = j \left(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}\right) \left(q_1^{\beta_1} q_2^{\beta_2} \dots q_m^{\beta_m}\right) = jab$ for some $j \in \mathbb{Z}$. Thus, $ab|n$.

If a, b, or n are less than -1, we can use the prime factorization of $-a$, $-b$ or $-n$ with the same reasoning. If $|a| \leq 1$ and $|b| \leq 1$ (and not zero), then the statement must be true because of identity properties. So in all cases, $a|n, b|n \implies ab|n$. $\square$

Problem 8 Let $a, b \in \mathbb{N}$. Define the least common multiple $\operatorname{lcm}(a, b)$ as the smallest positive integer that is a multiple of both a and b. Prove that $ab = \operatorname{lcm}(a, b)$ if and only if $\gcd(a, b) = 1$.

Solution.

We first prove that $ab = \operatorname{lcm}(a, b) \implies \gcd(a, b) = 1$. Let $a, b \in \mathbb{N}$. Assume to the contrary that $\gcd(a, b) = d$ for some $d > 1$. So $d|a$ and $d|b$, and we can write $a = dk_1$ and $b = dk_2$ for some $k_1, k_2 \in \mathbb{Z}$. Thus, $d^2|ab$, because $ab = (dk_1)(dk_2) = d^2k_1k_2$. So $a|\frac{ab}{d}$ because we can write $\frac{ab}{d} = (dk_1)k_2 = ak_2$ and $b|\frac{ab}{d}$ because we can write $\frac{ab}{d} = k_1(dk_2) = k_1b$. So $\frac{ab}{d}$ is a multiple of a and b, and therefore ab cannot be the least common multiple since $d > 1$ and thus $\frac{ab}{d} < ab$. Therefore $ab = \operatorname{lcm}(a, b) \implies \gcd(a, b) = 1$.

We now prove that $\gcd(a, b) = 1 \implies ab = \operatorname{lcm}(a, b)$. Let $a, b \in \mathbb{N}$. Assume $\gcd(a, b) = 1$ and $\operatorname{lcm}(a, b) = m$ for some $m < ab$. So $a|m$ and $b|m$, and thus by the result from (7) $ab|m$. But since a positive number cannot have a factor greater than itself, we cannot have $m < ab$, a contradiction. Therefore $\gcd(a, b) = 1 \implies ab = \operatorname{lcm}(a, b)$.

So $\gcd(a, b) = 1$ if and only if $ab = \operatorname{lcm}(a, b)$. □