Selected Answers for Contemporary Abstract Algebra

Ian Shaw

August 22, 2020

These are write-ups for the questions left to the reader in Joseph A. Gallian's 8th edition of *Contemporary Abstract Algebra*. The questions were selected because they were the most interesting.

Contents

1 Chapter 0: Preliminaries

5. Show that if a and b are positive integers, then $ab = \mathbf{lcm}(a, b) \bullet \mathbf{gcd}(a, b)$.

Proof. By the Fundamental Theorem of Arithmetic (Theorem 0.3 in the book) that a is the product of primes, and by definition the greatest common divisor is a product of a subset of these primes

$$a = \text{gcd}(a, b) \prod_{i=1}^{n} p_{a,i}$$

Since by this definition

$$\{\emptyset\} = \{p_{a,i}\} \cap \{p_{b,i}\}$$

Thus

$$\text{lcm}(a, b) = \text{gcd}(a, b) \prod_{i=1}^{n} p_{a,i} \prod_{j=1}^{m} p_{b,j}$$

Therefore

$$\begin{aligned}
\text{lcm}(a, b)\text{gcd}(a, b) &= \text{gcd}(a, b)\text{gcd}(a, b) \prod_{i=1}^{n} p_{a,i} \prod_{j=1}^{m} p_{b,j} \\
&= \big(\text{gcd}(a, b) \prod_{i=1}^{n} p_{a,i}\big)\big(\text{gcd}(a, b) \prod_{j=1}^{m} p_{b,j}\big) \\
&= ab
\end{aligned}$$

□

7. If a and b are integers and n is a positive integer, prove that $a \bmod n = b \bmod n$ if and only if n divides $a - b$.

Proof. Forward: If $a \bmod n = b \bmod n$, then n divides $a - b$.

So we know that

$$\begin{aligned} m_a, m_b, r, &\in \mathbb{Z} \\ a &= m_a n + r \\ b &= m_b n + r \end{aligned}$$

Doing some artihmetic

$$a - b = (m_a - m_b)n \implies n|(a-b)$$

Backward: If n divides $a - b$, then $a \bmod n = b \bmod n$.

$$\begin{aligned} mn &= a - b \\ a &= mn + b \end{aligned}$$

We also know by the Division Algortihm

$$\begin{aligned} b &= m_b n + r \\ r &= b \bmod n \end{aligned}$$

Thus with substitution

$$\begin{aligned} a &= mn + m_b n + r \\ &= n * (m - m_b) + r \implies r = a \bmod n \end{aligned}$$

□

11. Let n and a be positive integers and let $d = \gcd(a, b)$. Show that the equation $ax \mod n = 1$ has a solution if and only if $d = 1$.

Proof. Forward: If the equation $ax \mod n = 1$ has a solution, then $d = 1$.

By Theorem 0.2 (p.4),

$$d = \gcd(a, b) \implies \exists s, t \in \mathbb{Z} \text{ s.t. } as + nt = d$$

.

Also, by definition

$$\begin{aligned} ax \mod n = 1 \implies \exists m_n \in \mathbb{Z} \text{ s.t. } ax &= nm_n + 1 \\ ax - nm_n &= 1 \end{aligned}$$

Further reading of Theorem 0.2 says that $\gcd(a, b)$ is the smallest possible integer of the form $as + nt = d$. Since 1 is the smallest possible integer,

$$1 = \gcd(a, b)$$

Backward: If $d = 1$, then the equation $ax \mod n = 1$ has a solution.

This is pretty straight forward

$$\begin{aligned} \gcd(a, b) = 1 \implies \exists s, t \in \mathbb{Z} \text{ s.t. } as + nt &= 1 \\ as &= n(-t) + 1 \\ as \mod n &= 1 \end{aligned}$$

□

12. Show that $5n + 3$ and $7n + 4$ are relatively prime for all n.

Proof. As shown in Exercise 11, if the equation $ax \mod n = 1$ has a solution, then $\gcd(a, b) = 1$. Specified to this situation: If $(7n + 4)x \mod (5n + 3) = 1$ has a solution, then $\gcd(7n + 4, 5n + 3) = 1$ and thus are relatively prime.

Consider the equation for unknown $p, x \in \mathbb{X}$

$$(5n + 3)p + 1 = (7n + 4)x$$

Well this can be solved with a $p = -7$ and $x = 5$. Therefore $(7n+4)x \mod (5n+3) = 1$ has a solution and $5n + 3$ and $7n + 4$ are relatively prime for all n. □

17. Let a, b, s and t be integers. If $a \mod st = b \mod st$, show that $a \mod s = b \mod s$ and $a \mod t = b \mod t$. What condition on s and t is needed to make the converse true?

Proof. Given that $a \mod st = b \mod st$, we know that $\exists r \in \mathbb{Z}$ for $p, q \in \mathbb{Z}$ such that

$$a = stp + r$$
$$b = stq + r$$

□

2 Notation

Throughout the paper, we will reference the notation listed in this section.

$$\mathbb{Z} = \text{integers} \tag{1}$$
$$\mathbb{Z}^+ = \text{positive integers} \tag{2}$$
$$\tag{3}$$