

CSCI 124 - Discrete Structures II - Fall 2010
George Washington University

Homework 1 Solutions

1 (10 points total; 5 points each) Show that, if $a, b, c \in \mathbb{Z}$ such that $a|b$ and $b|c$, then (i) $na|nc \forall n \in \mathbb{Z}$ and (ii) $a^k|c^k$ for every positive integer k .

Solution: Divisibility is transitive, as shown in class. That is, if $a|b$ and $b|c$, then $a|c$. Further, (i)

$$a|c \Rightarrow \exists m \in \mathbb{Z} \text{ s.t. } c = ma \Rightarrow nc = nma = m(na) \Rightarrow na|nc$$

(ii)

$$\begin{aligned} a|c &\Rightarrow \exists m \text{ s.t. } c = ma \\ &\Rightarrow c^k = m^k a^k = na^k \text{ for some integer } n \\ &\Rightarrow a^k|c^k \end{aligned}$$

2 (20 points) Show that, if $a, b, c, d \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then (i) $na \equiv nb \pmod{m} \forall n \in \mathbb{Z}$ (ii) $a^k \equiv b^k \pmod{m}$ for every positive integer k and (iii) $n(a - c)^k \equiv n(b - d)^k \pmod{m} \forall n \in \mathbb{Z}$ and for every positive integer k .

Solution:

(i) (6 points) Let $n \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$. Then

$$\begin{aligned} a \equiv b \pmod{m} &\Rightarrow \exists j \in \mathbb{Z} \text{ s.t. } b = a + jm \\ &\Rightarrow nb = n(a + jm) = na + njm \\ &\Rightarrow nb = na + m(\dots) \end{aligned}$$

where the term in the parenthesis is an integer. Hence $nb \equiv na \pmod{m}$.

Alternate solution. Use the fact proven in class that, if $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$. Use induction on the multiplier, n .

Basis: Given that $a \equiv b \pmod{m}$. Hence statement $na \equiv nb \pmod{m}$ true for $n = 1$.

Inductive step: Suppose true for $n = k$. Need show true for $n = k + 1$. That is, suppose $kb \equiv ka \pmod{m}$. Then, using the fact that, if $c = ka$ and $d = kb$,

$$ka + a \pmod{m} \equiv kb + b \pmod{m} \Rightarrow (k + 1)a \pmod{m} \equiv (k + 1)b \pmod{m}$$

(ii) (6 points)

$$\begin{aligned} a \equiv b \pmod{m} &\Rightarrow \exists n \in \mathbb{Z} \text{ s.t. } b = a + nm \\ &\Rightarrow b^k = (a + nm)^k = a^k + \sum_{i=1}^k {}^k C_i a^{k-i} (nm)^i \\ &\Rightarrow b^k = a^k + m(\dots) \end{aligned}$$

where the term in the parenthesis is an integer. Hence $b^k \equiv a^k \pmod{m}$.

Alternate solution. Use the fact proven in class that, if $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. Use induction on the power, k .

Basis: Given that $a \equiv b \pmod{m}$. Hence formula true for $k = 1$.

Inductive step: Suppose true for $k = n$. Need show true for $k = n + 1$. That is, suppose $b^k \equiv a^k \pmod{m}$. Then, using the fact that, if $c = a^k$ and $d = b^k$,

$$a^k \times a \pmod{m} \equiv b^k \times b \pmod{m} \Rightarrow a^{k+1} \pmod{m} \equiv b^{k+1} \pmod{m}$$

(iii) (8 points) Can show using $a = b + qm$ etc., but will get tedious. Full credit for correctly using this approach. Better approach (give one point extra credit):

Using the fact proven in class that, $c \equiv d \pmod{m}$ and $x \equiv y \pmod{m} \Rightarrow xc \equiv yd \pmod{m}$, using $x = y = -1$ gives $-c \equiv -d \pmod{m} \Rightarrow -c \equiv -d \pmod{m}$. Further using the fact shown in class that $u \equiv v \pmod{m}$ and $x \equiv y \pmod{m} \Rightarrow x + u \equiv v + y \pmod{m}$ gives us $a - c \equiv b - d \pmod{m}$. Using (ii) shown above, $(a - c)^k \equiv (b - d)^k \pmod{m}$. Finally, using (i) shown above: $n(a - c)^k \equiv n(b - d)^k \pmod{m}$.

3 (10 points) Suppose m, n are positive integers such that $m|n$ and $m \neq n$. Further, consider a fixed $c \in \mathbb{Z}$ such that $0 \leq c < m$. Suppose $y \in \mathbb{Z}$ such that $0 \leq y < n$ and $y \equiv c \pmod{m}$. What are *all* possible values of y ?

Solution: $m|n \Rightarrow \exists q \in \mathbb{Z} \text{ s.t. } n = qm$. m, n positive integers and $m \neq n \Rightarrow q > 1$.

$$y \equiv c \pmod{m} \Rightarrow y = c + q'm \text{ for some } q' \in \mathbb{Z}$$

$$0 \leq y \Rightarrow 0 \leq c + q'm \Rightarrow -c \leq q'm$$

As $c < m$,

$$\Rightarrow -m < -c \leq q'm \Rightarrow -m < q'm \Rightarrow -1 < q' \Rightarrow q' \geq 0$$

$$y < n \Rightarrow c + q'm < n \Rightarrow c + q'm < qm$$

$$\Rightarrow y = c, c + m, c + 2m, \dots, c + (q - 1)m$$

y can take on any of the above $q = \frac{n}{m}$ values.

4. (10 points) Consider the set $\mathcal{G} = \{0, 1, 2, \dots, m-1\}$. Let $c \in \mathbb{Z}$. Let \diamond be the operation $a \diamond b = a + b + c \pmod{m}$, defined for all $a, b \in \mathcal{G}$. Is (\mathcal{G}, \diamond) a group? Why or why not?

Solution: First, we have shown in class that the above is a group if $c = 0$. Hence we now examine the case when $c \neq 0$.

We check if (\mathcal{G}, \diamond) satisfies the four properties of a group.

1. Closure: Closure requires: $a, b \in G \Rightarrow a \diamond b \in G$.

As $a, b \in \mathbb{Z}_m$ and $a \diamond b$ also defined as being in \mathbb{Z}_m (which contains all the remainders possible on division by m), G is closed under the operation \diamond .

2. Associativity: Requires that $x \diamond (y \diamond z) = (x \diamond y) \diamond z$.

We check this:

$$\begin{aligned} LHS : & \quad x \diamond (y \diamond z) \\ = & \quad x \diamond ((y + z + c) \bmod m) \\ = & \quad (x + ((y + z + c) \bmod m) + c) \bmod m \\ = & \quad x + y + z + 2c \bmod m \end{aligned}$$

$$\begin{aligned} RHS : & \quad (x \diamond y) \diamond z \\ = & \quad ((x + y + c) \bmod m) \diamond z \\ = & \quad ((x + y + c) \bmod m) + z + c \bmod m \\ = & \quad x + y + z + 2c \bmod m \end{aligned}$$

Thus the operation is associative.

3. Identity: Requires $e \in G$ such that, $\forall x \in G, x \diamond e = e \diamond x = x$.

As $c \neq 0$, $e = m - c$ satisfies the above, is the identity and belongs to G . Hence the identity exists in G .

4. Inverse: Requires that, $\forall x \in G \exists \bar{x} \in G$ such that $x \diamond \bar{x} = \bar{x} \diamond x = e$.

We need to find \bar{x} such that $x + \bar{x} + c \bmod m = m - c \bmod m$. Let $c' = c \bmod m$. We see that $\bar{x} = m - 2c' - x$ if $x \leq m - 2c'$; $\bar{x} = 2(m - c') - x$ if $2(m - c') \geq x > m - 2c'$ and $\bar{x} = 3m - 2c' - x$ if $x > 2(m - c')$.

Thus (G, \diamond) satisfies all four properties of a group, and is a group.

5. (15 points) Let $\mathcal{R} = \mathbb{R}^+$, the set of positive real numbers. Let \oplus be an operation on \mathcal{R} , defined by $a \oplus b = ab$ for all $a, b \in \mathcal{R}$. Let $a \odot b = a^{\log_2 b}$. Is $(\mathcal{R}, \oplus, \odot)$ a ring? Why or why not?

Solution: We check if $(\mathcal{R}, \oplus, \odot)$ has all the properties of a ring.

1. We first check if (\mathcal{R}, \oplus) satisfies the four properties of a group.

- (a) Closure: Closure requires: $a, b \in \mathcal{R} \Rightarrow a \oplus b \in \mathcal{R}$.

$a, b \in \mathbb{R}^+ \Rightarrow ab \in \mathbb{R}^+$ (product of two positive real numbers is also a positive real number). Hence \mathcal{R} is closed under the operation \oplus .

(b) Associativity: Requires that $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.

We check this:

$$\begin{aligned} LHS : & a \oplus (b \oplus c) \\ &= a \oplus bc \\ &= abc \end{aligned}$$

$$\begin{aligned} RHS : & (a \oplus b) \oplus c \\ &= ab \oplus c \\ &= abc \end{aligned}$$

Thus the operation \oplus is associative.

(c) Identity: Requires $e \in \mathcal{R}$ such that, $\forall x \in \mathcal{R}$, $x \oplus e = e \oplus x = x$.

$e = 1$ satisfies the above, and is the identity. Hence the identity with respect to operation \oplus exists in \mathcal{R} .

(d) Inverse: Requires that, $\forall x \in \mathcal{R} \exists \bar{x} \in \mathcal{R}$ such that $x \oplus \bar{x} = \bar{x} \oplus x = e$.

True if $\bar{x} = \frac{1}{x}$. The inverse of a positive real number is also a positive real number. Thus all elements in \mathcal{R} have inverses, with respect to operation \oplus , in \mathcal{R} .

Thus (\mathcal{R}, \oplus) satisfies all four properties of a group, and is a group.

2. The operation \oplus is commutative. That is $a \oplus b = ab = ba = b \oplus a$.
3. We check if \mathcal{R} is closed with respect to \odot . Suppose $a, b \in \mathcal{R}$. Then $a \odot b = a^{\log_2 b}$ which is a positive real number. Hence \mathcal{R} is closed with respect to \odot .
4. We check if \odot is associative. That is, is: $a \odot (b \odot c) = (a \odot b) \odot c$. To do so, we first observe the following:

$$x \odot y = x^{\log_2 y} = (2^{\log_2 x})^{\log_2 y} = 2^{\log_2 x \times \log_2 y}$$

and hence that \odot is commutative. Now to see if $a \odot (b \odot c) = (a \odot b) \odot c$.

$$\begin{aligned} LHS : & a \odot (b \odot c) \\ &= a \odot b^{\log_2 c} \\ &= a \odot 2^{\log_2 b \times \log_2 c} \\ &= a^{\log_2 b \times \log_2 c} \\ &= 2^{\log_2 a \times \log_2 b \times \log_2 c} \end{aligned}$$

$$\begin{aligned} RHS : & (a \odot b) \odot c \\ &= 2^{\log_2 a \times \log_2 b} \odot c \\ &= 2^{\log_2 a \times \log_2 b \times \log_2 c} \end{aligned}$$

Thus \odot is associative

5. Finally, we check if \odot is distributive over \oplus . That is, we check if

$$(a) \quad a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

$$\begin{aligned} LHS: \quad & a \odot (b \oplus c) \\ &= a \odot bc \\ &= a^{\log_2(bc)} \\ &= a^{\log_2 b + \log_2 c} \\ &= 2^{\log_2 a (\log_2 b + \log_2 c)} \end{aligned}$$

$$\begin{aligned} RHS: \quad & (a \odot b) \oplus (a \odot c) \\ &= 2^{\log_2 a \log_2 b} \times 2^{\log_2 a \log_2 c} \\ &= 2^{\log_2 a \log_2 b + \log_2 a \log_2 c} \\ &= 2^{\log_2 a (\log_2 b + \log_2 c)} \\ &= LHS \end{aligned}$$

$$(b) \quad \text{Check if } (a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$$

$$\begin{aligned} LHS: \quad & (a \oplus b) \odot c \\ &= (ab)^{\log_2 c} \\ &= (2^{\log_2 ab})^{\log_2 c} \\ &= 2^{(\log_2 a + \log_2 b) \log_2 c} \end{aligned}$$

$$\begin{aligned} RHS: \quad & (a \odot c) \oplus (b \odot c) \\ &= a^{\log_2 c} \times b^{\log_2 c} \\ &= 2^{\log_2 a \log_2 c} \times 2^{\log_2 b \log_2 c} \\ &= 2^{\log_2 a \log_2 c + \log_2 b \log_2 c} \\ &= 2^{(\log_2 a + \log_2 b) \log_2 c} \\ &= LHS \end{aligned}$$

1-5 demonstrate that $(\mathcal{R}, \oplus, \odot)$ has all the properties of a ring, and is a ring.

6. (10 points) Show that, if a is an odd integer, $a^2 \equiv 1 \pmod{8}$.

Solution: a is odd. Hence, $\exists q \in \mathbb{Z}$ such that $a = 2q + 1$.

$$a^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1$$

If q is even, then $\exists m \in \mathbb{Z}$ such that $q = 2m$. Then:

$$a^2 = 4q(q + 1) + 1 = 8m(m + 1) + 1 \equiv 1 \pmod{8}$$

Because $m(m + 1) \in \mathbb{Z}$ (as \mathbb{Z} is closed wrt addition and multiplication) implies that $8 \mid (a^2 - 1)$.

If q is odd, $\exists m \in \mathbb{Z}$ such that $q = 2m + 1$. Then:

$$a^2 = 4q(q + 1) + 1 = 4(2m + 1)(2m + 2) + 1 = 8(2m + 1)(m + 1) + 1 \equiv 1 \pmod{8}$$

Because $(2m + 1)(m + 1) \in \mathbb{Z}$ (as \mathbb{Z} is closed wrt addition and multiplication) implies that $8|(a^2 - 1)$.

7. (15 points) Use mathematical induction and results shown in class to prove that, if $a_1, a_2, \dots, a_n \in \mathbb{Z}$, $b_1, b_2, \dots, b_n \in \mathbb{Z}$ and m a positive integer, and, further, that $a_i \equiv b_i \pmod{m} \forall i$,

(a) $\sum_{i=1}^n a_i \equiv \sum_{i=1}^n b_i \pmod{m}$

Solution: We will show the above by induction.

Base Case: It is given that $a_1 \equiv b_1 \pmod{m}$. Hence the above is true for $n = 1$.

Inductive step: Suppose the above is true for $n = k$. We will show that it is true for $n = k + 1$.

Proof: Suppose that

$$\sum_{i=1}^k a_i \equiv \sum_{i=1}^k b_i \pmod{m}$$

Denote $a = \sum_{i=1}^k a_i$, $b = \sum_{i=1}^k b_i$, $c = a_{k+1}$ and $d = b_{k+1}$. Then, by the inductive hypothesis, $a \equiv b \pmod{m}$ and we are given that $c \equiv d \pmod{m}$. We showed in class that this implies that $a + c \equiv b + d \pmod{m}$. That is,

$$\sum_{i=1}^k a_i + a_{k+1} \equiv \sum_{i=1}^k b_i + b_{k+1} \pmod{m} \Rightarrow \sum_{i=1}^{k+1} a_i \equiv \sum_{i=1}^{k+1} b_i \pmod{m}$$

Thus we have shown the result by mathematical induction.

(b) $\prod_{i=1}^n a_i \equiv \prod_{i=1}^n b_i \pmod{m}$

Solution: We will show the above by induction.

Base Case: It is given that $a_1 \equiv b_1 \pmod{m}$. Hence the above is true for $n = 1$.

Inductive step: Suppose the above is true for $n = k$. We will show that it is true for $n = k + 1$.

Proof: Suppose that

$$\prod_{i=1}^k a_i \equiv \prod_{i=1}^k b_i \pmod{m}$$

Denote $a = \prod_{i=1}^k a_i$, $b = \prod_{i=1}^k b_i$, $c = a_{k+1}$ and $d = b_{k+1}$. Then, by the inductive hypothesis, $a \equiv b \pmod{m}$ and we are given that $c \equiv d \pmod{m}$. We showed in class that this implies that $ac \equiv bd \pmod{m}$. That is,

$$\left(\prod_{i=1}^k a_i\right)a_{k+1} \equiv \left(\prod_{i=1}^k b_i\right)b_{k+1} \pmod{m} \Rightarrow \prod_{i=1}^{k+1} a_i \equiv \prod_{i=1}^{k+1} b_i \pmod{m}$$

Thus we have shown the result by mathematical induction.

8 (12 points). Show the following formally:

a. The sum of an even integer and an odd integer is odd.

Solution: Let x be an even integer and y an odd integer. Then $\exists q_x, q_y \in \mathbb{Z}$ such that $x = 2q_x$ and $y = 2q_y + 1$.

$$x + y = 2q_x + 2q_y + 1 = 2(q_x + q_y) + 1$$

Let $m = q_x + q_y$. Then $m \in \mathbb{Z}$ because \mathbb{Z} is closed wrt addition. Hence $x + y = 2m + 1$ is odd.

b. The product of an even integer and an odd integer is even.

Solution: Let x be an even integer and y an odd integer. Then $\exists q_x, q_y \in \mathbb{Z}$ such that $x = 2q_x$ and $y = 2q_y + 1$.

$$xy = (2q_x)(2q_y + 1) = 2(q_x)(2q_y + 1)$$

Let $m = (q_x)(2q_y + 1)$. Then $m \in \mathbb{Z}$ because \mathbb{Z} is closed wrt addition and multiplication. Hence $xy = 2m$ is even.

c. The square of an integer is odd if and only if it is odd.

Solution: Let $x \in \mathbb{Z}$. Need to show that

$$x^2 \text{ is odd} \Leftrightarrow x \text{ is odd}$$

First we will show that:

$$x^2 \text{ is odd} \Rightarrow x \text{ is odd}$$

Proof. We will show this by showing that x is even is not possible. Suppose x is even. Then $x = 2q$ for some $q \in \mathbb{Z}$. $x^2 = 4q^2 = 2(2q^2)$ is also even because $q^2 \in \mathbb{Z}$. Thus, if x is even, so is x^2 , hence x must be odd.

Next we will show that

$$x \text{ is odd} \Rightarrow x^2 \text{ is odd}$$

Proof. Suppose x is odd. $\exists q \in \mathbb{Z}$ such that $x = 2q + 1$. Then $x^2 = 4q^2 + 2q + 1 = 2(2q^2 + q) + 1$. Because \mathbb{Z} is closed wrt addition and multiplication, $2q^2 + q \in \mathbb{Z}$ and x^2 is odd.

Thus x^2 is odd if and only if x is odd.