Math 31 - Homework 1 Solutions

1. Find $\gcd(a,b)$ and express $\gcd(a,b)$ as $ma+nb$ for:

(a) $(116,-84)$

Solution. Use the Euclidean algorithm:

$$\begin{aligned}
116 &= (-1)(-84) + 32\\
-84 &= (-3)(32) + 12\\
32 &= (2)(12) + 8\\
12 &= (1)(8) + 4\\
8 &= (2)(4) + 0,
\end{aligned}$$

so $\gcd(116,-84) = 4$. To compute the coefficients m and n, we work in reverse, solving for the remainder at each step:

$$\begin{aligned}
4 &= 12 - 8\\
&= 12 - (32 - 2\cdot 12) = (3)(12) - 32\\
&= 3(-84 + (3)(32)) - 32 = (3)(-84) + (8)(32)\\
&= (3)(-84) + 8(116 - 84) = (11)(-84) + 8(116)\\
&= 11(-84) + 8(116),
\end{aligned}$$

so the coefficients are 11 and 8.

(b) $(85,65)$

Solution. Again, use the Euclidean algorithm.

$$\begin{aligned}
85 &= (1)(65) + 20\\
65 &= (3)(20) + 5\\
20 &= (4)(5) + 0,
\end{aligned}$$

so $\gcd(85,65) = 5$. To find the coefficients,

$$\begin{aligned}
5 &= 65 - (3)(20)\\
&= 65 - 3(85 - 65)\\
&= (4)(65) - (3)(85)\\
&= 4(65) + (-3)(85),
\end{aligned}$$

so the coefficients are 4 and -3.

(c) $(72,26)$

Solution. Euclidean algorithm:

$$\begin{aligned} 72 &= (2)(26) + 20 \\ 26 &= (1)(20) + 6 \\ 20 &= (3)(6) + 2 \\ 6 &= (3)(2) + 0, \end{aligned}$$

so $\gcd(72, 26) = 2$. For the coefficients:

$$\begin{aligned} 2 &= 20 - (3)(6) \\ &= 20 - 3(26 - 20) = (4)(20) - (3)(26) \\ &= 4(72 - 2(26)) - 3(26) = 4(72) - 11(26) \\ &= 4(72) + (-11)(26), \end{aligned}$$

so the coefficients are 4 and -11.

(d) $(72, 25)$

Solution. Euclidean algorithm:

$$\begin{aligned} 72 &= (2)(25) + 22 \\ 25 &= (1)(22) + 3 \\ 22 &= (7)(3) + 1 \\ 3 &= (3)(1) + 0, \end{aligned}$$

so $\gcd(72, 25) = 1$. As for the coefficients,

$$\begin{aligned} 1 &= 22 - (7)(3) \\ &= 22 - 7(25 - 22) = (8)(22) - (7)(25) \\ &= 8(72 - (2)(25)) - 7(25) = 8(72) - 23(25) \\ &= 8(72) + (-23)(25), \end{aligned}$$

so the coefficients are 8 and -23.

2. Verify that the following elements of $\langle \mathbb{Z}_n, \cdot \rangle$ are invertible, and find their multiplicative inverses.

(a) 4 in $\mathbb{Z}_{15}$

Solution. To verify that 4 is invertible, we need to check that $\gcd(15, 4) = 1$. We'll use the Euclidean algorithm:

$$\begin{aligned} 15 &= (3)(4) + 3 \\ 4 &= (1)(3) + 1 \\ 3 &= (3)(1) + 0, \end{aligned}$$

so 4 is indeed invertible in $\mathbb{Z}_{15}$. To compute the inverse, we need to write $\gcd(15, 4)$ as a linear combination of 15 and 4:

$$\begin{aligned}1 &= 4 - 3\\ &= 4 - (15 - (3)(4)) = (4)(4) - 15\\ &= (4)(4) + (-1)(15).\end{aligned}$$

Therefore, $1 = 4(4) + (-1)(15)$, so the inverse of 4 in $\mathbb{Z}_{15}$ is 4.

(b) 14 in $\mathbb{Z}_{19}$

Solution. Again, we need to check that $\gcd(19, 14) = 1$:

$$\begin{aligned}19 &= (1)(14) + 5\\ 14 &= (2)(5) + 4\\ 5 &= (1)(4) + 1\\ 4 &= (4)(1) + 0,\end{aligned}$$

so 14 is invertible. Let's find the inverse:

$$\begin{aligned}1 &= 5 - 4\\ &= 5 - (14 - (2)(5)) = (3)(5) - 14\\ &= 3(19 - 14) - 14 = (3)(19) - (4)(14)\\ &= (3)(19) + (-4)(14).\end{aligned}$$

The coefficient of 14 is -4, which doesn't lie in $\mathbb{Z}_{19}$. However,

$$-4 \equiv 15 \bmod 19,$$

so 15 is the inverse of 14 in $\mathbb{Z}_{19}$.

3. In each case, determine whether $*$ defines a binary operation on the given set. If not, give reason(s) why $*$ fails to be a binary operation.

(a) $*$ defined on $\mathbb{Z}^+$ by $a * b = a - b$.

(b) $*$ defined on $\mathbb{Z}^+$ by $a * b = a^b$.

(c) $*$ defined on $\mathbb{Z}$ by $a * b = a/b$.

(d) $*$ defined on $\mathbb{R}$ by $a * b = c$, where c is at least 5 more than $a + b$.

Solution. (a) No. The reason is that $\mathbb{Z}^+$ is not closed under $*$. For example, notice that

$$2 * 3 = 2 - 3 = -1,$$

which is not in $\mathbb{Z}^+$.

(b) Yes. This $*$ gives a binary operation on $\mathbb{Z}^+$, since it is both well-defined and $\mathbb{Z}^+$ is closed under $*$.

(c) No. Given $a, b \in \mathbb{Z}$, we do not necessarily have $a/b \in \mathbb{Z}$. For example, if we take $a = 1$ and $b = 2$, then $a/b = 1/2$ is not an integer.

(d) No. This is not a binary operation since it is not well-defined. The definition of $a * b$ is ambiguous at best.

4. Determine whether the binary operation $*$ is associative, and state whether it is commutative or not.

(a) $*$ defined on $\mathbb{Z}$ by $a * b = a - b$.

(b) $*$ defined on $\mathbb{Q}$ by $a * b = ab + 1$.

(c) $*$ defined on $\mathbb{Z}^+$ by $a * b = a^b$.

Solution. (a) Subtraction on $\mathbb{Z}$ is not associative. For example, we have

$$(1 - 2) - 3 = -1 - 3 = -4,$$

while on the other hand,

$$1 - (2 - 3) = 1 - (-1) = 2.$$

It is not commutative either.

(b) This operation is not associative. If $a, b, c \in \mathbb{Q}$, then

$$(a * b) * c = (ab + 1) * c = abc + c + 1,$$

while

$$a * (b * c) = a * (bc + 1) = abc + a + 1,$$

and these two are not equal in general. (For example, take $a = 1$, $b = 1$, and $c = 2$.) It is commutative, however, since multiplication of rational numbers is commutative.

(c) This operation is not associative. If $a, b, c \in \mathbb{Z}^+$, then

$$(a * b) * c = (a^b) * c = (a^b)^c = a^{bc},$$

while

$$a * (b * c) = a * (b^c) = a^{b^c},$$

and these are not equal in general. For example, take $a = 2$, $b = 1$, and $c = 2$. Then

$$2^{1 \cdot 2} = 4,$$

but

$$2^{1^2} = 2^1 = 2.$$

The operation is not commutative, either, since we have

$$3 * 2 = 3^2 = 9$$

and

$$2 * 3 = 2^3 = 8,$$

for example.

5. [Saracino, Section 1, #1.9] If S is a finite set, then we can define a binary operation on S by writing down all the values of $s_1 * s_2$ in a table. For instance, if $S = \{a, b, c, d\}$, then the following gives a binary operation on S.

$*$	a	b	c	d
a	a	c	b	d
b	c	a	d	b
c	b	d	a	c
d	d	b	c	a

Here, for $s_1, s_2 \in S$, $s_1 * s_2$ is the element in row s_1 and column s_2. For example, $c * b = d$. Is the above binary operation commutative? Is it associative? (**Note:** The sort of table described in this problem is sometimes called a **Cayley table** or **group table**.)

Solution. The operation is commutative. An easy way to see this is to observe that the table is symmetric about the diagonal. You could also go through and check that $x * y = y * x$ for any $x, y \in S$. However, it is not associative. Observe that

$$(a * b) * c = c * c = a,$$

while

$$a * (b * c) = a * d = d.$$

6. Compute the Cayley table for $\langle \mathbb{Z}_6, +_6 \rangle$.

Solution. We just need to go through and compute all possible sums of elements in $\mathbb{Z}_6$. We obtain:

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Medium

7. Suppose that $*$ is an associative and commutative binary operation on a set S. Show that the subset

$$H = \{a \in S : a * a = a\}$$

of S is closed under $*$. (The elements of H are called **idempotents** for $*$.)

Proof. To show that H is closed, we need to verify that if $a, b \in H$, then $a * b \in H$. That is, we need to show that $a * b$ is an idempotent, i.e., that

$$(a * b) * (a * b) = a * b.$$

Since $*$ is associative, we can write

$$(a * b) * (a * b) = ((a * b) * a) * b. \tag{1}$$

Using associativity again, we get

$$(a * b) * a = a * (b * a).$$

Now using the fact that $*$ is commutative, we have

$$a * (b * a) = a * (a * b) = (a * a) * b = a * b,$$

again using associativity and the fact that $a * a = a$. Thus we have shown that

$$(a * b) * a = a * b.$$

Plugging this into (1), we get

$$(a * b) * (a * b) = (a * b) * b = a * (b * b) = a * b,$$

since $b * b = b$, so $a * b \in H$. Thus H is closed under $*$. $\square$