MATH 411: INTRODUCTION TO ABSTRACT ALGEBRA HOMEWORK #2

TRUNG DANG
33858723

Problem 1:
(a) Compute $\gcd(163, 1001)$ and express it as a linear combination of 163 and 1001 with integer coefficients.
(b) Compute $\gcd(629, 2023)$ and express it as a linear combination of 629 and 2023 with integer coefficients.

Solution. We write the transformations in accordance with the Euclidean algorithm.
(a)

$$\begin{aligned}
1001 &= 163 \times 6 + 23 \\
163 &= 23 \times 7 + 2 \\
23 &= 2 \times 11 + 1 \\
2 &= 1 \times 2.
\end{aligned}$$

So $\boxed{\gcd(163, 1001) = 1}$. Express the algorithm recursively, we have:

$$\begin{aligned}
1 &= 23 - 2 \times 11 \\
&= 23 - (163 - 23 \times 7) \times 11 \\
&= 23 \times 78 - 163 \times 11 \\
&= (1001 - 163 \times 6) \times 78 - 163 \times 11 \\
&= 1001 \times 78 - 163 \times 479
\end{aligned}$$

(b)

$$\begin{aligned}
2023 &= 629 \times 3 + 136 \\
629 &= 136 \times 4 + 85 \\
136 &= 85 \times 1 + 51 \\
85 &= 51 \times 1 + 34 \\
51 &= 34 \times 1 + 17 \\
34 &= 17 \times 2.
\end{aligned}$$

Therefore $\boxed{\gcd(629, 2023) = 17}$. Express the algorithm recursively, we have:

$$\begin{aligned}
17 &= 51 - 34 \\
&= 51 - (85 - 51) = 51 \times 2 - 85 \\
&= (136 - 85) \times 2 - 85 = 136 \times 2 - 85 \times 3 \\
&= 136 \times 2 - (629 - 136 \times 4) \times 3 = 136 \times 14 - 629 \times 3 \\
&= (2023 - 629 \times 3) \times 14 - 629 \times 3 \\
&= 2023 \times 14 - 629 \times 45
\end{aligned}$$

■

Problem 2: Are the following statements about integers true or false? If true, prove it. If false, provide a counterexample.
(a) If $r \mid ab$, then $r \mid a$ or $r \mid b$.
(b) If $a \mid b$ and $b \mid c$ then $a \mid c$.
(c) 314159265358979 is prime.
(d) If $a \mid b$ and $b \mid a$ then $a = \pm b$
(e) Any two consecutive Fibonacci numbers (for example, 8 and 13) are coprime.

Solution. (a) This statement is wrong. For example, let $r = 6, a = 2, b = 3$. Then $6|2(3) = 6$, but $6 \nmid 2$ and $6 \nmid 3$.

(b) If $a \mid b$, then we can write $b = ka$, for some $k \in \mathbb{Z}$.
If $b \mid c$, then we can write $c = qb$, for some $q \in \mathbb{Z}$. From the two conditions, we can write $c = qb = (qk) \cdot a$, with $qk \in \mathbb{Z}$. Therefore, $a \mid c$.

(c) Since $314159265358979 = 43 \times 7306029426953$, it is not a prime.

(d) Because $a \mid b$, we can write $b = ka$, for some integer k, and since $b \mid a$, we can also write $a = qb$, for some integer q.
This means $a = qb = qka$, thus $qk = 1$. Because q, k are both integers, either $q = k = 1$ or $q = k = -1$. This yields either $a = b$ or $a = -b$

(e) We will prove that this statement is correct. Assume the contrary, let F_n, F_{n+1} be the first two consecutive Fibonacci numbers where $\gcd(F_n, F_{n+1}) = d > 1$.
Then consider $F_{n-1} = F_{n+1} - Fn$. Because $d \mid F_n$ and $d \mid F_{n+1}$, d must also divides F_{n-1}. But that means $d \mid \gcd(F_n, Fn - 1)$, so $\gcd(F_n, F_{n-1}) > 1$, contradicting with the assumption that the F_n, F_{n+1} are the first elements of the sequence with the property above.
Therefore, the assumption is incorrect, and the statement is proven. ■

Problem 3: Prove that $a \equiv b \mod n$ is an equivalence relation (check all axioms).

Solution. We prove the statement by checking all three axioms of an equivalence relation: *reflexivity, symmetry, transitivity.*
Reflexivity: For all $a, n \in \mathbb{Z}$, $a - a = 0 = 0 \cdot n$, so $n \mid a - a$ or $a \equiv a \mod n$.
Symmetry: $a \equiv b \mod n \iff a - b = kn, \iff b - a = -kn \iff b \equiv a \mod n$ (where $k \in \mathbb{Z}$)
Transitivity: $a \equiv b \mod n$ and $b \equiv c \mod n \Longleftarrow n \mid a - b$ and $n \mid b - c$. Thus $n \mid (a - b) + (b - c)$, or$n \mid a - c$. So $a \equiv c \mod n$

Since we have fully checked the 3 axioms of equivalence relation, the proof is completed. ■

Problem 4: Compute multiplication tables of (a) $\mathbb{Z}_6^*$; (b) $\mathbb{Z}_7^*$; (c) $\mathbb{Z}_8^*$.

Solution. (a) The multiplication table of $\mathbb{Z}_6^*$ is as follows:

	1	5
1	1	5
5	5	1

(b) The multiplication table of $\mathbb{Z}_7^*$ is as follows:

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

(c) The multiplication table of $\mathbb{Z}_8^*$ is as follows: ∎

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Problem 5: Prove that the groups $\mathbb{Z}_7^*$ and $\mathbb{Z}_6$ are isomorphic by constructing an explicit isomorphism $f : \mathbb{Z}_6 \to \mathbb{Z}_7^*$ between them and rearranging multiplication tables of these groups to show that the binary operations are isomorphic

Solution. We define the bijection

$$\begin{aligned} f : \mathbb{Z}_6 &\to \mathbb{Z}_7^* \\ 0 &\mapsto 1 \\ 1 &\mapsto 5 \\ 2 &\mapsto 4 \\ 3 &\mapsto 6 \\ 4 &\mapsto 2 \\ 5 &\mapsto 3 \end{aligned}$$

Then, rearranging the multiplication table of 6 in the order of [0, 4, 5, 2, 1, 3] yields:

	0	4	5	2	1	3
0	0	4	5	2	1	3
4	4	2	3	0	5	1
5	5	3	4	1	0	2
2	2	0	1	4	3	5
1	1	5	0	3	2	4
3	3	1	2	5	4	0

Comparing with $\mathbb{Z}_7^*$ multiplication table, the proof is complete: ∎

0	4	5	2	1	3
4	2	3	0	5	1
5	3	4	1	0	2
2	0	1	4	3	5
1	5	0	3	2	4
3	1	2	5	4	0

1	2	3	4	5	6
2	4	6	1	3	5
3	6	2	5	1	4
4	1	5	2	6	3
5	3	1	6	4	2
6	5	4	3	2	1

Problem 6: Prove that the groups $\mathbb{Z}_8^*$ and $\mathbb{Z}_4$ are not isomorphic.

Solution. The multiplication tables for $\mathbb{Z}_8^*$ and $\mathbb{Z}_4$ are, respectively, as follows:

1	3	5	7
3	1	7	5
5	7	1	3
7	5	3	1

0	1	2	3
1	2	3	0
2	3	0	1
3	0	1	2

Assume the contrary, that $\mathbb{Z}_8^*$ and $\mathbb{Z}_4$ are isomorphic. Then there exists a bijection $f : \mathbb{Z}_8^* \to \mathbb{Z}_4$ such that $f(a \cdot b) = f(a) + f(b) \forall a, b \in \mathbb{Z}_8^*$.

Let $b = 1$, then $f(a\dot{1}) = f(a) + f(1), \forall a \in \mathbb{Z}_8^*$, so $f(1) = 0$.

Let $b = a^{-1}$. Then $f(a\dot{a}^{-1}) = f(1) = 0$, $\forall a \in \mathbb{Z}_8^*$. Thus, function f maps identity to identity, and inverses to inverses.

Also, we can easily verify that $\forall a \in \mathbb{Z}_8^*, a = a^{-1}$. In fact:

$$\begin{aligned} 1 \cdot 1 &\equiv 1 \mod 8 \\ 3 \cdot 3 &\equiv 1 \mod 8 \\ 5 \cdot 5 &\equiv 1 \mod 8 \\ 7 \cdot 7 &\equiv 1 \mod 8 \end{aligned}$$

Therefore, $f(a)^{-1} = f(a^{-1}) = f(a), \forall a \in \mathbb{Z}_8^*$. However, let b be an element in the domain such that $f(b) = 3$, then $f(b)^{-1} = 1 \neq f(b)$, a contradiction. Therefore, the assumption is false, and the proof is completed. ■

Problem 7: Prove that every symmetric (a) 2×2; (b) 3×3 Latin square is a multiplication table of some abelian group.

Solution. Remarks: all addition operations in the solutions are in the corresponding modulo.
(a) Because of symmetry, we assume that the symmetric 2×2 Latin square is of the form:

a	b
b	a

But then there exists an isomorphism between this table and the multiplication table of $(\mathbb{Z}_2, +)$:

0	1
1	0

by the bijection:

$$\begin{aligned} f : \mathbb{Z}_2 &\to G \\ 0 &\mapsto a \\ 1 &\mapsto b \end{aligned}$$

Therefore, since $(\mathbb{Z}_2, +)$ is an Abelian group, the Latin square is also a multiplication table of some Abelian group (as proven in homework 1)

(b) Because of the symmetry, we may assume that the first row of the Latin square contains a, b, c, and the first column of the Latin square must also contains a, b, c

a	b	c
b	$\star$	
c	$\circ$	

Then the $\star$ square cannot contain b. If the $\star$ square contains a, then the $\circ$ square contains c, which violates the definition of the Latin square. Therefore, $\star = c$, and $\circ = a$. Filling the rest of the square, we obtain the only form of the square being:

a	b	c
b	c	a
c	a	b

Consider group $(\mathbb{Z}_3, +)$: Let $(G, \circ)$ be a set $G = \{a, b, c\}$ and binary operation $\circ$ defined by the multiplication matrix above. Since there exists a isomorphism between $(\mathbb{Z}_3, +)$ and $(G, \circ)$, where:

$$\begin{aligned} f : \mathbb{Z}_3 &\to G \\ 0 &\mapsto a \\ 1 &\mapsto b \\ 2 &\mapsto c \end{aligned}$$

0	1	2
1	2	0
2	0	1

$\mapsto$

a	b	c
b	c	a
c	a	b

,$(G, \circ)$ is also an Abelian group (proven in Homework 1).

■

Problem 8: Find an example of a Latin square that is not a multiplication table of any group (with proof)

Solution. For brevity, in this example, we will represent rows by row matrices and columns by column matrices. For instance,

0
1
2
3

0	1	2	3

will be represented by $c = \begin{bmatrix} 0 \\ 1 \\ 2 \\ 3 \end{bmatrix}$ and $r = \begin{bmatrix} 0 & 1 & 2 & 3 \end{bmatrix}$, respectively. We now consider the following Latin square:

1	2	3	0
0	1	2	3
2	3	0	1
3	0	1	2

Assume this Latin square is a multiplication table of a group G. Let e be the identity element of this group.

Then, since $e \cdot e = e$, e must lie on the diagonal of the square. Denote r_e, c_e be the row and columns of e respectively, it is also clear that $r_e = c_e^T$. Therefore, we consider the following cases:

- $e = 1$, then either $r_e = \begin{bmatrix} 1 & 2 & 3 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 & 2 & 3 \end{bmatrix} = c_e^T$ or $r_e = \begin{bmatrix} 0 & 1 & 2 & 3 \end{bmatrix} \neq \begin{bmatrix} 2 & 1 & 3 & 0 \end{bmatrix} = c_e^T$
- $e = 0$, then $r_e = \begin{bmatrix} 2 & 3 & 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 3 & 2 & 0 & 1 \end{bmatrix} = c_e^T$
- $e = 2$, then $r_e = \begin{bmatrix} 3 & 0 & 1 & 2 \end{bmatrix} \neq \begin{bmatrix} 0 & 3 & 1 & 2 \end{bmatrix} = c_e^T$

Therefore, in all cases, the identity e of G cannot exist. So the assumption is false, and this Latin square is not a multiplication of any group G. ■

Problem 9: Prove that there is no group G of integers modulo n with operation multiplication modulo n such that $\mathbb{Z}_n^* \subset G \subset \mathbb{Z}_n$ (as sets) but $\mathbb{Z}_n^* \neq G$.

Solution. Assume by contradiction there is a group G of integers modulo n with operation multiplication $\mod n$ such that $\mathbb{Z}_n^*$ is a proper subset of G. Then, there exists an element d such that $d \in G$ and $d \notin Z_n^*$. In other words, $\gcd(d, n) > 1$.

Observe that 1 is still the identity element of G, for by regular multiplication rules, $a \cdot 1 = 1 \cdot a = a \equiv a \mod n, \forall a \in G$, and as proven in Homework 1, there cannot be 2 distinct identity elements in the same group.

We now show that d does not have an inverse in G. Assume the contrary, and d^{-1} is an element in group G such that $d \cdot d^{-1} \equiv 1 \mod n$. This yields:

$$d \cdot d^{-1} - 1 = nk, k \in \mathbb{Z}$$
$$d \cdot d^{-1} - nk = 1$$

This is a contradiction, for the LHS is divisible by $\gcd(d, n) > 1$, while the RHS is not.

Therefore, the assumption is false, and there is no group G of integers modulo n with operations multiplication $\mod n$ such that $\mathbb{Z}_n^*$ is a proper subset of G ■

Problem 10: Let $(G, \circ)$ be a group. Fix $a \in G$ and define the left multiplication by a function:

$$L_a : G \to G, x \mapsto a \circ x.$$

(a) Show that L_a is a bijection for every group $(G, \circ)$.
(b) Let $G = \mathbb{Z}_{11}^*$ and let $a = 3$. Describe L_a explicitly (in other words, compute where every element $x \in \mathbb{Z}_{11}^*$ goes).
(c) Let $G = D_3$ and let $a \in G$ be an operation number 2 (from the lecture notes). Compute L_a explicitly.

Solution. (a) We need to show that L_a is one-to-one and onto.
One-to-one: Assume that there are 2 elements $x_1 \neq x_2 \in G$ such that $L_a(x_1) = L_a(x_2)$, then $a \circ x_1 = a \circ x_2$. Left multiply both sides by a^{-1}, we have:

$$\begin{aligned}
&a^{-1} \circ (a \circ x_1) = a^{-1} \circ (a \circ x_2) \\
\Longrightarrow &(a^{-1} \circ a) \circ x_1 = (a^{-1} \circ a) \circ x_2 \text{ (by associativity)} \\
\Longrightarrow &e \circ x_1 = e \circ x_2 \\
\Longrightarrow &x_1 = x_2 \text{ (a contradiction)}
\end{aligned}$$

Therefore, L_a is one-to-one.

Onto: For all $y \in G$, consider $x = a^{-1} \circ y$. Then $L_a(x) = a \circ a^{-1} \circ y = e \circ y = y$. Therefore, L_a is onto.

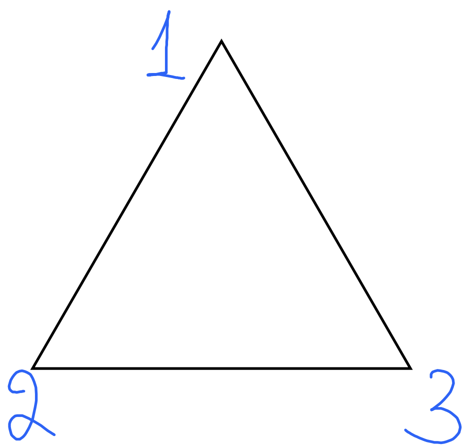
Therefore, L_a is a bijection for all $(G, \circ)$
(b)

$$\begin{aligned}
L_a : \mathbb{Z}_{11}^* &\to \mathbb{Z}_{11}^* \\
1 &\mapsto 3 \\
2 &\mapsto 6 \\
3 &\mapsto 9 \\
4 &\mapsto 1 \\
5 &\mapsto 4 \\
6 &\mapsto 7 \\
7 &\mapsto 10 \\
8 &\mapsto 2 \\
9 &\mapsto 5 \\
10 &\mapsto 8
\end{aligned}$$

(c) Define the operations in the following orders:

Operation #	Transformation
1	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
2	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
3	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
4	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
5	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
6	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Wherein the vertices of the triangles are labeled as follows:



Then:

$$\#1 \mapsto \#2$$
$$\#2 \mapsto \#1$$
$$\#3 \mapsto \#\cancel{4}5$$
$$\#\cancel{4}5 \mapsto \#3$$
$$\#\cancel{5}4 \mapsto \#6$$
$$\#6 \mapsto \#\cancel{5}4$$

■