Homework 2

1. **Some properties of $(\mathbb{Z}_p^*, \times)$.** Recall that $\mathbb{Z}_p^*$ is the set $\{1, \dots, p-1\}$ and $\times$ is integer multiplication $\mod p$, where p is a prime. For example, if $p = 5$, then 2×3 is 1. In this problem we shall prove that $(\mathbb{Z}_p^*, \times)$ is a group. The only part missing in the lecture was the proof that every $x \in \mathbb{Z}_p^*$ has an inverse. We will find the inverse of any element $x \in \mathbb{Z}_p^*$.

   (a) (10 points) Recall $\binom{p}{k} := \frac{p!}{k!(p-k)!}$. For a prime p, prove that p divides $\binom{p}{k}$, if $k \in \{1, 2, \dots, p-1\}$.
   Solution.

(b) (10 points) Recall that $(1+x)^p = \sum_{k=0}^{p} \binom{p}{k} x^k$. Prove by induction that, for any $x \in \mathbb{Z}_p^*$, we have

$$\overbrace{x \times x \times \cdots \times x}^{p\text{-times}} = x$$

Solution.

(c) (10 points) For $x \in \mathbb{Z}_p^*$, prove that the inverse of x is given by

$$\overbrace{x \times x \times \cdots \times x}^{(p-2)\text{-times}}$$

Formally, prove that $x^{p-1} = 1 \mod p$, for any prime p and $x \in \mathbb{Z}_p^*$.
Solution.

2. **Understanding Groups: Part One.** In this problem we shall derive some basic results based on the definition of groups as introduced in the lectures. Let $(G, \circ)$ be a group and let e be the identity element of the group.

   (a) (5 points) Prove that it is impossible that there exists $a, b, c \in G$ such that $a \neq b$ but $a \circ c = b \circ c$.
   Solution.

3. **Understanding Groups: Part Two.** Recall that when we defined a group $(G, \circ)$, we stated that there exists an element e such that for all $x \in G$ we have $x \circ e = x$. Note that e is "applied on x from the right."

   Similarly, for every $x \in G$, we are guaranteed that there exists $\mathsf{inv}(x) \in G$ such that $x \circ \mathsf{inv}(x) = e$. Note that $\mathsf{inv}(x)$ is again "applied to x from the right."

   In this problem, however, we shall explore the following questions: (a) Is there an "identity from the left?," and (b) Is there an "inverse from the left?"

   We shall formalize and prove these results in this question.

   (a) (5 points) Prove that $e \circ x = x$, for all $x \in G$.
   Solution.

(b) (8 points) Prove that if there exists an element $\alpha \in G$ such that for all $x \in G$ we have $\alpha \circ x = x$, then $\alpha = e$.
(Remark: Note that these two steps prove that the "left identity" is identical to the right identity e.)
Solution.

(c) (5 points) Prove that $\mathsf{inv}(x) \circ x = e$.
Solution.

(d) (8 points) Prove that if there exists an element $\alpha \in G$ and $x \in G$ such that $\alpha \circ x = e$, then $\alpha = \mathsf{inv}(x)$.
(Remark: Note that these two steps prove that the "left inverse of x" is identical to the left inverse $\mathsf{inv}(x)$.)
Solution.

4. **Understanding Groups: Part Three.** In this part, we will prove a crucial property of inverses in groups - they are unique. And finally, using this property, we will prove a result that is crucial to the proof of security of one-time pad over the group $(G, \circ)$.

   (a) (5 points) Suppose $a, b \in G$. Let $\mathsf{inv}(a)$ and $\mathsf{inv}(b)$ be the inverses of a and b, respectively (i.e., $a \circ \mathsf{inv}(a) = e$ and $b \circ \mathsf{inv}(b) = e$). Prove that $\mathsf{inv}(a) = \mathsf{inv}(b)$ if and only if $a = b$.
   Solution.

(b) (5 points) Suppose $m \in G$ is a message and $c \in G$ is a cipher text. Prove that there exists a unique $\mathsf{sk} \in G$ such that $m \circ \mathsf{sk} = c$.
Solution.

5. **Calculating Large Powers mod p.** Recall that we learned repeated squaring algorithm in class.
(8 points). Calculate the following using this concept

$$11^{507} \pmod{1237}$$

(Remark: 1237 is a prime number).
Solution.

6. **Practice with Fields.** We shall work over the field $(\mathbb{Z}_7, +, \times)$.

   (a) (5.6 points) Addition Table. The (i, j)-th entry in the table is $i+j$. Complete this table. You do not need to fill the black cells because the addition is commutative.

	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

Table 1: Addition Table.

   (b) (5.6 points) Multiplication Table. The (i, j)-th entry in the table is $i \times j$. Complete this table.

	0	1	2	3	4	5	6
0							
1							
2							
3							
4							
5							
6							

Table 2: Multiplication Table.

   (c) (2.6 points) Additive and Multiplicative Inverses. Write the additive and multiplicative inverses in the table below.

	0	1	2	3	4	5	6
Additive Inverse							
Multiplicative Inverse							

Table 3: Additive and Multiplicative Inverses Table.

(d) (7.2 points) Division Table. The (i, j)-th entry in the table is i/j. Complete this table.

	1	2	3	4	5	6
0						
1						
2						
3						
4						
5						
6						

Table 4: Division Table.

Collaborators :