Homework 2

1. **Some properties of $(\mathbb{Z}_p^*, \times)$ (25 points).** 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, when p is any prime. 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 on x that, for any $x \in \mathbb{Z}_p^*$, we have

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

Solution.

(c) (5 points) For $x \in \mathbb{Z}_p^*$, prove that the inverse of $x \in \mathbb{Z}_p^*$ is given by

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

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

2. **Understanding Groups: Part One (30 points).** 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) (7 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) (7 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 right inverse $\mathsf{inv}(x)$.)
Solution.

3. **Understanding Groups: Part Two (15 points).** 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) (7 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) (8 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.

4. **Calculating Large Powers mod p (15 points).** Recall that we learned the repeated squaring algorithm in class.
   Calculate the following using this concept

$$19^{2020} \pmod{101}$$

   (Remark: 101 is a prime number).
   Solution.

5. **Practice with Fields (20 points).** We shall work over the field $(\mathbb{Z}_5, +, \times)$.

(a) (5 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
0					
1					
2					
3					
4					

Table 1: Addition Table.

(b) (5 points) Multiplication Table. The (i,j)-th entry in the table is $i \times j$. Complete this table.

	0	1	2	3	4
0					
1					
2					
3					
4					

Table 2: Multiplication Table.

(c) (5 points) Additive and Multiplicative Inverses. Write the additive and multiplicative inverses in the table below.

	0	1	2	3	4
Additive Inverse					
Multiplicative Inverse					

Table 3: Additive and Multiplicative Inverses Table.

(d) (5 points) Division Table. The (i,j)-th entry in the table is i/j. Complete this table.

	1	2	3	4
0				
1				
2				
3				
4				

Table 4: Division Table.

6. **Order of an Element in $(\mathbb{Z}_p^*, \times)$. (20 points)** The *order* of an element x in the multiplicative group $(\mathbb{Z}_p^*, \times)$ is the smallest positive integer h such that $x^h = 1 \mod p$. For example, the order of 2 in $(\mathbb{Z}_5^*, \times)$ is 4, and the order of 4 in $(\mathbb{Z}_5^*, \times)$ is 2.

   (a) (5 points) What is the order of 4 in $(\mathbb{Z}_{11}^*, \times)$?
   Solution.

   (b) (10 points) Let x be an element in $(\mathbb{Z}_p^*, \times)$ such that $x^n = 1 \mod p$ for some positive integer n and let h be the order of x in $(\mathbb{Z}_p^*, \times)$. Prove that h divides n.
   Solution.

(c) (5 points) Let h be the order of x in $(\mathbb{Z}_p^*, \times)$. Prove that h divides $(p-1)$.
Solution.

7. **Defining Multiplication over $\mathbb{Z}_{27}^*$ (25 points).** In the class, we had considered the group $(\mathbb{Z}_{26}, +)$ to construct a one-time pad for one alphabet messages. A few students were interested in defining a group with 26 elements using a "multiplication"-like operation. This problem shall assist you to define the $(\mathbb{Z}_{27}^*, \times)$ group that has 26 elements.

   The first attempt from class. Recall that in the class we had seen that the following is also a group.

   $$(\mathbb{Z}_{27} \setminus \{0, 3, 6, 9, 12, 15, 18, 21, 24\}, \times),$$

   where $\times$ is integer multiplication $\mod 27$. However, the set had only 18 elements.

   In this problem, we shall define $(\mathbb{Z}_{27}^*, \times)$ in an alternate manner such that the set has 26 elements.

   A new approach. Interpret $\mathbb{Z}_{27}^*$ as the set of all triplets (a_0, a_1, a_2) such that $a_0, a_1, a_2 \in \mathbb{Z}_3$ and at least one of them is non-zero. Intuitively, you can think of the triplets as the ternary representation of the elements in $\mathbb{Z}_{27}^*$. We interpret the triplet (a_0, a_1, a_2) as the polynomial $a_0 + a_1 X + a_2 X^2$. So, every element in $\mathbb{Z}_{27}^*$ has an associated non-zero polynomial of degree at most 2, and every non-zero polynomial of degree at most 2 has an element in $\mathbb{Z}_{27}^*$ associated with it.

   The multiplication ($\times$ operator) of the element (a_0, a_1, a_2) with the element (b_0, b_1, b_2) is defined as the element corresponding to the polynomial

   $$(a_0 + a_1 X + a_2 X^2) \times (b_0 + b_1 X + b_2 X^2) \mod 2 + 2X + X^3$$

   The multiplication ($\times$ operator) of the element (a_0, a_1, a_2) with the element (b_0, b_1, b_2) is defined as follows.

   Input (a_0, a_1, a_2) and (b_0, b_1, b_2).

   (a) Define $A(X) := a_0 + a_1 X + a_2 X^2$ and $B(X) := b_0 + b_1 X + b_2 X^2$

   (b) Compute $C(X) := A(X) \times B(X)$ (interpret this step as "multiplication of polynomials with integer coefficients")

   (c) Compute $R(X) := C(X) \mod 2 + 2X + X^3$ (interpret this as step as taking a remainder where one treats both polynomials as polynomials with integer coefficients). Let $R(X) = r_0 + r_1 X + r_2 X^2$

   (d) Return $(c_0, c_1, c_2) = (r_0 \mod 3, r_1 \mod 3, r_2 \mod 3)$

   For example, the multiplication $(0, 1, 1) \times (1, 1, 2)$ is computed in the following way.

   (a) $A(X) = X + X^2$ and $B(X) = 1 + X + 2X^2$.

(b) $C(X) = X + 2X^2 + 3X^3 + 2X^4$.

(c) $R(X) = -6 - 9X - 2X^2$.

(d) $(c_0, c_1, c_2) = (0, 0, 1)$.

According to this definition of the $\times$ operator, solve the following problems.

- (5 points) Evaluate $(1, 0, 1) \times (1, 0, 1)$
  Solution.

- (10 points) Note that $e = (1, 0, 0)$ is a identity element. Find the inverse of $(1, 0, 1)$.
  Solution.

- (10 points) Assume that $(\mathbb{Z}_{27}^*, \times)$ is a group. Find the order of the element $(1, 1, 0)$.

  (Recall that, in a group $(G, \circ)$, the order of an element $x \in G$ is the smallest positive integer h such that $\overbrace{x \circ x \circ \cdots \circ x}^{h\text{-times}} = e$)

  Solution.

Collaborators :