Solution of Homework 2

1. **Some properties of** $(\mathbb{Z}_p^*, \times)$ **(25 points).** Recall that $\mathbb{Z}_p^*$ is the set $\{1, \ldots, p-1\}$ 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 $k \in \{1, 2, \ldots, p-1\}$.

   Solution.
   We know that $\binom{p}{k}$ is an integer and $p! = \binom{p}{k} \times k!(p-k)!$. Note that p divides $p!$, so it divides $\binom{p}{k} \times k! \times (p-k)!$. However, p does not divide $k!$ for any $1 \leqslant k \leqslant p-1$ since the prime factorization of $k!$ contains only prime numbers that are less than p. Similarly, p also does not divide $(p-k)!$ because $(p-k) < p$ and p is a prime. So, p divides the numerator of $\binom{p}{k}$ but does not divide the denominator of $\binom{p}{k}$, for $1 \leqslant k \leqslant p-1$. We know that $\binom{p}{k}$ is an integer. So, this implies that p divides the integer $\binom{p}{k}$, for $1 \leqslant k \leqslant p-1$.

   Note that in our argument we are using the assumption that p is a prime. If p is a prime and it divides $a \times b$ where a and b are two integers, then p divides a or b. Think if this property is true for non prime integers or not. Moreover, can we say that in general, m divides $\binom{m}{k}$ for $k \in \{1, \ldots, m-1\}$ when m is a non prime integer?

(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.

Base case. Note that $1^p = 1 \mod p$.

Assume that $t^p = t \mod p$.

We will prove the statement for $(t+1)^p$. Recall that

$$(1+t)^p = \sum_{k=0}^{p} \binom{p}{k} t^k = 1 + \sum_{k=1}^{p-1} \binom{p}{k} t^k + t^p.$$

So, we have $(1+t)^p = 1 + t^p \mod p$, because $\binom{p}{k} = 0 \mod p$ if $k \in \{1, \ldots, p-1\}$. By induction hypothesis $t^p = t \mod p$. So, we have $(1+t)^p = (1+t) \mod p$.

Hence, by the principle of mathematical induction, we are done.

(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.
According to part (b), we have $x^p \mod p = x$, so p divides $x^p - x = x(x^{p-1} - 1)$. Since $x \in \mathbb{Z}_p^*$, then p does not divide x. Now, since p divides $x(x^{p-1} - 1)$ but does not divide x and p is a prime, it must divide $x^{p-1} - 1$.

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) (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.
To solve this part, we shall show that for any $a, b, c \in G$ such that $a \circ c = b \circ c$, we have $a = b$. Since $c \in G$, there exists $\mathsf{inv}(c)$ such that $c \circ \mathsf{inv}(c) = e$. Now, we have:

$$
\begin{aligned}
a \circ c &= b \circ c \\
\implies (a \circ c) \circ \mathsf{inv}(c) &= (b \circ c) \circ \mathsf{inv}(c) \\
\implies a \circ (c \circ \mathsf{inv}(c)) &= b \circ (c \circ \mathsf{inv}(c)) \\
\implies a \circ e &= b \circ e \\
\implies a &= b
\end{aligned}
$$

(b) (6 points) Prove that $e \circ x = x$, for all $x \in G$.

Solution.

Since $x \in G$, there exists $\mathsf{inv}(x)$ such that $x \circ \mathsf{inv}(x) = e$. Let $a = e \circ x$ and $b = x$ and $c = \mathsf{inv}(x)$. Then, note that

$$a \circ c = (e \circ x) \circ \mathsf{inv}(x) = e \circ (x \circ \mathsf{inv}(x)) = e \circ e = e$$

and we also have

$$b \circ c = x \circ \mathsf{inv}(x) = e.$$

Therefore, we have $a \circ c = b \circ c$ and so according to part a, we can conclude that $a = b$ or equivalently $e \circ x = x$.

(c) (6 points) Prove that if there exists an element $\alpha \in G$ such that for **some** $x \in G$, 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.

Since $x \in G$, there exists $\mathsf{inv}(x)$ such that $x \circ \mathsf{inv}(x) = e$. Now, we have the following:

$$\alpha \circ x = x$$
$$\implies (\alpha \circ x) \circ \mathsf{inv}(x) = x \circ \mathsf{inv}(x)$$
$$\implies \alpha \circ (x \circ \mathsf{inv}(x)) = x \circ \mathsf{inv}(x)$$
$$\implies \alpha \circ e = e$$
$$\implies \alpha = e$$

(d) (8 points) Prove that $\mathsf{inv}(x) \circ x = e$.

Solution.

Let $a = \mathsf{inv}(x) \circ x$ and $b = e$ and $c = \mathsf{inv}(x)$. Then, we have:

$$a \circ c = \big(\mathsf{inv}(x) \circ x\big) \circ \mathsf{inv}(x) = \mathsf{inv}(x) \circ \big(x \circ \mathsf{inv}(x)\big) = \mathsf{inv}(x) \circ e = \mathsf{inv}(x)$$

$$b \circ c = e \circ \mathsf{inv}(x) = \mathsf{inv}(x)$$

Therefore, $a \circ c = b \circ c$ and so according to part a, we have $a = b$ or equivalently $\mathsf{inv}(x) \circ x = e$

(e) (5 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.

Since $x \in G$, there exists $\mathsf{inv}(x)$ such that $x \circ \mathsf{inv}(x) = e$. Now, we have:

$$\alpha \circ x = e$$
$$\implies (\alpha \circ x) \circ \mathsf{inv}(x) = e \circ \mathsf{inv}(x)$$
$$\implies \alpha \circ (x \circ \mathsf{inv}(x)) = e \circ \mathsf{inv}(x)$$
$$\implies \alpha \circ e = \mathsf{inv}(x)$$
$$\implies \alpha = \mathsf{inv}(x)$$

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) (9 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.
Since in previous problems we have proved that $e \circ x = x$ and $\mathsf{inv}(x) \circ x = e$ for each x, we have the following relations:

$$a = b \iff \mathsf{inv}(a) \circ a = \mathsf{inv}(a) \circ b \tag{1}$$
$$\iff e = \mathsf{inv}(a) \circ b \tag{2}$$
$$\iff e \circ \mathsf{inv}(b) = (\mathsf{inv}(a) \circ b) \circ \mathsf{inv}(b) \tag{3}$$
$$\iff e \circ \mathsf{inv}(b) = \mathsf{inv}(a) \circ (b \circ \mathsf{inv}(b)) \tag{4}$$
$$\iff e \circ \mathsf{inv}(b) = \mathsf{inv}(a) \circ e \tag{5}$$
$$\iff \mathsf{inv}(b) = \mathsf{inv}(a) \tag{6}$$

Note that in above, (3) implies (2) because we can mulitply both sides of (3) from right by b to get (2).

(b) (6 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.

We know that $m \circ \mathsf{sk} = c$. So, the solution for sk is the unique element $\mathsf{inv}(m) \circ c$. We have used the fact that the left inverse of m is identical to its right inverse and it is unique.

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

$$11^{2020^{2020}+2020} \pmod{101}$$

(Hint: Note that 101 is a prime number and before applying repeated squaring algorithm try to simplify the problem using what you learned in part C of question 1).
Solution.
Since 101 is a prime and $11 \in \mathbb{Z}^*_{101}$, then according to question 1, we have

$$11^{100} = 1 \pmod{101}.$$

Furthermore, $2020^{2020} + 2020 = 0 + 20 = 20 \pmod{100}$. Let $2020^{2020} + 2020 = 100 \cdot q + 20 = 1 \cdot 11^2 0 \pmod{101}$, where q is a positive integer. Therefore, we have

$$11^{2020^{2020}+2020} = 11^{100q+20} = \left(11^{100}\right)^q \cdot 11^{20} \pmod{101}$$

We know that $20 = 2^4 + 2^2$. Now, we use repeated squaring algorithm:

$$11^1 = 11 \pmod{101}$$
$$11^2 = 20 \pmod{101}$$
$$11^4 = 97 \pmod{101}$$
$$11^8 = 6 \pmod{101}$$
$$11^{16} = 54 \pmod{101}$$

So

$$11^{20} = 11^{16} \times 11^4 \pmod{101}$$
$$= 97 \times 54 \pmod{101}$$
$$= 87 \pmod{101}$$

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

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

   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	0	4	3	2	1
Multiplicative Inverse		1	3	2	4

   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.

12

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

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 5 in $(\mathbb{Z}_{11}^*, \times)$?
Solution.

$$5^1 = 5 \quad \text{mod } 11$$
$$5^2 = 3 \quad \text{mod } 11$$
$$5^3 = 4 \quad \text{mod } 11$$
$$5^4 = 9 \quad \text{mod } 11$$
$$5^5 = 1 \quad \text{mod } 11$$

Therefore, the order of 4 in $(\mathbb{Z}_{11}^*, \times)$ is 5.

(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.
Let $n = qh + r$, where q, h are integers such that $0 \leqslant r < h$. Then we have

$$x^n = x^{qh+r} = x^{qh} \cdot x^r = (x^h)^q \cdot x^r = 1^q \cdot x^r = x^r \quad \text{mod } p$$

So $x^r = 1 \mod p$ since we are given the fact that $x^n = 1 \mod p$. This implies that $r = 0$ because if $r > 0$, we have a contradiction with the assumption that h is the smallest positive integer such that $x^h = 1 \mod p$. Therefore, $x = qh$, in other words, h divides n.

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

Solution.

By part (c) of Question 1, we have $x^{p-1} = 1 \mod p$. Now, applying the result from part (b) above for $n = p-1$, it must be the case that h divides $(p-1)$.

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 <u>this definition</u> of the $\times$ operator, solve the following problems.

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

  (a) $A(X) = 1 + X^2$

  (b) $B(X) = 1 + X + X^2$

  (c) $C(X) = (1 + X^2)(1 + X + X^2) = 1 + X + 2X^2 + X^3 + X^4$

  (d) $R(X) = -1 - 3X$

  (e) $(c_0, c_1, c_2) = (-1 \mod 3, -3 \mod 3, 0 \mod 3) = (2, 0, 0)$.

  Answer: $(2, 0, 0)$

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

  Solution. Suppose (a, b, c) is the inverse of $(0, 1, 1)$. Then we must have

  $$(X + X^2)(a + bX + cX^2) = 1.$$

  Now we follow the multiplication procedure for two elements $A(X) = X + X^2$ and $B(X) = a + bX + cX^2$.

  (a) $C(X) = aX + (a + b)X^2 + (b + c)X^3 + cX^4$

  (b) $R(X) = (-2b - 2c) + (a - 2b - 4c)X + (a + b - 2c)X^2$

  (c) So $(-2b - 2c) \mod 3 = 1$, $(a - 2b - 4c) \mod 3 = 0$, and $(a + b - 2c) \mod 3 = 0$, which implies that $a = 2, b = 1, c = 0$.

  Thus, $(2, 1, 0)$ is the inverse of $(0, 1, 1)$.

- (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. Recall the fact that the order of any element of a finite group divides the order of the group. The group $\mathbb{Z}_{27}^*$ has 26 elements, so the order of any element in this group divides 26. This implies the follows:

  (a) The set of all possible orders of any element in $\mathbb{Z}_{27}^*$ is $\{1, 2, 13, 26\}$.

  (b) For any element $a \in \mathbb{Z}_{27}^*$, we have $a^{26} = 1$. In particular, $(1 + X^2)^{26} = 1$.

  Clearly, 1 is not the order of $(1, 1, 0)$. Since $(1, 1, 0)^2 = (1 + X)^2$, the order of $(1, 1, 0)$ is not equal to 2. It means that the order is either 13 or 26. Using the facts that $(1 + X^2)^2 = 1 + 2X^2 + X^4 = X(X^3 + 2X + 2) + (1 - 2X) = (1 - 2X) = 1 + X$ and $(1 + X^2)^{26} = 1$, we have

  $$1 = (1 + X^2)^{26} = ((1 + X^2)^2)^{13} = (1 + X)^{13}.$$

  Therefore, the order of $(1, 1, 0)$ is 13.

  Other solution: We just give the idea and skip the calculations here. Using the same argument as above to argue that the order of $(1, 1, 0)$ is in the set $\{1, 2, 13, 26\}$. Then brute force in ascending order to find the order of $(1, 1, 0)$ using repeated square algorithm.

Collaborators :