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 $k \in \{1, 2, \ldots, p-1\}$.

   $\frac{p!}{k!(p-k)!}$ **can be simplified to** $\frac{p(p-1)(p-2)\cdots(p-k+1)}{k!}$**.**

   This is because p is always going to be bigger than k, so when all of the factorials are expanded, some of the lower terms of $p!$ will be cancelled out by the terms of $(p-k)!$. For example, if p is 5 and k is 2, $p!$ will expand to $5*4*3*2*1$, and $(p-k)!$ will expand to $3*2*1$. Since $p!$ is in the numerator, and $(p-k)!$ is in the denominator, there will only be a $5*4$ left in the numerator after simplification.

   We know that p will always be present in the numerator because it cannot be divided by any k and is always greater than k. Therefore, since p is still present in the numerator, we can conclude that for a prime p, p divides $\binom{p}{k}$ if $k \in \{1, 2, \ldots, p-1\}$.

(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

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

Essentially, we must prove that $x^p = x \mod p$.

For proof by induction, we start with a base case. In this case, it will be when $x = 1$, since that's the lowest possible value in the group $\mathbb{Z}_p^*$. For $x = 1$, we can clearly see that $1^p = 1 \mod p$. Therefore, the base case holds true.

The next step is to assume that, for an arbitrary value $y \in \mathbb{Z}_p^*$,
$y^p = y \mod p$.
Now, we must prove that it works for a value $(1+y) \in \mathbb{Z}_p^*$. In other words, we are proving the statement that $(1+y)^p = (1+y) \mod p$.

We can start by evaluating what was given to us, $(1+y)^p = \sum_{k=0}^{p} \binom{p}{k} y^k$. This expands into the following:
$= \binom{p}{0} y^0 + \binom{p}{1} y^1 + \cdots + \binom{p}{p-1} y^{p-1} + \binom{p}{p} y^p$
Since $\binom{p}{0} y^0 = 1$ and $\binom{p}{p} y^p = y^p$, this further simplifies into:
$= 1 + \binom{p}{1} y^1 + \cdots + \binom{p}{p-1} y^{p-1} + y^p$

We also proved in part (a) that, for any $k \in \{1, 2, \cdots, p-1\}$, p divides $\binom{p}{k}$. Therefore, if we take the above equation $\mod p$, then all of the terms with coefficients between $\binom{p}{1}$ to $\binom{p}{p-1}$, inclusive, will cancel out, leaving us with the equation:

$= (1 + \binom{p}{1} y^1 + \cdots + \binom{p}{p-1} y^{p-1} + y^p) \mod p$
$= (1 + y^p) \mod p$

Since we assume that $y^p \mod p = y$, and we know that $1 \mod p = 1$, we can further simplify the right side, giving us the final equation:
$= (1+y) \mod p$
And when joined with the equation in the problem statement,
$(1+y)^p = (1+y) \mod p$
which is the equation that we desired.

Therefore, by induction, $x^p \mod p = x$.

(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 $x \in \mathbb{Z}_p^*$.

From the previous part, we proved that $x^p = x \mod p$.
Simplifying, if we divide both sides by x, we get the equation:
$x^{p-1} = 1 \mod p$
Which is the equation that we are looking for.

Therefore, the inverse of $x \in \mathbb{Z}_p^*$ is given by $x^{p-1} = 1 \mod p$ for any prime p and any $x \in \mathbb{Z}_p^*$.

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 $a \circ c = b \circ c$.

   Looking at the equation $a \circ c = b \circ c$, we can $\circ$ both sides of the equation by $inv(c)$. Since we also know from the problem statement that $x \circ inv(x) = e$, the following can be deduced:

   $a \circ c = b \circ c$
   $a \circ (c \circ inv(c)) = b \circ (c \circ inv(c))$
   $a \circ e = b \circ e$
   $a = b$

   a has to equal b, so we know that it is impossible that there exists $a, b, c \in G$ such that $a \neq b$ but $a \circ c = b \circ c$.

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

Due to the identity property of a group, we know that $\exists e \in G$ **such that for all** $x \in G$, $x \circ e = x$.

Also, due to the inverse property of a group, we know that for every element $x \in G$, $\exists inv(x) \in G$ **such that** $x \circ inv(x) = e$.

Therefore, using associativity, we can deduce the following:

$e \circ x = x$
$(x \circ inv(x)) \circ x = x$
$x \circ (inv(x) \circ x) = x$
$x \circ e = x$

Since $x \circ e = x$ **is 100% true (it's a property of a group), we can say with confidence that** $e \circ x = x$.

(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.)

From part (a), we know that it is impossible that $a \circ b = a \circ c$ where $b \neq c$.

This means that there is only ONE element x where $a \circ x = x$.

We also know that, by the identity property of a group, $\exists e \in G$ such that for all $a \in G$, $a \circ e = a$.

Therefore, since we know that there is only ONE element that holds for $a \circ x = x$, and applying the identity element to a variable doesn't change it (which is what is happening here), we can say with confidence that a must equal e.

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

Say that an element x **has an inverse from the left,** i_L**, and an inverse from the right,** i_R**. This means that:**
$i_L \circ x = e$ **and** $x \circ i_R = e$

Consider the equation $i_L \circ x \circ i_R$**. Using the associativity property of a group, and the fact that a group has both a left and right identity (as proved in part (c)), we know that:**

$(i_L \circ x) \circ i_R = i_L \circ (x \circ i_R)$
$e \circ i_R = i_L \circ e$
$i_R = i_L$

Since the inverse from the left i_L **equals the inverse from the right** i_R**, and the problem statement says that there exists** $inv(x) \in G$ **such that** $x \circ inv(x) = e$**, we know for a fact that** $inv(x) \circ x = e$**.**

(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 $\mathsf{inv}(x)$.)

In part (d), we already proved that $inv(x) \circ x = x \circ inv(x) = e$.
The important equation here is that $inv(x) \circ x = e$.

So, since we also know from part (a) that there can only be ONE variable where $a \circ x = e$, we can confidently say that a MUST equal $inv(x)$.

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 $a = b$.

   Say we have an inverse $i \in G$, for 2 separate elements $a, b \in G$, where $a \circ i = e$ and $b \circ i = e$. Due to the fact that there is a left and right inverse AND identity (proved in question 2), we can derive the following:

   $a = a \circ e$
   $= a \circ (b \circ i)$
   $= a \circ (i \circ b)$
   $= (a \circ i) \circ b$
   $= e \circ b$
   $= b$
   $\therefore a = b$

   Since we simplified to $a = b$, we know that $inv(a) = inv(b)$ if and only if $a = b$.

(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 $m \circ \mathsf{sk} = c$.

Say we have $sk_1 \in G$ **where** $m \circ sk_1 = c$**.**
And another $sk_2 \in G$ **where** $m \circ sk_2 = c$**.**

We know from the previous question that $inv(a) = inv(b)$ **if and only if** $a = b$**.**
We also know that decryption for one-time pad with secret key $sk \in G$ **is defined as** $c \circ inv(sk) = m$**.**

Using all of the above equations, we can do the following:

$c \circ inv(sk_1) = m$
$= (m \circ sk_2) \circ inv(sk_1) = m$
$= m \circ (sk_2 \circ inv(sk_1) = m$

In problem 2, we have already proved that there can only be one element that holds for an equation $m \circ x = m$ **- the identity element** e**. This means that** $\mathsf{sk}_2 \circ inv(sk_1) = e$**. We also proved in part 2 that an element has a unique inverse. Therefore, the only way that** $sk_2 \circ inv(sk_1) = e$ **is if** $sk_1 = sk_2$**. Given all of this information, we can conclude that there is a unique secret key** sk **such that** $m \circ sk = c$**.**

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).

   $11^{2020^{2020}+2020} \pmod{101}$ **can be expanded to** $11^{2020^{2020}} * 11^{2020} \pmod{101}$**.**
   In part C of question 1, we derived the equation $x^{p-1} = 1 \mod p$**, for any prime number** p**. We know that** 101 **is a prime number, so with** $x = 11$**, we have the equation** $11^{100} = 1 \mod 101$**.**

   Focusing on the lone 11^{2020} **(note that the** $\mod 101$ **is abstracted out for readability):**
   11^{2020}
   $= 11^{100*20+20}$
   $= (11^{100})^{20} * 11^{20}$
   $= 1^{20} * 11^{20}$
   $= 11^{20}$
   Doing the same for $11^{2020^{2020}}$**, and that** $11^{2020} = 11^{20}$ **(** $\mod 101$ **is implicit):**
   $11^{2020^{2020}}$
   $= 11^{20^{2020}}$
   $= 11^{20^{100*20+20}}$
   $= \left((11^{20})^{100}\right)^{20} * 11^{20^{20}}$
   $= 1^{20} * 11^{20^{20}}$
   $= 11^{20^{20}}$
   $= \left(11^{20^2}\right)^{10}$
   $= \left(11^{400}\right)^{10}$
   $= \left((11^{100})^4\right)^{10}$
   $= \left(1^4\right)^{10}$
   $= 1$
   Therefore, the equation from the 1st paragraph simplifies into:
   $11^{2020^{2020}} * 11^{2020} \pmod{101}$
   $= 1 * 11^{20} \pmod{101}$
   $= 11^{20} \mod 101$

   The repeating squares algorithm for this problem defines the following:
   $\alpha_0 = 11^{2^0} \mod 101 = 11^1 \mod 101 = 11 \mod 101 = 11$

$\alpha_1 = 11^{2^1} \mod 101 = \alpha_0 * \alpha_0 \pmod{101} = 121 \mod 101 = 20$
$\alpha_2 = 11^{2^2} \mod 101 = \alpha_1 * \alpha_1 \pmod{101} = 400 \mod 101 = 97$
$\alpha_3 = 11^{2^3} \mod 101 = \alpha_2 * \alpha_2 \pmod{101} = 9409 \mod 101 = 16$
$\alpha_4 = 11^{2^4} \mod 101 = \alpha_3 * \alpha_3 \pmod{101} = 256 \mod 101 = 54$

Our simplified equation can be broken apart into:
$11^{20} \mod 101$
$= 11^{16+4} \mod 101$
$= 11^{16} * 11^4 \pmod{101}$
$= \alpha_4 * \alpha_2 \pmod{101}$
$= 54 * 97 \pmod{101}$
$= 5238 \mod 101$
$= 87$ **Therefore,** $11^{2020^{2020}+2020} = 87$

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.

	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 $(\mathbb{Z}_{11}^*, \times)$?

   $5^1 \mod 111 = 5 \mod 11 = 5$
   $5^2 \mod 111 = 25 \mod 11 = 3$
   $5^3 \mod 111 = 125 \mod 11 = 4$
   $5^4 \mod 111 = 625 \mod 11 = 9$
   $5^5 \mod 111 = 3125 \mod 11 = 1$

   Therefore, the order of 5 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.

   First off, we know that $x^n = 1 \mod p$ **and that** $x^h = 1 \mod p$**. To simplify, we will call** $1 \mod p = e$**, where** e **is the identity for this group. Therefore,** $x^n = e$ **and** $x^h = e$

   Let us say that $n = c * h + r$**, where** c **is some positive integer coefficient, and** r **is some remainder. I set it up this way because** h **is the SMALLEST positive integer such that** $x^h = 1 \mod p$**. Therefore,** n **will always be greater than or equal to** h**. If we plug in this equation to** $x^n = e$ **and simplify, we see the following:**

   $x^n = e$
   $x^{ch} * x^r = e$

   $x^{ch} = e$**, so:**

   $x^{ch} * x^r = e$
   $e * x^r = e$
   $x^r = e$

We know that $e = 1 \mod p$**, which will always equal** 1**. Therefore, if** $x^r = 1$**,** r **has to be** 0**. If** $r = 0$**, that means that** $n = c * h$**. Clearly,** h **divides** n**.**

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

From part C of problem 1, $x^{p-1} = 1 \mod p$**. Since, in 6b,** $x^n = 1 \mod p$**, we can use the exact same logic as in 6b, but instead drop** $p-1$ **in the place of** n**, we can clearly see 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 $a_0 + a_1X + a_2X^2$. 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

$$(a_0 + a_1X + a_2X^2) \times (b_0 + b_1X + b_2X^2) \mod 2 + 2X + X^3$$

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 $A(X) := a_0 + a_1X + a_2X^2$ and $B(X) := b_0 + b_1X + b_2X^2$

(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 $R(X) = r_0 + r_1X + r_2X^2$

(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 $(1, 0, 1) \times (1, 1, 1)$

(a) $A(X) = a_0 + a_1X + a_2X^2 = 1 + X^2$.

(b) $B(X) = b_0 + b_1X + b_2X^2 = 1 + X + X^2$

(c) $C(X) = A(X) \times B(X) = (X^2 + 1)(X^2 + X + 1) = 1 + X + 2X^2 + X^3 + X^4$.

(d) $R(X) = C(X) \mod 2 + 2X + X^3 = (X^4 + X^3 + 2X^2 + X + 1) \mod (2 + 2X + X^3) = -1 - 3X$.

(e) $(c_0, c_1, c_2) = (r_0 \mod 3, r_1 \mod 3, r_2 \mod 3) = (2, 0, 0)$.

$(1, 0, 1) \times (1, 1, 1) = (2, 0, 0)$

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

The inverse i of $(0, 1, 1)$ would mean that $(0, 1, 1) \times i = (1, 0, 0)$.
If we work backwards using the $\times$ operator, we will be able to find out the inverse.

(a) $(c_0, c_1, c_2) = (1, 0, 0)$**, and since** (c_0, c_1, c_2) **is a modulo of** $R(X)$**, we can set** $R(X) = (1, 0, 0)$**, so** $R(X) = 1$**.**

(b) $R(X) = C(X) \mod 2 + 2X + X^3$**, and** $C(X) = A(X) \times B(X)$**. We know that** $A(X) = X + X^2$**, so we have to make** $(B(X) \times (X + X^2))$ $(\text{mod } 2 + 2X + X^3)$ **be a polynomial that reduces into** $(1, 0, 0)$ **based on the definition of $\times$ in this group.**

(c) **After testing some triplets in this group, I found that** $(2, 1, 0) = 2 + X$ **works. By the definition of $\times$ in this group,** $(0, 1, 1) \times (2, 1, 0)$ $(\text{mod } 2 + 2X + X^3) = -2 + 3X^2$**. This corresponds to the polynomial** $(-2 \mod 3, 0, 3 \mod 3)$**, which simplifies to** $(1, 0, 0)$**.**

Therefore, the inverse of $(0, 1, 1) = (2, 1, 0)$**.**

- (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 $\overbrace{x \circ x \circ \cdots \circ x}^{h\text{-times}} = e$)

  The element $(1, 1, 0)$ **corresponds to the polynomial** $1 + X$**. We need to find the smallest positive integer** h **such that** $(1+X)^h \mod 2+2X+X^3 = e$**.**

  The result of the equation $(1+X)^{13} \mod 2+2X+X^3 = -3767-7065X-2826X^2$**. Turning it into the form** $(r_0 \mod 3, r_1 \mod 3, r_2 \mod 3)$**, we get the result** $(-2826 \mod 3, -7065 \mod 3, -3767 \mod 3) = (1, 0, 0)$**, which means that the order** h **of the element** $(1, 1, 0)$ **is 13.**

Collaborators: Vidur Gupta, Giovanni Ordonez