Homework 2

Collaborators :

Practice Questions

These are practice questions. They will **NOT** be graded. We have also provided the final answers. However, it is up to you to understand how or why the given solution is correct. You do not need to submit these on Gradescope. However, you may find it easier to just include them in the pdf. In that case, please do not mark these questions on Gradescope.

1. **Calculating Large Powers mod p (0 points).** Recall that we learned the repeated squaring algorithm in class. Calculate the following using this concept

$$10^{2025^{2025}+2025} \pmod{101}$$

(Hint: Note that 101 is a prime number, and before applying the repeated squaring algorithm, try to simplify the problem using what you learned in part C of question 1.)

(Note: as can be seen from the latex file, the entirety of $2025^{2025} + 2025$ is in the exponent of 10. Also recall that $a^{b^c} = a^{(b^c)}$, not $\left(a^b\right)^c$, which is $a^{b \cdot c}$)

Solution.

100

2. **Order of an Element in $(\mathbb{Z}_p^*, \times)$. (0 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) (0 points) What is the order of 3 in $(\mathbb{Z}_7^*, \times)$?

   Solution.

   The order of 3 in $(\mathbb{Z}_7^*, \times)$ is 6.

3. **Elliptic curve (0 points).** In class, we have briefly discussed elliptic curves. Here we will see some concrete examples of elliptic curves on finite prime fields.

   Let $Y^2 = X^3 + X$ be an elliptic curve over the field $(F_{23}, +, \cdot)$. A point (X, Y) lies on the elliptic curve if it satisfies the equation $Y^2 = X^3 + X$.

   (a) (0 points) Are the two points $P = (9, 18)$ and $Q = (11, 10)$ on the curve?

   Solution.

   Yes, they are.

   (b) (0 points) Find the point R where the line connecting P and Q intersects the elliptic curve $Y^2 = X^3 + X$. For $R = (x, y)$, define the "inverse of R" to be the point $S = (x, -y)$. Find the inverse of point R. Recall from the lecture that "$P + Q$" is defined to be the point $S :=$ "inverse of R."

   Solution.

   The inverse of R is $S = (19, 22)$.

Homework Questions

These are homework questions and will be graded. Please make sure to clearly mark each problem on Gradescope.

1. **Some properties of $(\mathbb{Z}_p^*, \times)$ (5+5 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) (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.

(b) (5 points) Let p, and q be two distinct primes. Prove that $(p^q - p) + (q^p - q)$ is divisible by pq.

Solution.

2. **Understanding Groups: Part one (5+6+6+8+5 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.

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

(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.

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

(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.

3. **Understanding Groups: Part Two (9+6 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 crucial result for the security of the 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.

(b) (6 points) Suppose $m \in G$ is a message and $c \in G$ is a ciphertext. Prove that there exists a unique $\mathsf{sk} \in G$ such that $m \circ \mathsf{sk} = c$.

Solution.

4. **Order of an Element in $(\mathbb{Z}_p^*, \times)$. (10+5+10+5 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) (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.

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

(c) (10 points) Let h be the order of x in $(\mathbb{Z}_p^*, \times)$, and k be a positive integer. Let r denote the order of $y = x^k \mod p \in \mathbb{Z}_p^*$. Show that $r = \frac{h}{d} \in \mathbb{Z}$ where d denotes the greatest common divisor of h and k.
Hint: Use part (a) and prove that r divides $\frac{h}{d}$ and $\frac{h}{d}$ divides r.
Solution.

(d) (5 points) Let $p > 2$ be a prime, and $a \in (\mathbb{Z}_p^*, \times)$. Then, show that the element $b = a^{\frac{p-1}{2}} \in (\mathbb{Z}_p^*, \times)$ is equal to 1 or has order 2.
Solution.

5. **Defining Multiplication over $\mathbb{Z}_{27}^*$ (5+10+10 points).** In the class, we had considered the group $(\mathbb{Z}_{26}, +)$ to construct a one-time pad for a one-alphabet message. Can we define a group with 26 elements using a "multiplication"-like operation? This problem will help you define the $(\mathbb{Z}_{27}^*, \times)$ group, which has 26 elements.

   The first attempt from class. Recall that in class we saw 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 a different 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 $(2, 0, 1) \times (2, 0, 2)$.
  Solution.

- (10 points) Note that $e = (1, 0, 0)$ is an identity element. Find the inverse of $(0, 0, 2)$.
  Solution.

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

6. **Special Group: Quotient Group $\left(\mathbb{Z}_p^* / \{-1,+1\}, \times\right)$ (1+1 points)**

We will define the group $\left(\mathbb{Z}_p^* / \{-1,+1\}, \times\right)$ using the quotient group and coset notation.

In general, given a group G and a subgroup H, G/H means the set of cosets formed by H in G. The cosets of H in G are $gH := \{g \times h : h \in H\}$ for $g \in G$.

Now, consider the elements in $\mathbb{Z}_p^*$, which are

$$\left\{1, 2, 3, \ldots, \frac{p-1}{2} - 1, \frac{p-1}{2}, \frac{p-1}{2} + 1, \frac{p-1}{2} + 2, \ldots, p-3, p-2, p-1\right\}.$$

The cosets $\mathbb{Z}_p^* / \{-1,+1\}$ are

$$\left\{1 \times \{-1,+1\}, 2 \times \{-1,+1\}, 3 \times \{-1,+1\}, \ldots, \frac{p-1}{2} \times \{-1,+1\}\right\}.$$

Observe that $1 \times \{-1,+1\}$ contains both 1 and $-1 = p-1$. Similarly, $2 \times \{-1,+1\}$ contains both 2 and $p-2$. Finally, $\frac{p-1}{2} \times \{-1,+1\}$ contains both $\frac{p-1}{2}$ and $\frac{-p+1}{2} = p + \frac{-p+1}{2} = \frac{p-1}{2} + 1$. The final set of elements in $\mathbb{Z}_p^* / \{-1,+1\}$ are $\left\{1, 2, \ldots, \frac{p-1}{2} - 1, \frac{p-1}{2}\right\}$.

Intuitively, you can think of it as for any $x \in \mathbb{Z}_p^*$, both x and $-x \in \mathbb{Z}_p^*$ represent the same element in $\mathbb{Z}_p^* / \{-1,+1\}$. The same way that an integer x and $x+p$ represent the same element in $\mathbb{Z}_p^*$. For this reason, $\mathbb{Z}_p^*$ can also be written as $\mathbb{Z}/p\mathbb{Z}$.

Let us look at a concrete example: $\left(\mathbb{Z}_7^* / \{-1,+1\}, \times\right)$. The elements in $\mathbb{Z}_7^*$ are $\{1,2,3,4,5,6\}$. The elements in $\mathbb{Z}_7^* / \{-1,+1\}$ are $\{1,2,3\}$.

$\times$ is defined as multiplication in $\mathbb{Z}_p^*$, then fitting it into elements in $\mathbb{Z}_p^* / \{-1,+1\}$. For example, $2 \times 2 = 4 = 1$.

Answer the following questions:

(a) (1 point) What is 2×3?
Solution.

(b) (1 point) What is 3×3?
Solution.

7. **Special Group: Elliptic Curve Group (2+2+3+3+1+2 points)** An elliptic curve over a field K is the graph E of an equation $Y^2 = X^3 + aX + b$ where $X, Y, a, b \in K$. The identity of the elliptic curve group is a point at infinity, denoted as ∞. Note that the point ∞ is not a point on the graph $Y^2 = X^3 + aX + b$.

   (a) **Addition Rule.** Consider a point $P = (x, y)$ lies on the elliptic curve $E\colon\ Y^2 = X^3 + aX + b$, we define $-P := (x, -y)$ as P reflected in the x-axis. Given, two points $P = (x_p, y_p), Q = (x_q, y_q)$ on E, if $x_p \neq x_q$, the two points are not on the same vertical line, define the addition as $P + Q = -R$, where R is the third point on the straight line passing through P and Q. If $x_p = x_q$, the two points are on the same vertical line, then $y_p = -y_q$ and $Q = -P$. In this case, we define $P + Q = \infty$, the identity of the elliptic curve group. Moreover, define $P + \infty = \infty + P = P$ for any element $P \in E$.

      i. (2 points) Consider $E\colon\ Y^2 = X^3 - 2X + 5$ over F_{19}. Let $P = (2, 3)$ and $Q = (10, 4)$. Check that P and Q are points on E.
      Solution.

      ii. (2 points) Compute $P + Q$.
      Solution.

      iii. (3 points) To add a point $P \neq \infty$ to itself, draw a tangent line on the elliptic curve E at point P. If the line is vertical, then $P + P = \infty$. If the tangent line is not vertical, then it intersects E at exactly one more point. For $P = (2, 3), Q = (10, 4)$ and $-R = P + Q$, compute $P + P, Q + Q$ and $R + R$.
      Solution.

(b) **Elliptic Curve forms a group with identity element ∞.** Consider elliptic curve E: $Y^2 = X^3 + aX + b$ over field K. Let $P = (x_p, y_p), Q = (x_q, y_q)$ be two points on E. Let $-R = P + Q = (x_r, -y_r)$. We will show the following.

i. (3 points) Let $Y = mX + t$ be the line intersecting P and Q. Assume $x_p \neq x_q$. Let $m = \frac{y_p - y_q}{x_p - x_q}$ be the slope of the line. Show that $x_r = m^2 - x_p - x_q$ and $y_r = y_p - m(x_p - x_r)$.
(Hint: Recall Vieta's formula for degree 3 polynomial $a_1X^3 + a_2X^2 + a_1X + a_0 = 0$ over field K, i.e. $a_0, a_1, a_2, a_3 \in K$. Let $r_1, r_2, r_3 \in K$ be the roots of the polynomial. The following equality holds.

$$\begin{cases} r_1 + r_2 + r_3 = -\frac{a_2}{a_3} \\ r_1r_2 + r_2r_3 + r_1r_3 = \frac{a_1}{a_3} \\ r_1r_2r_3 = -\frac{a_0}{a_3} \end{cases}.$$

)
Solution.

ii. (1 point) Show that if $x_p = x_q$ and $y_p = -y_q$, then $P + Q = \infty$.
Solution.

iii. (2 points) Show that if $x_p = x_q$ and $y_p = y_q \neq 0$, then $x_r = m^2 - 2x_p$ and $y_r = m(x_p - x_r) - y_p$ with $m = \frac{3x_p^2 + a}{2y_p}$.
Solution.