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.

   Recall from combinatorial formulae that $\binom{p}{k}$ is an integer.
   1. We know for a fact that p divides $p!$ since $p! = \prod_{i=1}^{p} i$, which includes p. Furthermore, from the question,
   $$p! = \binom{p}{k} \cdot k! \cdot (p-k)!$$
   .
   2. However, since
   $$k \in \{1, 2, ..., p-1\}$$
   , where $1 \leqslant k \leqslant p-1$. This means that p will not divide $k!$ since the prime factorization of $k!$ will only consist of numbers of value $< p$.
   3. Also, since $(p-k) < p$, p does not divide $(p-k)!$.
   4. Hence, what is left is that p divides $\binom{p}{k}$, for p to divide $p!$ as mentioned above in step 1. Therefore, p divides $\binom{p}{k}$, if $k \in \{1, 2, ..., p-1\}$.

(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

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

Solution.

Proof by induction

Let the statement $C(n)$ be:

$$n^p = n \ mod \ p$$

Base case: When $n = 1$, $C(1) = 1^p = 1 \ mod \ p$

Inductive Hypothesis: Assume that $n^p = n \ mod \ p$ holds true.

Inductive Step: We now prove that $C(n+1) = (n+1)^p$ holds true as well.

Using the identity from the question, we know that

$$(1+x)^p = \sum_{k=0}^{p} \binom{p}{k} x^k$$

.

We can then use it on $(n+1)^p$:

$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k$$

$$= 1 + \sum_{k=1}^{p-1} \binom{p}{k} n^k + n^p$$

(Taking out the first and last terms in summation operation)

Furthermore, we know that for $k \in \{1, 2, ..., p-1\}$,

$$\binom{p}{k} = 0 \ mod \ p$$

.

Then, using the inductive hypothesis $n^p = n \ mod \ p$, the equation above can be simplified to:

$$(n+1)^p = (1+n) \ mod \ p$$

$$= (n+1) \ mod \ p$$

Henceforth, $C(n+1)$ holds and $x^p = x \ mod \ p$.

(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.

From part (b), we know that $x^p \ mod \ p = x$.

1. Extending from this, $x^p - x = 1 \ mod \ p$.
2. This means that p divides $(x^p - x)$.
3. Factorising x, $(x^p - x) = x(x^{p-1} - 1)$
4. However, since $x \in \mathbb{Z}_p^*$, this means that p does not divide x.
5. Hence, since p divides $x^p - x = x(x^{p-1} - 1)$, this means that p divides $(x^{p-1} - 1)$ and thus, $x^{p-1} = 1 \mod p$.

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

   Solution.

   Proof by contradiction

   Suppose $\exists\ a, b, c \in G$ such that $a \neq b$ but $a \circ b = b \circ c$.

   1. Since $c \in G$, by definition of a Group, $\exists\ inv(c)$ such that $c \circ inv(c) = e$(identity).

   2.

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

$\Rightarrow$

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

$\Rightarrow$

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

$\Rightarrow$

$$a \circ e = b \circ e$$

$\Rightarrow$

$$a = b$$

   3. Hence, there is a contradiction here that $a \neq b$ as $a = b$ as shown above. This means 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 $x \in G$.

Solution.

Since $x \in G, \exists\ inv(x)$ such that $x \circ inv(x) = e$.

1. Let us define $a = e \circ x, b = x, c = inv(x)$

2.
$$a \circ c = (e \circ x) \circ inv(x)$$

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

$$= e \circ e$$

$$= e$$

3.
$$b \circ c = x \circ inv(x)$$

$$= e$$

4. Since $a, b, c \in G$, by definition, we note that from part (a), $a \circ c = b \circ c$ denotes that $a = b$.

5. Thus, $e \circ x = x, \forall x \in G$.

(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.

1. Since $x \in G, \exists\ inv(x)$ such that $x \circ inv(x) = e$.
2. From question,

$$\alpha \circ x = x$$

$\Rightarrow$

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

$\Rightarrow$

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

$\Rightarrow$

$$\alpha \circ e = e$$

$\Rightarrow$

$$\alpha = e$$

.

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

Solution.

1. Let $a = inv(x) \circ x$, $b = e$, $c = inv(x)$.
2. $a \circ c = (inv(x) \circ x) \circ inv(x)$
$= inv(x) \circ (x \circ inv(x))$
$= inv(x) \circ e$
$= inv(x)$
3. $b \circ c = e \circ inv(x)$
$= inv(x)$
4. Thus, we note that $a \circ c = b \circ c$. Using result from part (a), since $a \circ c = b \circ c, a = b$.
$\Leftrightarrow$

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

(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.

1. Since $x \in G, \exists\ inv(x)$ such that $x \circ inv(x) = e$, by properties of a group.
2. From question,

$$a \circ x = e$$

$\Rightarrow$

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

$\Rightarrow$

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

(By associativity property of a group)
$\Rightarrow$

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

(From part (c) that left identity is identical to right identity)
$\Rightarrow$

$$a = inv(x)$$

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.

   1. We know from Q2 above that the left identity is identical to the right identity, and the left inverse is identical to the right inverse.

   $\Rightarrow$

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

   2. From the question:

   $$a = b$$

   $\Rightarrow$

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

   $\Rightarrow$

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

   $\Rightarrow$

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

   $\Rightarrow$

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

   (By associativity of groups)

   $\Rightarrow$

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

   $\Rightarrow$

   $$inv(b) = inv(a)$$

(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.

1. We know from Q2 above that the left inverse is identical to the right inverse.

$\Rightarrow$

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

2. Since $m \in \mathbb{G}$, by property of groups, $inv(m) \in G$.
3. Then, from question:

$$m \circ sk = c$$

$\Rightarrow$

$$inv(m) \circ (m \circ sk) = inv(m) \circ c$$

$\Rightarrow$

$$(inv(m) \circ m) \circ sk = inv(m) \circ c$$

$\Rightarrow$

$$e \circ sk = inv(m) \circ c$$

$\Rightarrow$

$$sk = inv(m) \circ c$$

Thus, $sk = inv(m) \circ c$ is a unique element $\in G$, 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

$$11^{2024^{2024}+2024} \pmod{101}$$

(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.

1. We first note that 101 is prime and $11 \in \mathbb{Z}^*_{101}$. Using Fermat's Little Theorem as presented in part C of question 1, $x^{p-1} = 1 \ mod \ p$, we obtain the following:

$$11^{100} = 1 \ (mod \ 101)$$

2. To simplify the expression further, we are interested in mod 100 since the exponent to 11 above is 100, and since we are only interested in mod 100, we can note that only the last 2 digits of 2024 would affect the remainder produced by mod 100.
3. Thus, for 2024, the last digits are 24. We can observe the following pattern below for $24 \cdot k \ (mod \ 100)$, where k is a positive integer:

$$24 = 24(mod \ 100)$$

$$24^2 = 76(mod \ 100)$$

$$24^3 = 24(mod \ 100)$$

$$24^4 = 76(mod \ 100)$$

4. Hence, we can note that in the case when the exponent is even, the result is $76(mod \ 100)$, while in the case when the exponent is odd, the result is $24(mod \ 100)$. Since 2024 is an even number, this means that $24^{2024} = 76(mod \ 100)$. This means the following:

$$2024^{2024} + 2024 = 76 + 24 \ (mod \ 100)$$

$$= 0(mod \ 100)$$

5. Next, let $2024^{2024} + 2024 = 100 \cdot a$, where a is some positive random integer. Thus, the expression given in the question simplifies to:

$$11^{2024^{2024}+2024} \ (mod \ 101) = 11^{100 \cdot a} \ (mod \ 101)$$

$$= (11^{100})^a \ (mod\ 101)$$

$$= (1)^a \ (mod\ 101)$$

$$1 \ (mod\ 101)$$

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.

	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 $(\mathbb{Z}_7^*, \times)$?
   Solution.
   1. We can make the following calculations to find the smallest integer h such that $x^h = 1\ mod\ p$.

$$5^1 = 5\ mod\ 7$$

$$5^2 = 4\ mod\ 7$$

$$5^3 = 6\ mod\ 7$$

$$5^4 = 2\ mod\ 7$$

$$5^5 = 3\ mod\ 7$$

$$5^6 = 1\ mod\ 7$$

   Hence, the order of 5 in $(\mathbb{Z}_7^*, \times)$ is 6.

   (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.
   1. Since $x^n = 1\ mod\ p$, and h is the order of x in $(\mathbb{Z}_p^*, \times)$, we can express n in terms of h and a constant, a:

$$n = a \cdot h + b$$

   , where a, b are integers such that $0 \leqslant b < a$.
   2. This means the following:

$$x^n\ (mod\ p) = x^{a \cdot h + b}\ (mod\ p)$$

$$= x^{a \cdot h} \cdot x^b\ (mod\ p)$$

$$= (x^h)^a \cdot x^b\ (mod\ p)$$

$$= (1)^a \cdot x^b \ (mod\ p)$$

$$= x^b \ (mod\ p)$$

3. Then, from question, $x^n = 1\ mod\ p$. This means that $x^b = 1\ mod\ p$ given the expression in step 2.
4. This means that since $b < h$, and h is the order of x in $(\mathbb{Z}_p^*, \times)$, which means that h is the smallest positive integer such that $x^h = 1\ mod\ p$. This implies that $b = 0$ indefinitely, as there exists a contradiction if $b \neq 0$ given h is the order of x in $(\mathbb{Z}_p^*, \times)$.
5. Thus, $n = a \cdot h$, which implies that 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.

From question 1 part (c), $x^p = 1\ mod\ p$.
1. Since we know from part (b) above that h divides p as $x^p = 1\ mod\ p$,
2. We can further extend this to $(p-1)$ following question 1 part (c). This means 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 message. Can we define 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 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 $a_0 + a_1 X + a_2 X^2$. 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 $(1, 1, 1) \times (1, 0, 1)$.
  Solution.

(a)

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

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

(b)

$$C(X) = (1 + X + X^2)(1 + X^2)$$

$$= 1 + X^2 + X + X^3 + X^2 + X^4$$

$$= 1 + X + 2X^2 + X^3 + X^4$$

(c)

$$R(X) = 1 + X + 2X^2 + X^3 + X^4 - X(2 + 2X + X^3)$$

$$= 1 - X + X^3 - (2 + 2X + X^3)$$

$$= -1 - 3X$$

(d)

$$(C_0, C_1, C_2) = (r_0 \; mod \; 3, r_1 \; mod \; 3, r_2 \; mod \; 3)$$

$$= (2, 0, 0)$$

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

  Solution.

  Let (a, b, c) be the inverse of $(0, 1, 1)$.
  This means that $(X + X^2)(a + bX + cX^2) = 1$ (by property of a Group that multiplying an element with its corresponding inverse = identity)
  Next, applying the multiplication defined in question:
  (a)

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

$$B(X) = a + bX + cX^2$$

  (b)

$$C(X) = (X + X^2)(a + bX + cX^2)$$

$$= aX + bX^2 + cX^3 + aX^2 + bX^3 + cX^4$$

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

  (c)

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

$$= (a - 2c)X + (a + b - 2c)X^2 + (b + c)X^3 - (b + c)(2 + 2X + X^3)$$

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

  This means that $(-2b - 2c) \bmod 3 = 1$, $(a - 2b - 4c) \bmod 3 = 0$, $(a + b - 2c) \bmod 3 = 0$. Solving this equates to $a = 2, b = 1, c = 0$.
  Hence, this means that $(2, 1, 0)$ 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.

  We know that the order of any element of a finite group divides the number of elements in the group. Since the group has 26 elements, this means that the order of $(1, 1, 0) \in \{1, 2, 13, 26\}$. Using repeated squaring algorithm, we can find that the order of $(1, 1, 0)$ is 13, since $(1 + X)^{13} = 1$.

8. **Elliptic curve (10 points).** In class, we have briefly discussed elliptic curve. Here we will see some concrete examples of elliptic curve on finite prime fields.

   (a) (5 points). 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 $Y^2 = X^3 + X$.

      i. (2 points) Verify that the two points $P = (21, 6)$ and $Q = (18, 10)$ are on the curve.
      Solution.

      Given equation of elliptic curve is $Y^2 = X^3 + X$.
      When $x = 21$,

$$x^3 + x = (21)^3 + 21 \ (mod\ 23)$$

$$= 9261 + 21 \ (mod\ 23)$$

$$= 9282 - 9269 \ (mod\ 23)$$

$$= 13 \ (mod\ 23)$$

      When $y = 6$,

$$y^2 = 6^2 \ (mod\ 23)$$

$$= 36 \ (mod\ 23)$$

$$= 13 \ (mod\ 23)$$

      Hence, verified that when $x = 21, y = 6$, $y^2 = x^3 + x$, thus point P lies on the curve.
      When $x = 18$,

$$x^3 + x = (18)^3 + 18 \ (mod\ 23)$$

$$= 5850 \ (mod\ 23)$$

$$= 5850 - 5842 \ (mod\ 23)$$

$$= 8 \ (mod\ 23)$$

When $y = 10$,

$$y^2 = 10^2 \ (mod\ 23)$$

$$= 100 \ (mod\ 23)$$

$$= 100 - 92 \ (mod\ 23)$$

$$= 8 \ (mod\ 23)$$

Hence, verified that when $x = 18, y = 10$, $y^2 = x^3 + x$, thus point Q lies on the curve.

ii. (3 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.

1. Let the gradient of the line connecting P and Q, be m.

$$m = \frac{10 - 6 \ (mod\ 23)}{18 - 21 \ (mod\ 23)}$$

$$= \frac{4 \ (mod\ 23)}{-3 \ (mod\ 23)}$$

$$= \frac{4 \ (mod\ 23)}{20 \ (mod\ 23)}$$

$$= (4 \cdot 15) \ (mod\ 23)$$

$$= 14 \ (mod\ 23)$$

2. Next, we can compute (x_3, y_3) using:

$$x_3 = m^2 - x_1 - x_2 \ (mod\ 23)$$

$$= 14^2 - 18 - 21 \ (mod\ 23)$$

$$= 196 - 18 - 21 \ (mod\ 23)$$

$$= 19 \ (mod\ 23)$$

$$y_3 = m(x_1 - x_3) - y_1 \ (mod\ 23)$$

$$= 14(21 - 19) - 6 \ (mod\ 23)$$

$$= 22 \ (mod\ 23)$$

3. Hence, R $= (19, 22)$. This means that the inverse of R $= (19, -22) = (19, 1)$ since $-22\ (mod\ 23) = 1$.

(b) (5 points). Let $Y^2 = X^3 + X + 7$ be an elliptic curve over the field $(F_{17}, +, \cdot)$.

i. (2 points) Verify that the two points $P = (5, 16)$ and $Q = (1, 3)$ are on the curve.
Solution.

Given equation of elliptic curve is $Y^2 = X^3 + X + 7$.
When $x = 5$,

$$x^3 + x + 7 = (5)^3 + 5 + 7 \ (mod\ 17)$$

$$= 1 \ (mod\ 17)$$

When $y = 16$,

$$y^2 = 16^2 \ (mod\ 17)$$

$$= 1 \ (mod\ 17)$$

Hence, verified that when $x = 5, y = 16$, $y^2 = x^3 + x + 7$, thus point P lies on the curve.
When $x = 1$,

$$x^3 + x + 7 = 1^3 + 1 + 7 \ (mod\ 17)$$

$$= 9 \ (mod\ 17)$$

When $y = 3$,

$$y^2 = 3^2 \ (mod\ 17)$$

$$= 9 \ (mod\ 17)$$

Hence, verified that when $x = 1, y = 3$, $y^2 = x^3 + x + 7$, thus point Q lies on the curve.

ii. (3 points) Find the point R where the line connecting P and Q intersects the elliptic curve $Y^2 = X^3 + X + 7$. Find the inverse of point R.
Solution.

1. Let the gradient of the line connecting P and Q, be m.

$$m = \frac{6 - 3\ (mod\ 17)}{5 - 1\ (mod\ 17)}$$

$$= \frac{13\ (mod\ 17)}{4\ (mod\ 17)}$$

$$= (13 \cdot 13)\ (mod\ 17)$$

$$= 16\ (mod\ 17)$$

2. Next, we can compute (x_3, y_3) using:

$$x_3 = m^2 - x_1 - x_2\ (mod\ 17)$$

$$= 16^2 - 5 - 1\ (mod\ 17)$$

$$= 12\ (mod\ 17)$$

$$y_3 = m(x_1 - x_3) - y_1\ (mod\ 17)$$

$$= 16(5 - 12) - 16\ (mod\ 17)$$

$$= 8\ (mod\ 17)$$

3. Hence, R $= (12, 8)$. This means that the inverse of R $= (12, -8) = (12, 9)$ since $-8\ (mod\ 17) = 9$.

Collaborators :

Josh Tseng, Rohan Purandare, Adam Nasr, Nate Johnson