MATH 3311, FALL 2025: HOMEWORK 1

Much of the material in this homework is very classical and all over the interweb. So I urge you to resist the call of Google or ChatGPT, and work everything out for yourself. It'll be *much* more rewarding that way. Even if this resistance proves ultimately futile, keep in mind that the exams are in-class with no assistance, LLM-flavored or otherwise, so you should at least understand what you're writing down.

Now, to business: Long division (that is, the Euclidean algorithm) says that if $a, b \in \mathbb{Z}$ then we can find $q, r \in \mathbb{Z}$ with $|r| < b$ such that $a = qb + r$. Consider the following process: Set $r_0 = r$, and apply the Euclidean algorithm to the pair b, r_0 to get q_1, r_1 such that $b = q_1 r_0 + r_1$. Then apply the Euclidean algorithm again to the pair r_0, r_1: $r_0 = q_2 r_1 + r_2$, and then to the pair r_1, r_2, and so on. At each stage, if you prefer, you can take r_i to be the *positive* remainder.

(1) Show that the process terminates; that is, for some natural number $n \geq 1$, we must get $r_n = 0$. Show also that $r_{n-1} = \gcd(a, b)$: This is the largest integer (in magnitude) that divides both a and b.

At each stage, we will take the r_i to be the nonnegative remainder.

Part 1: Proving that the process terminates. For each r_i where $i \geq 1$, it is true that $r_{i+1} < r_i$ because $r_{i-1} = q_{i+1} r_i + r_{i+1}$ and r_{i+1} is the positive remainder such that $|r_{i+1}| = r_{i+1} < r_i$. Therefore, if this process doesn't terminate, we have infinitely many nonnegative integers less than r_1 (we demonstrated that $r_1 > r_2 > r_3 > \cdots$). This cannot happen because there are only a finite amount of such nonnegative integers less than r_1. Therefore, this process must terminate.

Part 2: We will show that if a number x divides both a and b (meaning $a = jx$ and $b = kx$ for some integers j and k), it must divide r_{n-1}.

For convenience, we will label $b = r_{-1}$ and $a = r_{-2}$. This will be used in part 3 as well.

By strong induction, we may prove that $x \mid r_i$ for $-2 \leq i \leq n-1$. By assumption, we have the base cases that $x \mid r_{i-2} = a$ and $x \mid r_{i-1} = b$.

Inductive step: Given $x \mid r_{i-2}$ and $x \mid r_{i-1}$ we wish to prove $x \mid r_i$. Proof: since $x \mid r_{i=2}$ and $x \mid r_{i-1}$, $r_{i-2} = jx$ and $r_{i-1} = kx$ for some integers j and k. Then, $r_i = r_{i-2} - q_i r_{i-1} = jx - q_i kx = (j - q_i k)x$ meaning $x \mid r_i$.

Therefore, we also reach the conclusion that $x \mid r_{n-1}$. This means that no common factor of a and b can be greater than r_{n-1}.

Part 3: We will now show that r_{n-1} divides both a and b.

By strong induction, we may prove that $r_{n-1} \mid r_i$ for $n - 1 \geq i \geq -2$. (We will work upwards from $i = n - 1$ to $i = -2$. Base cases: clearly $r_{n-1} \mid r_{n-1}$. Also, since $r_{n-2} = q_n r_{n-1} + r_n = q_n r_{n-1}$ so $r_{n-1} \mid r_{n-2}$

Inductive step: Given $r_{n-1} \mid r_{i+2}$ and $r_{n-1} \mid r_{i+1}$, we wish to prove that $r_{n-1} \mid r_i$. Proof: Since $r_{n-1} \mid r_{i+2}$ and $r_{n-1} \mid r_{i+1}$, $r_{i+2} = j r_{n-1}$ and $r_{i+1} = k r_{n-1}$ for some integers j and k. Then, $r_i = q_{i+2} r_{i+1} + r_{i+2}$ and substitution yields $r_i = q_{i+2} k r_{n-1} + j r_{n-1} = (q_{i+2} k + j) r_{n-1}$, thereby establishing $r_{n-1} \mid r_i$.

Therefore, we know r_{n-1} divides both $r_{-2} = a$ and $r_{-1} = b$

Combining parts 2 and 3 tells us that r_{n-1} is the greatest possible common factor of a and b, i.e. $\gcd(a, b)$.

(2) Use the above process to conclude that we can find integers $s, t \in \mathbb{Z}$ such that

$$\gcd(a, b) = sa + tb.$$

Lemma: If x and y are linear combinations of a and b, any linear combination of x and y are linear combinations of a and b. Proof: Suppose $x = k_1a + k_2b$ and $y = j_1a + j_2b$. Then a linear combination of those would look like $c(k_1a + k_2b) + d(j_1a + j_2b)$. This is equal to $(ck_1 + dj_1)a + (ck_2 + dj_2)b$, which is a linear combination of a and b.

Note that $a - qb = r_0$ and $b - q_1r_0 = b - q_1(a - qb) = r_1$. Notice that r_0 and r_1 are linear combinations of a and b (r_1 is a linear combination by our lemma). For $i \geq 2$, $r_{i-2} - q_ir_{i-1} = r_i$. By the lemma, is clear that r_i is therefore a linear combination of a and b if we know that r_{i-1} and r_{i-2} are both such linear combinations. Inductively, this is true for any i until we run out of remainders because we have the base cases that r_0 and r_1 are linear combinations of a and b. Therefore, we have that the last nonzero remainder, $r_{n-1} = \gcd(a, b)$ is a linear combination of a and b. In other words, there are integers $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$.

(3) If $b = p$ is a prime number and $p \nmid a$, show that we can find integers $s, t \in \mathbb{Z}$ such that

$$1 = sa + tp.$$

We wish to prove that $\gcd(p, a) = 1$. The only factors of p is 1 and p because p is prime. However, $p \nmid a$, so a is not a common factor. Obviously $1 \mid a$, so 1 is the only common factor between p and a, and thus $\gcd(p, a) = 1$.

By problem 2, we may now find $s, t \in \mathbb{Z}$ such that $\gcd(a, p) = 1 = sa + tp$.

An *equivalence relation* on a set X is a relation $x \sim y$ on pairs of elements $x, y \in X$ with the following properties:
Reflexivity: $x \sim x$ for all $x \in X$;
Symmetry: $x \sim y \Leftrightarrow y \sim x$;
Transitivity: $x \sim y$ and $y \sim z \Rightarrow x \sim z$.

An *equivalence class* for an equivalence relation $\sim$ on X is a subset $C \subset X$ such that for all $x, y \in C$, we have $x \sim y$, and if $z \notin C$, then $x \nsim z$ (this means that C contains only elements that are equivalent to each other, and no element outside C is equivalent to something within it).

An element x in an equivalence class C will be called a *representative* for C. A *full set of representatives* is a subset $P \subset X$ that contains a unique representative for each equivalence class for the relation $\sim$. This means that P is in bijection with the set of equivalence classes for the relation $\sim$, and can therefore be used (with care) as a stand-in for the set of all such classes.

(4) If $n \in \mathbb{Z}$ is an integer, show that the relation $x \equiv y \pmod{n}$ whenever $n \mid x - y$ is an equivalence relation on $\mathbb{Z}$, and show that the subset $\{0, 1, 2, \ldots, n - 1\} \subset \mathbb{Z}$ consists of a full set of representatives for this relation.

Part 1: showing reflexivity, symmetry, and transitivity of the relation to determine it is an equivalence relation.

Reflexivity: $\forall x \in \mathbb{Z}, x \equiv x \pmod{n}$ because $n \mid x - x = 0$.

Symmetry: $\forall x, y \in \mathbb{Z}, x \equiv y \pmod{n} \iff n \mid x - y \iff n \mid y - x \iff y \equiv x \pmod{n}$. Note that $n \mid x - y \iff n \mid y - x$ because $n \mid x - y$ means $x - y = kn$ for some integer k and therefore $y - x = -kn$, meaning $n \mid y - x$. The other direction for this if and only if statement follows the same reasoning.

Transitivity: $\forall x, y, z \in \mathbb{Z}, x \equiv y \pmod{n} \wedge y \equiv z \pmod{n} \implies n \mid x - y \wedge n \mid y - z \implies n \mid (x - y) + (y - z) = x - z \implies x \equiv z \pmod{n}$. For more clarity, note that $n \mid x - y \wedge n \mid y - z \implies$

$n \mid (x-y)+(y-z) = x-z$ because $n \mid x-y \wedge n \mid y-z$ means $x-y = jn$ and $y-z = kn$ for some $j, k \in \mathbb{Z}$. Then, $x-z = (x-y)+(y-z) = jn-kn = (j-k)n$ so $n \mid x-z$.

Part 2: showing all integers have a representative in the set $\{0, 1, 2, ..., n-1\}$. Suppose we have an arbitrary integer a. Applying the Euclidean algorithm (with the nonnegative remainder), we get $a = qn + r$ for $q, r \in \mathbb{Z}$ and $|r| = r < n$. Clearly, $r \in \{0, 1, 2, ..., n-1\}$, as it is a nonnegative integer smaller than n. We claim that r is a suitable representative for a: i.e. $a \equiv r \pmod{n}$. This is true because $a - r = qn$, meaning $n \mid a - r$, proving our claim. So each integer has a representative for the relation in that set. Now we must show that each integer has a unique such representation. Suppose both r and s are representatives of a in the aforementioned set. Since s is a representative, $a \equiv s \pmod{n}$. Using symmetry, we have $s \equiv a \pmod{n}$. Since r is also a representative, we have $a \equiv r \pmod{n}$. By transitivity, we may combine $s \equiv a \pmod{n}$ and $a \equiv r \pmod{n}$ to obtain $s \equiv r \pmod{n}$. This means $n \mid s-r$. Since s and r are in $\{0, 1, 2, ..., n-1\}$, their maximum difference is $n-1-0 = n-1$. Therefore, $|s-r| < n$. The only multiple of n with absolute value less than n is 0. Therefore, $s - r = 0$, forcing $s = r$. The representative is unique.

(5) Let $\mathbb{Z}/n\mathbb{Z}$ be the set of equivalence classes for the relation $x \equiv y \pmod{n}$. It is in bijection with the set $\{0, 1, 2, \ldots, n-1\}$ by the previous problem, and it carries structures of addition and multiplication: For instance $2 \cdot (n-1)$ is $n-2$ and $2 + n - 1$ is 1. Show that if $n = p$ is prime, then, for any $a \in \mathbb{Z}/p\mathbb{Z}$, $a \neq 0$, the equation $ax = 1$ always admits a solution in $\mathbb{Z}/p\mathbb{Z}$.

By problem 3, we can find $s, t \in \mathbb{Z}$ such that $1 = sa + tp$. $sa \equiv 1 \pmod{p}$ because $sa - 1 = -tp$, meaning $p \mid sa - 1$. If we want to restrict s to the set $\{0, 1, 2, ..., p-1\}$, we can do so by applying the Euclidean algorithm, taking the nonnegative remainder: $s = kp + r$ for some $k, r \in \mathbb{Z}$. Then, as demonstrated in the previous problem, $s \equiv r \pmod{p}$ with $r \in \{0, 1, 2, ..., p-1\}$. Furthermore, $sa \equiv ra \pmod{p}$ because $sa - ra = (s-r)a = kpa$, so $p \mid sa - ra$. Using transitivity shown in the previous problem, $ra \equiv sa \pmod{p}$ and $sa \equiv 1 \pmod{p}$ means $ra \equiv 1 \pmod{p}$. Therefore, r is a solution in $\mathbb{Z}/p\mathbb{Z}$ to $ax = 1$.

(6) Show that the subset $\{a, 2a, 3a, \ldots, (p-1)a\} \subset \mathbb{Z}/p\mathbb{Z}$ is equal to the subset $\{1, 2, \ldots, p-1\}$.

First note that a must not be a multiple of p. Else, $p \mid a$ so $a \equiv 0 \pmod{p}$ but $0 \notin \{1, 2, \ldots, p-1\}$.

Lemma: $a \equiv b \pmod{p} \implies ca \equiv cb \pmod{p}$. Proof: $a \equiv b \pmod{p}$ means $p \mid a - b$, i.e. $a - b = kp$ for some integer k. Therefore, $ca - cb = ckp$, meaning $p \mid ca - cb$. Therefore, $ca \equiv cb \pmod{p}$.

By number 5, we have r such that $ra \equiv 1 \pmod{p}$. We want that $\{ra, 2ra, 3ra, ..., (p-1)ra\} = \{a, 2a, 3a, ..., (p-1)a\}$. We want this because $\{ra, 2ra, 3ra, ..., (p-1)ra\} = \{1, 2, ..., p-1\}$. This is true because we have $ra \equiv 1 \pmod{p}$ and by the lemma, this scales up: for every $k \in \{1, 2, ..., p-1\}$, $kra \equiv k \cdot 1 \pmod{p}$, and therefore $kra \equiv k \pmod{p}$.

$\{a, 2a, 3a, ..., (p-1)a\}$ contains every nonzero multiple of a. If we had ka with either $k < 1$ or $k > p-1$, we can apply the euclidean algorithm to get $k = jp + l$ for $j, l \in \mathbb{Z}$. Then, as demonstrated in the previous problem, $la \equiv ka \pmod{p}$ with $l \in \{0, 1, 2, ..., p-1\}$, meaning $la \in \{a, 2a, 3a, ..., (p-1)a\}$ (we didn't want nonzero multiples, so we excluded $l = 0$).

Since $\{ra, 2ra, 3ra, ..., (p-1)ra\} = \{1, 2, 3, ..., p-1\}$ is a set of nonzero multiples of a, we have that $\{1, 2, 3, ..., p-1\} \subseteq \{a, 2a, 3a, ..., (p-1)a\}$. However, they both have $p-1$ elements. This forces equality: $\{1, 2, 3, ..., p-1\} = \{a, 2a, 3a, ..., (p-1)a\}$.

(7) Conclude that we must have

$$a^{p-1} \cdot (p-1)! = (p-1)! \in \mathbb{Z}/p\mathbb{Z},$$

and so prove Fermat's little theorem: For any integer $a \in \mathbb{Z}$ with $p \nmid a$, $p \mid a^{p-1} - 1$.

Note: the notion of equality in the context of this problem will always be referring to being in the same equivalence class.

Notice that $a^{p-1} \cdot (p-1)! = \Pi_{i=1}^{p-1} ai = \Pi_{k \in \{a,2a,3a,\ldots,(p-1)a\}} k$. We know that $\{a, 2a, 3a, \ldots, (p-1)a\} = \{1, 2, 3, ..., p-1\}$ by problem 6. Therefore, $\Pi_{k \in \{a,2a,3a,\ldots,(p-1)a\}} k = \Pi_{k \in \{1,2,3,\ldots,p-1\}} k$. Recall that the left hand side is equal to $a^{p-1} \cdot (p-1)!$ and the right hand side is equal to $(p-1)!$. Therefore, $a^{p-1} \cdot (p-1)! = (p-1)! \in \mathbb{Z}/p\mathbb{Z}$.

Lemma 0: if $p \mid ab$, then $p \mid a \vee p \mid b$. Proof: Suppose $p \nmid a$ (because if $p \mid a$ we're already done with the proof). Then, as demonstrated in problem 3, $\gcd(p, a) = 1$. Then we have integers m, n such that $1 = ma + np$. Multiplying each side by b, we obtain $b = mab + npb$. Since $p \mid ab$, $ab = kp$ for some integer k. Substituting, we see $b = mkp + npb = (mk + nb)p$, meaning $p \mid b$. Therefore, p divides either a or b.

Lemma 1: if $xz \equiv yz \pmod{p}$ where neither xz not yz is equivalent to 0 in $\mathbb{Z}/p\mathbb{Z}$, then $x \equiv y \pmod{p}$. Proof: $xz \equiv yz \pmod{p} \implies p \mid xz - yz = (x-y)z$. By lemma 0, $p \mid x - y \vee p \mid z$. However, $p \mid z$ cannot be the case because if so, we would have $z = kp$ for some integer k, and then we would have $xz \equiv 0 \pmod{p}$ as $p \mid xz - 0 = xz = akp$. Therefore, it must be the case that $p \mid x - y$, meaning $x \equiv y \pmod{p}$.

Lemma 2: $(p-1)!$ is nonzero in $\mathbb{Z}/p\mathbb{Z}$. This is equivalent to the statement that p does not divide $p-1$: $(p-1)! \equiv 0 \pmod{p}$ means p divides $(p-1)! = 0$. First, note that none of $k \in \{1, 2, ..., p-1\}$ is divisible by p because applying the Euclidean algorithm with the nonnegative remainder yields $k = 0p + k$ as $|k| = k < p$, so we have a nonzero remainder.

Next, we want to apply Lemma 0 repeatedly. Assuming $p \mid (p-1)! = (p-1)(p-2)!$ by way of contradiction, $p \mid p-1 \vee p \mid (p-2)!$. Since we have shown $p \nmid p-1$, we check if $p \mid (p-2)! = (p-2)(p-3)!$. But we again know that $p \nmid p-2$. So we continue checking down the line similarly, until we have $p \mid 1 \vee p \mid 2$. Since both are not true, we arrive at a contradiction. Thus $p \nmid (p-1)!$ and $(p-1)!$ is nonzero in $\mathbb{Z}/p\mathbb{Z}$.

Now we can finally prove Fermat's little theorem. By lemma 2, we proved that $(p-1)!$ is nonzero in $\mathbb{Z}/p\mathbb{Z}$. Since we proved $a^{p-1} \cdot (p-1)! = (p-1)!$ in $\mathbb{Z}/p\mathbb{Z}$, $a^{p-1} \cdot (p-1)!$ is also nonzero. We now have $a^{p-1} \cdot (p-1)! \equiv 1 \cdot (p-1)! \pmod{p}$, and we're ready to apply lemma 1. Using lemma 1, we can cancel out $(p-1)!$ from each side, obtaining $a^{p-1} \equiv 1 \pmod{p}$, yielding $p \mid a^{p-1} - 1$.

(8) Suppose that you have a deck of n cards. A *riffle shuffle* (see: `https://www.youtube.com/watch?v=adNeBLkP8ZM`) is when you cut the deck into two halves, and then interleave them together in alternating fashion. There are two ways to do this: With the top card still on top, or with the top card going second, depending on which half goes first. Can you realize all possible shuffles of n cards using a sequence of riffle shuffles (of either type)?

We will call a pair position positions in which one is in the kth spot (starting at $k = 1$) and another is in the $n - k + 1$th spot. Notice that these are in mirror positions down the middle of the deck of cards. We claim that cards from a pair position, after shuffling, will still remain in a pair position.

Proof: Suppose we take the riffle shuffle such that the top card is still on top. Then, the kth position card gets sent to the $2(k-1) + 1 = 2k - 1$th position. (Here, we take $k \leq \frac{n}{2}$ to ensure this specific card is on top.) This is because there are $k - 1$ cards originally above the kth position, which each gets paired with a card from the bottom half. Therefore, the new position would be below the $2(k-1)$th position. For the originally $n - k + 1$th position, there are $n - k - \frac{n}{2} = \frac{n}{2} - k$ cards in the bottom half

above that card. Then, the new position would be $2(\frac{n}{2}-k)+2 = n-2k+2$ because the new card position is after the $\frac{n}{2}-k$ cards get paired and also after the next top half card is put down. Now we can see that if we let $\tilde{k} = 2k-1$, we see that the $2k-1 = \tilde{k}$th card and $n-2k+2 = n-\tilde{k}+1$th cards are still in pair positions. The shuffling took cards from a pair position to another pair position.

Similarly, if we took the riffle shuffle in which the top card is not still on top, we would have the kth position card sent to the $2k$th position, and the $n-k+1$th position card sent to the $n-2k+1$th position. Taking $\tilde{k} = 2k$, we see again that the two cards are in position because they are in the $2k = \tilde{k}$th position and $n-2k+1 = n-\tilde{k}+1$th positions.

Let's say shuffling is a function that takes each pair of cards in pair positions to another pair position (individual card placements do not matter: we just want to know that the pair as a whole is preserved). We proved this happens for our two riffle shuffles.

The function is also injective. Suppose we have two distinct pairs with each pair having positions k_1 and k_2 as their top half card. Then for a riffle shuffle where the top stays on top, these cards are sent to the $2k_1-1$th and $2k_2-1$th positions, respectively. These must be different: assuming not, $2k_1-1 = 2k_2-1$ yields $k_1 = k_2$, which is a contradiction. Similarly, for a riffle shuffle where the top doesn't stay on top, these cards are sent to the $2k_1$th and $2k_2$th positions, respectively. Again, these must be different. Since we have established that a pair can be determined by one card, we now know that two different pairs must get sent to two different pair positions.

The function is also surjective: if a certain new pair position is not hit by a pair, there would be $\frac{n}{2}$ pairs going into at most $\frac{n}{2}-1$ pair positions, and by the pigeonhole principle, one of the pairs must go into the same pair position, contradicting injectivity.

Because this described shuffling function is bijective, we have that each card in a pair position gets sent to a new pair position by this function, and each possible new pair position is obtained. We have proved the stated claim.

Now, it is inductively clear that cards in pair position will remain in pair position. We can then find a counterexample for every even n. We label each card from top to bottom 1 to n. Then the shuffle from top to bottom $1, n, 2, 3, ...n-1$ is impossible because 1 and n are no longer in pair positions.

The next problem require the notions of *group* and *group homomorphism*, which will be introduced in class on Wednesday.

First, a definition: For any set X, write $\mathrm{Fun}(X)$ for the set of functions $f : X \to X$ from X to itself. Within it, we have the subset $\mathrm{Bij}(X)$ of functions f that are *bijective*.

(9) Show that function composition defines an operation

$$\circ : \mathrm{Fun}(X) \times \mathrm{Fun}(X) \to \mathrm{Fun}(X)$$

with the following properties:

- It is *associative*: $f \circ (g \circ h) = (f \circ g) \circ h$;
- If $\mathrm{Id} : X \to X$ is the identity transformation $\mathrm{Id}(x) = x$, then $\mathrm{Id} \circ f = f \circ \mathrm{Id} = f$, for all $f \in \mathrm{Fun}(X)$;
- If $f \in \mathrm{Fun}(X)$, and there exists $\tilde{f} \in \mathrm{Fun}(X)$ satisfying $f \circ \tilde{f} = \mathrm{Id}$, then f is surjective and $\tilde{f}$ is injective.
- If $f \in \mathrm{Bij}(X)$, then there exists a unique $f^{-1} \in \mathrm{Bij}(X)$ such that $f \circ f^{-1} = \mathrm{Id}$. Moreover, it also satisfies $f^{-1} \circ f = \mathrm{Id}$.

Conclude that $\mathrm{Bij}(X)$ equipped with the composition operation is naturally a group.

First bullet point: $\forall x \in X$, $f \circ (g \circ h)(x) = f(g(h(x))) = ((f \circ g) \circ h)(x)$, meaning $f \circ (g \circ h) = (f \circ g) \circ h$.

Second bullet point: $\forall x \in X$, $(\mathrm{Id} \circ f)(x) = \mathrm{Id}(f(x)) = f(x)$ because $f(x) \in X$. Also, $(f \circ \mathrm{Id})(x) = f(\mathrm{Id}(x)) = f(x)$. Therefore, $\mathrm{Id} \circ f = f \circ \mathrm{Id}$.

Third bullet point: Proving surjectivity of f: $\forall y \in X \exists x \in X$ such that $f(x) = y$. This is true because we can set $x = \tilde{f}(y)$. Since $f \circ \tilde{f} = \mathrm{Id}$, $f(x) = f(\tilde{f}(y)) = y$.

Proving injectivity of $\tilde{f}$ (i.e. proving that $\forall x_1, x_2 \in X, x_1 \neq x_2 \implies \tilde{f}(x_1) \neq \tilde{f}(x_2)$: By way of contradiction, suppose $x_1, x_2 \in X$ with $x_1 \neq x_2$ and $\tilde{f}(x_1) = \tilde{f}(x_2)$. Since we know $f \circ \tilde{f} = \mathrm{Id}$, we have $f(\tilde{f}(x_1)) = x_1$ and $f(\tilde{f}(x_2)) = x_2$. However, we now have $f(\tilde{f}(x_1)) = f(\tilde{f}(x_2)) = x_2$ but $x_1 \neq x_2$. This is a contradiction. Therefore, $\tilde{f}$ is injective.

Fourth bullet point: First, we define $\forall x \in X, f^{-1}(x) = y$ for which $y \in X$ with $f(y) = x$. We know that such a y must exist by surjectivity of f. For each input in f^{-1}, there must be only one output, for if $f^{-1}(x) = y_1$ and $f^{-1}(x) = y_2$, we have $f(y_1) = x$ and $f(y_2) = x$ by our definition. Therefore, $f(y_1) = f(y_2) \implies y_1 = y_2$ since f is injective. Therefore, f^{-1} is a function.

We now want to demonstrate that $f \circ f^{-1} = \mathrm{Id}$. $\forall x \in X, f(f^{-1}(x)) = f(y)$ where $f(y) = x$. We know such a y exists because f is surjective. So $f(f^{-1}(x)) = x$. Since $\forall x \in X$, $f \circ f^{-1}(x)$ yields x, it is the identity function Id.

Next, we want to demonstrate that $\forall x \in X, (f^{-1} \circ f)(x) = x$. $(f^{-1} \circ f)(x) = f^{-1}(f(x))$. By definition, $f^{-1}(f(x))$ is the element $\tilde{x}$ in X such that $f(\tilde{x}) = f(x)$. We notice that $\tilde{x} = x$ satisfies this, and its uniqueness follows from injectivity of f. Therefore, $f^{-1}(f(x)) = x$. Since $\forall x \in X, (f^{-1} \circ f)(x) = x$, we can conclude that $f^{-1} \circ f = \mathrm{Id}$.

Lastly, we wish to demonstrate that f^{-1} is bijective. Since we already proved that $f \circ f^{-1} = \mathrm{Id}$, by the third bullet point we know that f^{-1} is injective. We only need to prove surjectivity now. This means that $\forall y \in X$, $\exists x \in X$ for which $f^{-1}(x) = y$. By definition, $f^{-1}(x) = y$ when $f(y) = x$ Since f is a function on X, we know that $f(y)$ must exist. Therefore, if we let $x = f(y)$, we have $f^{-1}(x) = f^{-1}(f(y)) = y$, thereby proving surjectivity: $\forall y \in X$, $\exists x \in X$ for which $f^{-1}(x) = y$. Since $f^{-1} \in \mathrm{Fun}(X)$ is injective and surjective, $f^{-1} \in \mathrm{Bij}(X)$.