Math 127: Equivalence Relations

Mary Radcliffe

1 Equivalence Relations

Relations can take many forms in mathematics. In these notes, we focus especially on equivalence relations, but there are many other types of relations (such as order relations) that exist.

Definition 1. Let X, Y be sets. A *relation* $R = R(x, y)$ is a logical formula for which x takes the range of X and y takes the range of Y, sometimes called a *relation from* X *to* Y. If $R(x, y)$ is true, we say that x *is related to* y *by* R, and we write xRy to indicate that x is related to y by R.

Example 1. Let $f : X \to Y$ be a function. We can define a relation R by $R(x, y) \equiv (f(x) = y)$.

Example 2. Let $X = Y = \mathbb{Z}$. We can define a relation R by $R(a, b) \equiv a|b$.

There are many other examples at hand, such as ordering on $\mathbb{R}$, multiples in $\mathbb{Z}$, coprimality relationships, etc. The definition we have here is simply that a relation gives some way to connect two elements to each other, that can either be true or false.

Of course, that's not a very useful thing, so let's add some conditions to make the relation carry more meaning. For this, we shall focus on relations from X to X, also called relations *on* X. There are several properties that will be interesting in considering relations:

Definition 2. Let X be a set, and let $\sim$ be a relation on X.

- We say that $\sim$ is *reflexive* if $x \sim x \ \forall x \in X$.
- We say that $\sim$ is *symmetric* if $x \sim y \Rightarrow y \sim x \ \forall x, y \in X$.
- We say that $\sim$ is *antisymmetric* if $x \sim y \wedge y \sim x \Rightarrow x = y \ \forall x, y \in X$.
- We say that $\sim$ is *transitive* if $x \sim y \wedge y \sim z \Rightarrow x \sim z \ \forall x, y, z \in X$.

Example 3. Let $X = \mathbb{Z}$, and define a relation $\sim$ by $x \sim y \equiv \gcd(x, y) = 1$. Let's consider what properties $\sim$ satisfies.

- Reflexivity: NO. Take $|x| > 1$, then $\gcd(x, x) = x \neq 1$, so $x \sim x$ is almost never true.
- Symmetry: YES. Since $\gcd(x, y) = \gcd(y, x)$, we definitely have symmetry.
- Antisymmetry: NO. Obviously we can't have symmetry and antisymmetry at the same time.
- Transitivity: NO. Take $x = 10, y = 9, z = 20$. Then we have $x \sim y$ and $y \sim z$, but we definitely don't get $x \sim z$.

Example 4. Let $X = \mathbb{R}$, and define a relation $\leq$ as is standard. Let's consider what properties $\leq$ satisfies.

- Reflexivity: YES. Certainly $x \leq x$ is always true.
- Symmetry: NO. It doesn't make sense that $x \leq y \Rightarrow y \leq x$.
- Antisymmetry: YES. If $x \leq y \wedge y \leq x$, it is standard to conclude that $x = y$.
- Transitivity: YES. If $x \leq y \wedge y \leq z$, we know that $x \leq z$.

What we are most interested in here is a type of relation called an *equivalence relation*.

Definition 3. A relation R on X is called an equivalence relation if it is reflexive, symmetric, and transitive.

Example 5. Define a relation $\sim$ on $\mathbb{Z}$ by $x \sim y$ if x and y have the same parity (even or odd). We claim that $\sim$ is an equivalence relation:

- Reflexivity: Since x has the same parity as x, $x \sim x$.
- Symmetry: If $x \sim y$, then x and y have the same parity. Thus y and x have the same parity, and hence $y \sim x$.
- Transitivity: If $x \sim y$, then x and y have the same parity. If $y \sim z$, then y and z have the same parity. Since y has only one parity, we can thus conclude that x and z have the same parity, so $x \sim z$.

Therefore $\sim$ is an equivalence relation.

What we notice about this example is that the equivalence relation we defined sliced up $\mathbb{Z}$ into two groups: the evens, and the odds. Everything in the evens group is related to everything else in the evens group under $\sim$, and everything in the odds group is related to everything else in the odds group under $\sim$, but there are no relations between the evens and odds. In general, this is exactly how equivalence relations will work.

Theorem 1. *Let X be a set. Let*

$$\mathcal{S} = \{R \mid R \text{ is an equivalence relation on } X\},$$

and let

$$\mathcal{U} = \{\text{pairwise disjoint partitions of } X\}.$$

Then there is a bijection $F : \mathcal{S} \to \mathcal{U}$, such that $\forall R \in \mathcal{S}$, if xRy, then x and y are in the same set of $F(R)$.

Proof. We first define the function F. Given a relation R, define $[x]_R = \{y \in X \mid xRy\}$. We then define the function F by $F(R) = \{[x]_R \mid x \in X\}$. We must first show that F is well defined; that is, that $F(R)$ is a pairwise disjoint partition of X.

We note that there are two properties to verify: that these sets are pairwise disjoint, and that they cover all of X. First, let us consider pairwise disjointness. Let $x \in X$, and note that $x \in [x]_R$ by symmetry, so $x \in \cup_{A \in F(R)} A$. This verifies that $F(R)$ covers all of X.

Now, let us suppose that for some $y \in X$, we also have that $x \in [y]_R$ for some $y \in X$. Let $z \in [y]_R$. Then $y \sim x$ and $y \sim z$, so by symmetry and transitivity, we have $x \sim z$. Thus, $z \in [x]_R$ $\forall z \in [y]_R$, so $[y]_R \subseteq [x]_R$. But then $y \in [x]_R$, so by repeating this argument we obtain $[x]_R \subseteq [y]_R$. Thus, $[y]_R = [x]_R$, and hence x appears only in the set $[x]_R$ in $F(R)$. This establishes pairwise disjointness.

Hence, the function is well-defined.

Next, we establish bijectivity.

For injectivity, suppose that R_1 and R_2 are equivalence relations on X, and $R_1 \not\equiv R_2$. Then there exist $x, y \in X$ that are related under one of R_1, R_2, but not the other; wolog, say xR_1y and $x \not R_2 y$. Then $y \in [x]_{R_1}$, but $y \notin [x]_{R_2}$, and hence $F(R_1) \neq F(R_2)$. Thus, the function is injective.

For surjectivity, let U be a pairwise disjoint partition of X. Define a relation R on X by $xRy \equiv (x, y$ are in the same set in $U)$. It is straightforward to establish that this is an equivalence relation, and that $F(R) = U$. Hence F is surjective.

We note, moreover, that the property described on F is immediate by definition of F. □

This theorem allows us fundamentally to think about equivalence relations as giving a mathematically precise way to simply break up a set into a partition that has properties we like. Indeed, we often care almost exclusively about the partitioning we have performed, and hence we give this a special name.

Definition 4. Let $\sim$ be an equivalence relation on X. The set $[x]_\sim$ as defined in the proof of Theorem 1 is called the *equivalence class*, or simply *class* of x under $\sim$. We write $X/\sim = \{[x]_\sim \mid x \in X\}$.

Example 6. If we consider the equivalence relation as defined in Example 5, we have two equivalence classes: odds and evens. We can then write $\mathbb{Z}/\sim = \{\{\text{odd integers}\}, \{\text{even integers}\}\}$.

2 Modular Arithmetic

The most important reason that we are thinking about equivalence relations is to apply them to a particular situation. Specifically, we are interested in developing some theory around what is usually called modular arithmetic.

Definition 5. Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. We say that a *is congruent to* b *modulo* n if $n|(a-b)$. We write this as $a \equiv b \pmod{n}$.

We note the following theorem, whose proof is left as an exercise to the interested reader (but is quite straightforward).

Theorem 2. *Let $n \in \mathbb{N}$ and let $a, b \in \mathbb{Z}$. TFAE:*

1. $a \equiv b \pmod{n}$.
2. *a and b leave the same remainder when divided by n.*
3. $a = b + kn$ *for some* $k \in \mathbb{Z}$.

Notice that this theorem is sufficient to establish the following corollary:

Corollary 1. *Congruence modulo n is an equivalence relation on $\mathbb{Z}$.*

This is immediate, as the dividing of $\mathbb{Z}$ into classes based on what remainder is left when dividing by n is clearly a pairwise disjoint partition of $\mathbb{Z}$, since remainders are unique by the Division Theorem. Hence, using part (b) of Theorem 2 together with Theorem 1, we immediately have that congruence forms an equivalence relation on $\mathbb{Z}$.

Definition 6. Let $n \in \mathbb{N}$. We denote by $\mathbb{Z}_n$ or $\mathbb{Z}/n\mathbb{Z}$ the set of equivalence classes under the relation of congruence modulo n.

Now, what we'd really like to do is think about how we can perform arithmetic operations modulo n, and if there is a consistent way to do so. That is to say, is there a well-defined way to understand $[a]_n + [b]_n$? Certainly, we could think of this as $[a+b]_n$, but the question that must be answered here is whether this is a well-defined operation. Since there are many different elements in $[a]_n$, would the arithmetic look different if we selected a different representative, instead of a?

The good news is that, in most cases, the answer is no. The following theorem establishes that performing addition, multiplication, and subtraction is well-defined modulo n.

Theorem 3. *Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, and let $n \in \mathbb{N}$. Suppose, further, that $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$. Then*

1. $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$.
2. $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.
3. $a_1 - b_1 \equiv a_2 - b_2 \pmod{n}$.

Proof. The proofs of all three properties are similar. We include here only the proof of property 2, and leave the remaining proofs as an exercise.

Note that as $a_1 \equiv a_2 \pmod{n}$, we have by Theorem 2 that a_1 and a_2 have the same remainder when divided by n, so there exist q_1, q_2, r such that $0 \leq r < n$ and $a_1 = q_1 n + r$, $a_2 = q_2 n + r$. Likewise, there exist q_1', q_2', r' such that $0 \leq r' < n$ and $b_1 = q_1' n + r'$ and $b_2 = q_2' n + r'$.

Consider, then

$$\begin{aligned} a_1 b_1 - a_2 b_2 &= (q_1 n + r)(q_1' n + r') - (q_2 n + r)(q_2' n + r') \\ &= q_1 q_1' n^2 + q_1 n r' + q_1' n r + r r' - (q_2 q_2' n^2 + q_2 n r' + q_2' n r + r r') \\ &= n(q_1 q_1' n + q_1 r' + q_1' r - q_2 q_2' n - q_2 r' - q_2' r) + r r' - r r' \\ &= n(q_1 q_1' n + q_1 r' + q_1' r - q_2 q_2' n - q_2 r' - q_2' r). \end{aligned}$$

Then we have that $n | (a_1 b_1 - a_2 b_2)$, and hence by definition $a_1 b_1 \equiv a_2 b_2 \pmod{n}$. □

This allows us to perform these three basic arithmetic operations modulo n.

Example 7. Determine x so that

$$3x + 9 = 2x + 6 \pmod{7}.$$

Solution. We can perform subtraction, addition, and multiplication modulo 7. Moreover, as the theorem shows, we can replace a number with any other number that it shares congruence with modulo 7. First, we subtract $2x$ from both sides, and then subtract 9 from both sides, to obtain

$$x \equiv -3 \pmod{7}.$$

In general, we'd prefer to have positive numbers, so since $-3 \equiv 4 \pmod{7}$, we can write

$$x \equiv 4 \pmod{7}.$$

Ok, this is pretty great, but it's missing one operation! How do we perform division modulo n? Or even, can we?

Example 8. Determine x so that

$$3x \equiv 1 \pmod 7.$$

Notice that there's no meaningful way to write $x \equiv \frac{1}{3} \pmod 7$, since the equivalence relation of congruence modulo 7 is defined only in the integers. However, because we're very clever, we notice that 15 and 1 give the same remainder when divided by 7, so we can say that $x \equiv 5 \pmod 7$ will solve our problem.

But.... what if we're not very clever? Or what if the numbers are too big to just see the answer via observation. And also, will this always even work?

This leads us to our next section.

2.1 Multiplicative Inverses

As a reminder of how we defined division way back when, we had the following definition for the number $\frac{1}{n}$:

Definition 7. Let $n \in \mathbb{Z}$, with $n \neq 0$. We define $\frac{1}{n}$ to be a number such that $\frac{1}{n}n = 1$.

That is to say, our definition of division is really based on multiplication. The reciprocal if n is defined to be a number such that when you multiply by n, you get back to 1, the multiplicative identity. This is the definition we will adapt for modular arithmetic.

Definition 8. Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. We say that u is a *multiplicative inverse* for $a \pmod n$ if $au \equiv 1 \pmod n$.

So, in Example 8, we showed that 5 is a multiplicative inverse for 3 modulo 7. Let's take a look at another example:

Example 9. Determine x so that $3x \equiv 1 \pmod 6$.

Solution. Well, in the previous example we just checked that we had an x that worked. Since multiplication is the same for equivalent values, we can just try all the possible equivalence classes. That is to say, we can try all x between 1 and 6 to see if they are the inverse:

$$\begin{aligned}
3 \cdot 1 &\equiv 3 \not\equiv 1 \pmod 6 \\
3 \cdot 2 &\equiv 6 \not\equiv 1 \pmod 6 \\
3 \cdot 3 &\equiv 3 \not\equiv 1 \pmod 6 \\
3 \cdot 4 &\equiv 6 \not\equiv 1 \pmod 6 \\
3 \cdot 5 &\equiv 3 \not\equiv 1 \pmod 6 \\
3 \cdot 6 &\equiv 6 \not\equiv 1 \pmod 6
\end{aligned}$$

So.... nothing works. No such x exists.

So sometimes inverses exist, and sometimes they don't. Let's take a look at a few examples to see if we can develop some intuition as to why. Here, you can imagine that the existence of inverses has been brute forced, as in the previous example.

Example 10. Which numbers have inverses modulo 6?

By exhaustive checking:

1 has an inverse, 1
2 does not have an inverse
3 does not have an inverse
4 does not have an inverse
5 has an inverse, 5
6 does not have an inverse

Example 11. Which numbers have inverses modulo 7?

By exhaustive checking:

1 has an inverse, 1
2 has an inverse, 4
3 has an inverse, 5
4 has an inverse, 2
5 has an inverse, 3
6 has an inverse, 6
7 does not have an inverse

Example 12. Which numbers have inverses modulo 8?

By exhaustive checking:

1 has an inverse, 1
2 does not have an inverse
3 has an inverse, 3
4 does not have an inverse
5 has an inverse, 5
6 does not have an inverse
7 has an inverse, 7
8 does not have an inverse

Examining the above 3 examples, you might notice a pattern: multiplicative inverses do not exist anytime the number we are interested in shares a factor with the modulus. This, in general, is the feature we are looking for.

Theorem 4. *Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then a has a multiplicative inverse modulo n if and only if $a \perp n$.*

Proof. Notice:

$$\begin{aligned} a \text{ has an inverse modulo } n &\Leftrightarrow \exists u \in \mathbb{Z},\ n|(au-1) \qquad \text{(by definition)} \\ &\Leftrightarrow \exists u, v \in \mathbb{Z},\ au - 1 = nv \\ &\Leftrightarrow \exists u, v \in \mathbb{Z},\ au - nv = 1 \\ &\Leftrightarrow a \perp n \qquad \text{(by Bezout's Lemma)} \end{aligned}$$

□

Cool, so we know exactly when inverses exist! Moreover, we can explain what's going on with 7: 7 is prime, so it's relatively prime to every number (other than 7 itself). This is of course always going to work for primes:

Corollary 2. *Let $p \in \mathbb{N}$ be a prime, and let $a \in \mathbb{Z}$, with $p \not| a$. Then a has an inverse modulo p.*

This, however, doesn't really help us to find inverses. We know when they exist, but we don't really know what they are. In homework, you will show that they are unique $(\mathrm{mod}\, n)$, but we don't have a mechanism for calculating them, at least not yet. So let's build one.

Definition 9. Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$. We define the *order* of a modulo n as

$$\inf\{k > 0 \mid a^k \equiv 1 \pmod{n}\},$$

if such a number exists. If not, we say that the order of a modulo n is infinite.

Theorem 5. *Let $n \in \mathbb{N}$ and let $a \in \mathbb{Z}$. Then a is of finite order modulo n if and only if $a \perp n$.*

Proof. First, suppose that $a \not\perp n$. Then a does not have a multiplicative inverse modulo n. Suppose, for the sake of contradiction, that the order of a is finite; say the order of a is $k > 0$. Then $a^k \equiv 1 \pmod{n}$, and hence $a(a^{k-1}) \equiv 1 \pmod{n}$, so a^{k-1} is a multiplicative inverse for a, which is impossible.

For the other direction, suppose that $a \perp n$. Then by Theorem 4, a does have a multiplicative inverse modulo n, say u.

Now, consider $S = \{a^k \pmod{n} \mid k \in \mathbb{N}\}$. Notice that as there are only n distinct equivalence classes modulo n, we have that $|S| \leq n$. Hence, by the Pigeonhole Principle, there must exist $k, \ell \in \mathbb{N}$, with $k \neq \ell$ and $a^k \equiv a^\ell \pmod{n}$. WOLOG, suppose that $k > \ell$. Then we have

$$\begin{aligned} a^k \equiv a^\ell \pmod{n} &\Rightarrow a^k u^\ell \equiv a^\ell u^\ell \pmod{n} \\ &\Rightarrow a^{k-\ell} a^\ell u^\ell \equiv a^\ell u^\ell \pmod{n} \\ &\Rightarrow a^{k-\ell} \equiv 1 \pmod{n} \\ &\Rightarrow \text{the order of } a \text{ is at most } k - \ell, \text{ which is finite.} \end{aligned}$$

□

Cool! So if we wanted to find an inverse to an element, it is enough just to multiply that element by itself, and eventually we'll get to the identity. For example:

Example 13. Calculate a multiplicative inverse for $8 \pmod{17}$.

Solution. By Theorem 5, we know that for some $k > 0$, we have that $10^k \equiv 1 \pmod{17}$. We then would have that the inverse of 10 is 10^{k-1}. So we can just check what the order of 10 is mod 17,

by repeatedly multiplying by 10 until we get 1.

$$\begin{aligned}
10^1 &\equiv 10 \pmod{17} \\
10^2 &\equiv 100 \equiv 15 \pmod{17} \\
10^3 &\equiv 10 \cdot 15 \equiv 150 \equiv 14 \pmod{17} \\
10^4 &\equiv 10 \cdot 14 \equiv 140 \equiv 4 \pmod{17} \\
10^5 &\equiv 10 \cdot 4 \equiv 40 \equiv 6 \pmod{17} \\
10^6 &\equiv 10 \cdot 6 \equiv 60 \equiv 9 \pmod{17} \\
10^7 &\equiv 10 \cdot 9 \equiv 90 \equiv 5 \pmod{17} \\
10^8 &\equiv 10 \cdot 5 \equiv 50 \equiv 16 \pmod{17} \\
10^9 &\equiv 10 \cdot 16 \equiv 160 \equiv 7 \pmod{17} \\
10^{10} &\equiv 10 \cdot 7 \equiv 70 \equiv 2 \pmod{17} \\
10^{11} &\equiv 10 \cdot 2 \equiv 20 \equiv 3 \pmod{17} \\
10^{12} &\equiv 10 \cdot 3 \equiv 30 \equiv 13 \pmod{17} \\
10^{13} &\equiv 10 \cdot 13 \equiv 130 \equiv 11 \pmod{17} \\
10^{14} &\equiv 10 \cdot 11 \equiv 110 \equiv 8 \pmod{17} \\
10^{15} &\equiv 10 \cdot 8 \equiv 80 \equiv 12 \pmod{17} \\
10^{16} &\equiv 10 \cdot 12 \equiv 120 \equiv 1 \pmod{17}
\end{aligned}$$

Therefore, we obtain that the multiplicative inverse of $10 \pmod{17}$ is 10^15, which by our same set of calculations is congruent to $12 \pmod{17}$.

This, however, was a lot of freakin work. It basically was terrible. It would be very nice if we could get a simpler approach than just brute force multiplication, because it required a lot of steps. This will be the subject of the totient theorem in the next section.

2.2 Euler's Totient Theorem

Euler's totient function is a tool that shows up in lots of places in mathematics. We begin this section here by defining the totient and stating the theorem.

Definition 10. Let $n \in \mathbb{N}$. We define *Euler's φ-function* on n to be

$$\varphi(n) = |\{m \in \mathbb{N} \mid m < n \wedge m \perp n\}|.$$

That is to say, $\varphi(n)$ is just the number of integers less than n to which n is coprime. Since we know that every integer is congruent to a number at most n modulo n, we can also see this as asking how many equivalence classes modulo n have multiplicative inverses.

Example 14. If p is prime, then $\varphi(p) = p - 1$.

This is immediate, since p being prime means that p shares no factors with any number less than p. Hence, every positive integer less than p is coprime to p, so $\varphi(n) = p - 1$.

Example 15. If p is an odd prime, then $\varphi(2p) = p - 1$.

Notice that $2p$ can only share a factor with $m < 2p$ if either m is even or if $m = p$. Notice that there are $\left\lfloor \frac{2p-1}{2} \right\rfloor = \frac{2p-2}{2} = p - 1$ even numbers less than $2p$, and hence there are $p - 1 + 1 = p$ numbers less than $2p$ with which $2p$ shares a factor. Thus, the number of numbers less than $2p$ with which $2p$ is coprime is $(2p - 1) - (p) = p - 1$, so $\varphi(2p) = p - 1$.

Of course, the purpose of this section was ultimately to connect this idea to finding multiplicative inverses modulo n for some n. In particular, we have the following important theorem, known as Euler's Totient Theorem.

Theorem 6 (Euler's Totient Theorem)**.** *Let $n \in \mathbb{N}$, and let $a \in \mathbb{Z}$ with $a \perp n$. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Before we prove the theorem, let's think about what this tells us. We already know that if a is coprime to n, then we can find its multiplicative inverse by looking at powers of a. However, up to this point, we didn't know what power to look at, so we just had to keep slamming powers until we got the one we wanted. Now, though, we can simply take the power of a given by the φ function.

Example 16. Let's revisit Example 13 with this newfound knowledge.
We wish to calculate the multiplicative inverse of $10 \pmod{17}$. Since 17 is prime, we know that $\varphi(17) = 16$. By Euler's Totient Theorem, we know that $10^{\varphi(17)} = 10^{16} \equiv 1 \pmod{17}$. Hence, the multiplicative inverse of 10 modulo 17 is 10^{15}.
Now, of course, that's exactly what we discovered in the previous example. However, now that we know that what we're after is 10^{15}, we can calculate it much more efficiently. Consider:

$$\begin{aligned} 10^2 &\equiv 100 \equiv 15 \pmod{17} \\ 10^4 &\equiv (10^2)^2 \equiv 15^2 \equiv 225 \equiv 4 \pmod{17} \\ 10^8 &\equiv (10^4)^2 \equiv 4^2 \equiv 16 \pmod{17} \end{aligned}$$

Now, we can put these pieces together to get what we're really after, which is 10^{15}:

$$\begin{aligned} 10^{15} &\equiv 10^8 10^4 10^2 10 \pmod{17} \\ &\equiv 16 \cdot 4 \cdot 15 \cdot 10 \pmod{17} \\ &\equiv 160 \cdot 60 \pmod{17} \\ &\equiv 7 \cdot 9 \pmod{17} \\ &\equiv 63 \equiv 12 \pmod{17}. \end{aligned}$$

This is, generally, a lot less work than having to calculate all the powers of 10 modulo 17.

What remains, then, is to demonstrate a proof of the totient theorem.

Proof. [Proof of Theorem 6.] For simplicity, write $\varphi = \varphi(n)$. Since $a \perp n$, we know that a has a multiplicative inverse modulo n; let u denote this inverse.

Define $X = \{m < n \mid m \perp n\}$, the set of integers from 1 to n that are coprime to n. By definition, $|X| = \varphi$, and hence we can write $X = \{x_1, x_2, \ldots, x_\varphi\}$.

Claim 1: $ax_i \in X$ for all $1 \leq i \leq \varphi$.

Proof of Claim 1: Since $a \perp n$ and $x_i \perp n$, we must have that $ax_i \perp n$. This is immediate if we consider the gcd in terms of prime decompositions, as in Homework 10, problem 3. □

Hence, we can define a function $f : X \to X$ by $f(x_i) = ax_i \pmod{n}$, and this function is well defined.

Claim 2: f is bijective.

Proof of Claim 2: First, suppose that $f(x_i) \equiv f(x_j) \pmod{n}$. Then we must have that $ax_i \equiv ax_j \pmod{n}$. Multiplying by u on both sides, we thus obtain that $x_i \equiv x_j \pmod{n}$, and hence f is injective.

Therefore, since $f : X \to X$ is injective, we must have that $|X| = |f(X)|$. But this must imply that $f(X) = X$, since X is finite, and hence f is also surjective.

Therefore, f is bijective. □

For $1 \leq i \leq \varphi$, put $y_i = f(x_i)$. Since f is a bijection, we have that $X = \{x_1, x_2, \ldots, x_\varphi\} = \{y_1, y_2, \ldots, y_\varphi\}$ are two different enumerations of X, possibly listing the elements in a different order.

Therefore, if we consider $\prod_{x \in X} x$, we can write this as either $x_1 x_2 \ldots x_\varphi$ or as $y_1 y_2 \ldots y_\varphi$ and we will get the same outcome. Thus, we have

$$\begin{aligned} x_1 x_2 \ldots x_\varphi &\equiv y_1 y_2 \ldots y_\varphi \pmod{n} \\ &\equiv f(x_1) f(x_2) \ldots f(x_\varphi) \pmod{n} && \text{(by definition of } y_i\text{)} \\ &\equiv a x_1 a x_2 \ldots a x_\varphi \pmod{n} && \text{(by definition of } f\text{)} \\ &\equiv a^\varphi x_1 x_2 \ldots x_\varphi \pmod{n} \end{aligned}$$

Now, since $x_i \in X$ for all i, we have that $x_i \perp n$ for all i, so each x_i has a multiplicative inverse modulo n. In particular, put u_i to be the inverse to x_i for each $1 \leq i \leq \varphi$. Then multiplying both sides of the above equation by $u_1 u_2 \ldots u_\varphi$, we obtain

$$\begin{aligned} x_1 x_2 \ldots x_\varphi &\equiv a^\varphi x_1 x_2 \ldots x_\varphi \pmod{n} \\ x_1 x_2 \ldots x_\varphi u_1 u_2 \ldots u_\varphi &\equiv a^\varphi x_1 x_2 \ldots x_\varphi u_1 u_2 \ldots u_\varphi \pmod{n} \\ (x_1 u_1)(x_2 u_2) \ldots (x_\varphi u_\varphi) &\equiv a^\varphi (x_1 u_1)(x_2 u_2) \ldots (x_\varphi u_\varphi) \pmod{n} \\ 1 &\equiv a^\varphi \pmod{n} \end{aligned}$$

□