7. Modular Arithmetic

Let’s first discuss briefly the concept of an equivalence relation on a set.

**Definition 1.** Let $S$ be a set. A relation $\sim$ on $S$ is called an *equivalence relation* if the following hold for all $a, b, c \in S$:

1. $a \sim a$. (The reflexive property)
2. If $a \sim b$ then $b \sim a$. (The symmetric property)
3. If $a \sim b$ and $b \sim c$ then $a \sim c$. (The transitive property)

Equality is an equivalence relation on any set. But there are many other examples of equivalence relations. For example, let $S$ be the set of all people. Define a relation $\sim$ on $S$ by setting, for $P, Q \in S$, that $P \sim Q$ if and only if $P$ and $Q$ have the same birthday. As an example in a more mathematical setting, let $\Lambda$ be the set of all triangles. Define a relation $\sim$ on $\Lambda$ by defining, for $A, B \in \Lambda$ that $A \sim B$ if and only if $A$ and $B$ have the same perimeter. It is easy to see both of these are equivalence relations. On the other hand, the relation on $\Lambda$ (the set of all triangles) by $A \sim B$ if and only if $A$ and $B$ have at least one congruent angle is not an equivalence relation. (Why?)

**Exercise:** Define a relation $\sim$ on $\mathbb{Z}$ by $a \sim b$ if and only if $a - b$ is even. Is this an equivalence relation? What about if we define $a \sim b$ by $a - b$ is odd?

**Definition 2.** Let $n$ be a positive integer and $a, b \in \mathbb{Z}$. We say $a$ is congruent to $b$ modulo $n$ if $n \mid (a - b)$. We write this as $a \equiv b \pmod{n}$.

For example, $12 \equiv 22 \pmod{5}$, since $5 \mid (12 - 22)$. Also, $100 \equiv -11 \pmod{37}$, since $37 \mid (100 - (-11))$. On the other hand, $-14 \not\equiv 30 \pmod{7}$ since 7 does not divide $-14 - 30$.

Congruence modulo $n$ defines a relation on the set $\mathbb{Z}$ of integers by $a \sim b$ if $a \equiv b \pmod{n}$. In fact, it defines an equivalence relation on $\mathbb{Z}$.

**Exercise:** Prove that congruence modulo $n$ is an equivalence relation on $\mathbb{Z}$. That is, for all $a, b, c \in \mathbb{Z}$, the following hold:

1. $a \equiv a \pmod{n}$.
2. If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then $a \equiv c \pmod{n}$.

**Exercise:** Let $n$ be a positive integer, and $a \in \mathbb{Z}$. Let $r$ be the remainder upon dividing $a$ by $n$. Prove that $a \equiv r \pmod{n}$.

On the other hand, suppose $a \equiv s \pmod{n}$ and $0 \leq s < n$. Then $s$ is the remainder upon dividing $a$ by $n$. To see this, note that $n \mid (a - s)$, so $a - s = nq$ for some $q \in \mathbb{Z}$. Then $a = nq + s$. Since $0 \leq s < n$, $s$ must be the remainder. Therefore, the remainder upon dividing $a$ by $n$ is the smallest nonnegative integer which is congruent to $a$ modulo $n$. In fact, this remainder is
the only nonnegative integer less than \( n \) which is congruent to \( a \) modulo \( n \). We call this integer the least nonnegative residue of \( a \) modulo \( n \) and denote it by \( \text{lnr}(a, n) \). It is just another name for the remainder upon dividing \( a \) by \( n \).

Now, a very important property of congruence modulo \( n \) is that it respects the operations of addition and multiplication:

**Proposition 3.** Let \( n \) be a positive integer and \( a, b, c, d \in \mathbb{Z} \). Suppose that \( a \equiv b \pmod{n} \) and \( c \equiv d \pmod{n} \). Then

1. \( a + c \equiv b + d \pmod{n} \).
2. \( ac \equiv bd \pmod{n} \).
3. \( a^m \equiv b^m \pmod{n} \) for all \( m \geq 1 \).

*Proof.* By assumption, we have \( n \mid a - b \) and \( n \mid c - d \). This means that \( a - b = nr \) and \( c - d = ns \) for some \( r, s \in \mathbb{Z} \). So \( a = b + nr \) and \( c = d + ns \). Then \( (a + c) - (b + d) = (b + nr + d + ns) - (b + d) = nr + ns = n(r + s) \). This shows that \( n \) divides \( (a+b) - (c+d) \), which implies \( a + b \equiv c + d \pmod{n} \). For the second part, we have \( ac - bd = (b + nr)(d + ns) - bd = bd + bns + dnr + n^2rs - bd = bns + dnr + n^2rs = n(bs + dr + nrs) \). This shows that \( n \) divides \( ac - bd \), so \( ac \equiv bd \pmod{n} \). The proof of the last part is one of your homework problems. \( \square \)

**Exercise:** Without use of a calculator, find \( \text{lnr}((21)^{10}, 5) \) and \( \text{lnr}((39)^{17}, 5) \).

**Homework:**

1. Prove part 3 of Propostion 3. (Use induction.)
2. Find \( \text{lnr}((14)^{20}, 16) \)
3. Find \( \text{lnr}((10)^{100}, 101) \).