7.4 Modular Arithmetic

In this section, we'll explore some properties of modular arithmetic that will be useful in the next chapter, when we study cryptographic algorithms based on modular arithmetic. First, recall the definition of modular equivalence from 7.1 Introduction to Number Theory.

Definition. Let $a, b, n \in \mathbb{Z}$, and assume $n \neq 0$. We say that a **is equivalent to** b **modulo** n when $n \mid a - b$. In this case, we write $a \equiv b \pmod{n}$.

This definition captures the idea that a and b have the *same remainder* when divided by n. You should think of this congruence relation as being analogous to numeric equality, with a relaxation. When we write $a = b$, we mean that the numeric values of a and b are literally equal. When we write $a \equiv b \pmod{n}$, we we mean that if you look at the remainders of a and b when divided by n, those remainders are literally equal.

We will next look at how addition, subtraction, and multiplication all behave in an analogous fashion under modular arithmetic. The following proof is a little tedious because it is calculation-heavy; the main benefits here are practicing reading and using a new definition, and getting comfortable with this particular notation.

Theorem. For all $a, b, c, d, n \in \mathbb{Z}$, if $n \neq 0$, $a \equiv c \pmod{n}$, and $b \equiv d \pmod{n}$, then:

1. $a + b \equiv c + d \pmod{n}$
2. $a - b \equiv c - d \pmod{n}$
3. $ab \equiv cd \pmod{n}$

Translation. We will only show how to translate and prove (2), and leave (1) and (3) as exercises.

$$\forall a, b, c, d, n \in \mathbb{Z},\ \big(n \neq 0 \wedge (n \mid a - c) \wedge (n \mid b - d)\big) \Rightarrow n \mid (a - b) - (c - d).$$

Proof. Let $a, b, c, d, n \in \mathbb{Z}$. Assume that $n \neq 0$, $n \mid a - c$, and that $n \mid b - d$. This means we want to prove that $n \mid (a - c) - (b - d)$.

By the Divisibility of Linear Combinations Theorem, since $n \mid (a - c)$ and $n \mid (b - d)$, it divides their difference:

$$\begin{array}{l} n \mid (a - c) - (b - d) \\ n \mid (a - b) - (c - d) \end{array}$$

■

Modular division

The above example stated that addition, subtraction, and multiplication all preserve modular equivalence—but what above division? The following statement is a "divide by k" property, but is actually **False**:[1]

$$\forall a, b, k, n \in \mathbb{Z},\ n \neq 0 \wedge ak \equiv bk \pmod{n} \Rightarrow a \equiv b \pmod{n}$$

[1] A good exercise is to disprove this statement!

For the real numbers, division $\frac{x}{y}$ has a single "gap": division by y is undefined when $y = 0$. As we'll see in the next theorem, division in modular arithmetic has many such "gaps", but we can predict exactly where these gaps will occur.

Theorem. (*Modular inverse*) Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $\gcd(a, n) = 1$, then there exists $p \in \mathbb{Z}$ such that $ap \equiv 1 \pmod{n}$. (We say that p is a **modular inverse of** a **modulo** n.)

Translation. $\forall n \in \mathbb{Z}^+, \forall a \in \mathbb{Z},\ \gcd(a, n) = 1 \Rightarrow \big(\exists p \in \mathbb{Z},\ ap \equiv 1 \pmod{n}\big)$

Proof. Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Assume $\gcd(a, n) = 1$.

Since $\gcd(a, n) = 1$, by the GCD Characterization Theorem we know that there exist integers p and q such that $pa + qn = \gcd(a, n) = 1$.

Rearranging this equation, we get that $pa - 1 = qn$, and so (by the definition of divisibility, taking $k = q$), $n \mid pa - 1$.

Then by the definition of modular equivalence, $pa \equiv 1 \pmod{n}$.

■

From this theorem about modular inverses, we can build up a form of division for modular arithmetic. To gain some intuition, first think about division $\frac{a}{b}$ as the *solution* to an equation of the form $ax = b$. We'll turn this into a statement about modular equivalence now.

Example. Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $\gcd(a, n) = 1$, then for all $b \in \mathbb{Z}$, there exists $k \in \mathbb{Z}$ such that $ak \equiv b \pmod{n}$.

Translation. This statement is quite complex! Remember that we focus on translation to examine the structure of the statement, so that we know how to set up a proof. We aren't going to expand every single definition for the sake of expanding definitions.

$$\forall n \in \mathbb{Z}^+,\ \forall a \in \mathbb{Z},\ \gcd(a, n) = 1 \Rightarrow \big(\forall b \in \mathbb{Z},\ \exists k \in \mathbb{Z},\ ak \equiv b \pmod{n}\big).$$

Discussion. So this is saying that under the given assumptions, b is "divisible" by a modulo n. This comes after the theorem about modular inverses, so that should be useful. The conclusion is "there exists a $k \in \mathbb{Z}$ such that…" so that I know that at some point I'll need to define a variable k in terms of a, b, and/or n, which satisfies the modular equivalence statement.

I notice that the hypothesis here ($\gcd(a, n) = 1$) matches with the hypothesis from the previous theorem, so that seems to be something I can use. That gives me a $p \in \mathbb{Z}$ such that $ap \equiv 1 \pmod{n}$…

Wait, I can multiply both sides by b, right?!

Proof. Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Assume $\gcd(a, n) = 1$, and let $b \in \mathbb{Z}$. We want to prove that there exists $k \in \mathbb{Z}$ such that $ak \equiv b \pmod{n}$.

First, using the previous *Modular Inverses* theorem, since we assmed $\gcd(a, n) = 1$, we know that there exists $p \in \mathbb{Z}$ such that $ap \equiv 1 \pmod{n}$.

Second, we know from statement (3) of our first example above that multiplication preserves modular equivalence, and so we know $apb \equiv b \pmod{n}$.

Then we let $k = pb$, and we have that $ak \equiv b \pmod{n}$.

■

These two theorems bring together elements from all of our study of proofs so far. We have both types of quantifiers, mixed with a larger implication. We used the GCD Characterization Theorem for a key step in our proof. This illustrates the power of separating ideas into different statements and using each one to prove the next, just like we separate code into different functions in our programs!