1 Modular Arithmetic and its properties

One interesting form of equivalence among integers is what is called *modular congruence*. Informally we may think of two numbers as *congruent modulo n* when they have the same remainder on division by n. In some ways this is a generalization of the concept of parity: even numbers are those which leave a remainder of 0 when divided by 2, and odd numbers are those that leave a remainder of 1. So, for instance, one might think of -1, 7, and 79 as "congruent" modulo 4, because they all leave a remainder of 3 on division by 4. (this is not entirely obvious for -1, of course). This is an intuitive way of thinking about it, but in this course we are demanding rigor, so we need to come up with a more formal and explicit definition!

Definition 1. For integers a, b, and n, it is said that a is *congruent to b modulo n*, or that $a \equiv b \pmod{n}$ if and only if $n \mid a - b$.

Sor for instance, the above assertion that 7 and 79 were congruent modulo 4 is justified here by the explicit assertion that $4 \mid (79 - 7)$, which, if further jsutification was needed, could be confirmed by noting that $79 - 7 = 72 = 4 \cdot 18$.

There are several useful properties of modular arithmetic. First, there is the fact that congruence modulo n satisfies 3 popular properties of relations:

Proposition 1 (Reflexivity of modular congruence)**.** *If a and n are integers, then $a \equiv a \pmod{n}$.*

Proof. We know that $a - a = 0$, and one of the elementary results seen previously is that $n \mid 0$ for any integer n. Thus, since $n \mid a - a$, it follows from the definition of modular congruence that $a \equiv a \pmod{n}$. □

Proposition 2 (Symmetry of modular congruence)**.** *For integers a, b, and n, if $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*

Proof. Since $a \equiv b \pmod{n}$, it follows that $n \mid a - b$. We may use a result from the previous section (specifically, the result that asserted that any multiple of a number divisible by n was also divisible by n), to derive from $n \mid a - b$ that $n \mid (-1) \cdot (a - b)$, or, arithmetically simplifying, $n \mid b - a$. Then, by definition, $b \equiv a \pmod{n}$. □

Proposition 3 (Transitivity of modular congruence)**.** *For integers a, b, c, and n, if $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Proof. Since $a \equiv b \pmod{n}$, it follows that $n \mid a - b$. Likewise, since $b \equiv c \pmod{n}$, it follows that $n \mid b - c$. Using a result from a previous day (that the sum of two numbers divisible by n is itself divisible by n), we may thus conclude that $n \mid (a - b) + (b - c)$; simplifying arithmetically, it follows that $n \mid a - c$, so $a \equiv c \pmod{n}$. □

Proposition 4 (Additivity of modular congruence)**.** *For integers a, b, c, d, and n, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $a + b \equiv c + d \pmod{n}$.*

Proof. Since $a \equiv c \pmod{n}$, it follows that $n \mid a - c$. Likewise, since $b \equiv d \pmod{n}$, it follows that $n \mid b - d$. Using a result from a previous day (that the sum of two numbers divisible by n is itself divisible by n), we may thus conclude that $n \mid (a - c) + (b - d)$; rearranging arithmetically, it follows that $n \mid (a + b) - (c + d)$, so $a + b \equiv c + d \pmod{n}$. □

Proposition 5 (Multiplicitivity of modular congruence)**.** *For integers a, b, c, d, and n, if $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$, then $ab \equiv cd \pmod{n}$.*

Proof. Since $a \equiv c \pmod{n}$, it follows that $n \mid a - c$. Likewise, since $b \equiv d \pmod{n}$, it follows that $n \mid b - d$. From these two divisibility criteria, we may use the linear condination theorem proven yesterday to show that

$$n \mid [b(a-c) + c(b-d)]$$

which will simplify algebraically to $n \mid ab - cd$, so $ab \equiv cd \pmod{n}$. $\square$