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* ≡ *b* (mod *n*) if and only if *n* | *a* − *b*.

So for instance, the above assertion that 7 and 79 were congruent modulo 4 is justified here by the explicit assertion that 4 | (79 − 7), which, if further justification was needed, could be confirmed by noting that 79 − 7 = 72 = 4 · 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 ≡ a* (mod *n*).

*Proof.* We know that *a* − *a* = 0, and one of the elementary results seen previously is that *n* | 0 for any integer *n*. Thus, since *n* | *a* − *a*, it follows from the definition of modular congruence that *a* ≡ *a* (mod *n*). □

**Proposition 2** (Symmetry of modular congruence). *For integers a, b, and n, if a ≡ b* (mod *n*), *then b ≡ a* (mod *n*).

*Proof.* Since *a* ≡ *b* (mod *n*), it follows that *n* | *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* | *a* − *b* that *n* | (−1) · (*a* − *b*), or, arithmetically simplifying, *n* | *b* − *a*. Then, by definition, *b* ≡ *a* (mod *n*). □

**Proposition 3** (Transitivity of modular congruence). *For integers a, b, c, and n, if a ≡ b* (mod *n*) *and b ≡ c* (mod *n*), *then a ≡ c* (mod *n*).

*Proof.* Since *a* ≡ *b* (mod *n*), it follows that *n* | *a* − *b*. Likewise, since *b* ≡ *c* (mod *n*), it follows that *n* | *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* | (*a* − *b*) + (*b* − *c*); simplifying arithmetically, it follows that *n* | *a* − *c*, so *a* ≡ *c* (mod *n*). □

**Proposition 4** (Additivity of modular congruence). *For integers a, b, c, d, and n, if a ≡ c* (mod *n*) *and b ≡ d* (mod *n*), *then a + b ≡ c + d* (mod *n*).

*Proof.* Since *a* ≡ *c* (mod *n*), it follows that *n* | *a* − *c*. Likewise, since *b* ≡ *d* (mod *n*), it follows that *n* | *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* | (*a* − *c*) + (*b* − *d*); rearranging arithmetically, it follows that *n* | (*a* + *b*) − (*c* + *d*), so *a* + *b* ≡ *c* + *d* (mod *n*). □

**Proposition 5** (Multiplicativity of modular congruence). *For integers a, b, c, d, and n, if a ≡ c* (mod *n*) *and b ≡ d* (mod *n*), *then ab ≡ cd* (mod *n*).
Proof. Since $a \equiv c \ (\text{mod } n)$, it follows that $n \mid a - c$. Likewise, since $b \equiv d \ (\text{mod } n)$, 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 $ab \equiv cd \ (\text{mod } n)$. \qed