

## Congruence mod $n$

Given a positive integer  $n$ , and two integers  $a$  and  $b$ , we say “ $a$  is congruent to  $b$  modulo  $n$ ” and write “ $a \equiv b \pmod{n}$ ” iff  $a - b$  is a multiple of  $n$  (or equivalently iff  $n$  divides  $a - b$ ). Example:  $(11) - (-19)$  is a multiple of 10, so  $11 \equiv -19 \pmod{10}$ .

Doerr and Levasseur define congruence in terms of division and remainders, but this only works when  $a$  and  $b$  are both non-negative, at least with respect to the ordinary way we think about division. (Of course, if you’re happy with saying that  $-19$  divided by 10 gives a quotient of  $-2$  and a remainder of 1, then Doerr and Levasseur’s approach shouldn’t cause you any confusion. For the rest of us, though, it’s better to use the “ $a - b$  is a multiple of  $n$ ” criterion, which is the one most mathematicians prefer anyway.)

Congruence mod  $n$  (with  $n$  fixed) is an example of an equivalence relation:

- $a \equiv a \pmod{n}$  for all  $a$  (reflexive property);
- If  $a \equiv b \pmod{n}$ , then  $b \equiv a \pmod{n}$  (symmetric property); and
- If  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ , then  $a \equiv c \pmod{n}$  (transitive property).

Consequently, the relation congruence-mod- $n$  gives a partition of the set of integers into blocks.

When  $n = 2$ , the two blocks are the set of even integers  $\{\dots, -4, -2, 0, 2, 4, \dots\}$  and the set of odd integers  $\{\dots, -3, -1, 1, 3, \dots\}$ . Two integers are congruent mod 2 iff they’re either both even or both odd.

When  $n = 10$ , there are ten blocks. One of them is  $\{\dots, -20, -10, 0, 10, 20, \dots\}$  (the set of multiples of ten); another is  $\{\dots, -19, -9, 1, 11, 21, \dots\}$  (the set of numbers that are 1 more than a multiple of ten); etc. Each of the ten blocks can be described as an arithmetic progression with difference 10.

If  $n$  is a positive integer, there are  $n$  blocks (also called equivalence classes) under the relation congruence-mod- $n$ , and each of them is an arithmetic progression with difference  $n$ . Two integers are equivalent mod  $n$  if they belong to the same block, that is, if they belong to the same arithmetic progression mod  $n$ , which happens precisely when the two numbers differ by a multiple of  $n$ .