

## MODULAR ARITHMETIC

## Why

We want to count in circles.<sup>1</sup>

## Definition

Let  $n \in \mathbf{Z}$  with n > 1 and take  $a, b \in \mathbf{Z}$ . The integers a and b are congruent modulo n (or with respect to the modulus n) if n is a divisor of their difference.<sup>2</sup>

<sup>&</sup>lt;sup>1</sup>Future editions will expand.

 $<sup>^2\</sup>mathrm{Future}$  editions will expand, and may need a sheet on congruence relations.

