

MODULAR ARITHMETIC

Why

We want to count in circles.¹

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.²

¹Future editions will expand.

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

