# Modular Arithmetic

Mathematics

Arithmetic on remainders, and exactly when division is allowed.

*Working in $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n.*

## 1 Reduce as you go

a ≡ b (mod n) means n divides a − b. Reduce at every step.

## 2 Add and multiply freely

Congruence respects + and ×, so reduce before or after either one.

## 3 Treat division separately

a has an inverse mod n exactly when gcd(a, n) = 1.

## 4 Find inverses

Run the extended Euclidean algorithm on a and n.

## 5 Use Fermat or Euler

For prime p not dividing a, a^(p−1) ≡ 1 (mod p).

**Cancellation fails in general: 2 × 3 ≡ 2 × 8 (mod 10), yet 3 is not congruent to 8. Only units may ever be cancelled.**