Worksheet: Arithmetic Modulo m

In this worksheet, we'll explore arithmetic modulo m. This means we do addition and multiplication, but instead of writing down the whole number, we only write the remainder after dividing by m. Think of it like working with a clock, where the numbers wrap around once you pass a certain point.

Key Definitions

Addition Modulo m: (a + b) mod m is the remainder when a+b is divided by m.

Multiplication Modulo m: (a × b) mod m is the remainder when a×b is divided by m.

Example 8:

Work in Z■■ (the set of remainders when dividing by 11).

a) Compute (7 + 9) mod 11.

b) Compute (7 × 9) mod 11.

Practice Example (Easier):

Work in Z■ (the set of remainders when dividing by 5).

a) Compute (3 + 7) mod 5.

b) Compute (3 × 7) mod 5.

Practice Example (Harder):

Work in Z■■ (the set of remainders when dividing by 17).

Compute ((12 × 15) + 9) mod 17.

Exploring Properties with Real Numbers

1. Closure: If you add or multiply two integers, you always get another integer. Example: $2+3=5$, $4\times7=28$.

2. Associativity: Grouping doesn’t change the result. Example: $(2+3)+4=9$ and $2+(3+4)=9$.

3. Commutativity: Order doesn’t matter. Example: $5+7=12$ and $7+5=12$. Same for multiplication.

4. Identity: Adding 0 or multiplying by 1 leaves numbers unchanged. Example: $7+0=7$, $9\times1=9$.

5. Additive Inverse: Every number has an opposite that adds to zero. Example: 6 and -6.

6. Distributivity: Multiplication spreads over addition. Example: $2\times(3+4)=14$ and $2\times3+2\times4=14$.

Reflection: How does modular arithmetic compare with ordinary arithmetic? Why do you think these properties are useful when working with modular arithmetic?