Lesson Plan: Divisibility, Congruences, and Modular Arithmetic

Class Length: 90 minutes

Topic: Number Theory Foundations – Divisibility and Modular Arithmetic

0–10 min | Warm-up & Motivation

• Introduce the question: Why do computers care about remainders? Use real-world hooks like clocks, encryption, and error-checking digits.

• Learning goals on board:

1. Understand divisibility and the division algorithm.

2. Use modular arithmetic with remainders.

3. Solve simple congruences and see crypto connections.

10–30 min | Divisibility & The Division Algorithm

• Direct instruction with definitions (divides, quotient, remainder).

• Worksheet A: Division Algorithm

- Guided example: 101 ÷ 13 = 7 remainder 10.

- Try it: 43 ÷ 5.

- Challenge: 2025 ÷ 29.

• Debrief: Check answers using $a = dq + r$ with $0 \leq r < d$.

30–55 min | Modular Arithmetic Basics

• Define congruences. Work through examples like $17 \equiv 5 \pmod{12}$.

• Worksheet B: Congruences

- Guided: $17 \equiv 5 \pmod{12}$.

- Try it: $20 \equiv 2 \pmod{9}$.

- Challenge: $-23 \equiv 4 \pmod{9}$.

• Transition: Introduce working with negatives and powers.

55–75 min | Arithmetic Modulo m

• Define addition and multiplication modulo m.

• Worksheet C: Tables & Inverses

- Build addition table in Z3.
- Guided multiplication table in Z5 (all elements invertible).
- Challenge: Multiplication in Z6 (zero divisors).

• Debrief: Highlight closure, identity, inverses, prime vs composite modulus.

75–90 min | Cryptography Connection & Wrap-Up

• Introduce modular exponentiation as crypto backbone.

• Worksheet D: Modular Powers & RSA Toy Example

- Guided: 7^4 (mod 10) by repeated squaring.
- Try it: 3^3 (mod 7).
- Challenge: Encrypt M = 4 with (e=3, n=33).

• Closing reflection: Why modular arithmetic powers are vital for security.

• Exit Question: Explain in one sentence why remainders matter for computers.