Modular Arithmetic

Definition 1. *If a and b are integers with $a \neq 0$, we say that a* divides *b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer.*

When a divides b we say that a is a factor *or* divisor *of b, and that b is a* multiple *of a.*

The notation $a|b$ denotes that a divides b. We write $a \not| b$ when a does not divide b.

1. Does $3|7$?

2. Does $4|3214$?

3. Use quantifiers to write the definition of $a|b$.

4. Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

5. Prove the following: Let a, b, and c be integers where $a \neq 0$. If $a|b$ and $a|c$, then $a|(b+c)$.

Check your answers by consulting page 238.

Definition 2. *If a and b are integers and m is a positive integer, then a is* congruent *to b* modulo m *if m divides $a - b$.*

We use the notation $a \equiv b \mod m$ to indicate that a is congruent to b modulo m.

We say that $a \equiv b \mod m$ is a congruence *and that m is its* modulus *(plural* moduli*).*

If a and b are not congruent modulo m we write $a \not\equiv b \mod m$.

6. Is $17 \equiv 5 \mod 6$?

7. Is $24 \equiv 14 \mod 6$?

Definition 3. *The set of all integers congruent to an integer a modulo m is called the* congruence class *of a modulo m.*

8. Write down four distinct integers in the congruence class of 5 modulo 6.

9. Find $13 \mod 3$

10. Find $-97 \mod 11$